

مصرف ليبيا المركزي

CENTRAL BANK OF LIBYA



القواعد التنظيمية لشبكة الدفع المحلية الليبية

Regulatory Rules of The Libyan
National Payment Scheme

BOOK 1
ORGANIZATION
PRINCIPLES

الكتاب 1
مبادئ التنظيم

Regulatory Rules of The Libyan National Payment Scheme

BOOK 1 ORGANIZATION PRINCIPLES

Important Information on Confidentiality and Copyright
©2023 CBL. All Rights Reserved.

This information is proprietary and Confidential to CBL. It is distributed to Libyan National Payment Scheme/Network participants programs. It must not be duplicated, published, distributed or disclosed, in whole or in part, to merchants, cardholders or any other person without prior written permission from CBL or National Payment Scheme/Network operator.

The logos, trade names, brand and service marks within Libya, whether registered or unregistered are trademarks owned by CBL.

NOTE:

All unspecified values listed in this document denoted by X or multiple X, will be defined later by relevant department at CBL.

القواعد التنظيمية لشبكة الدفع المحلية الليبية

الكتاب 1 مبادئ التنظيم

معلومات مهمة عن السرية وحقوق التأليف والنشر
مصرف ليبيا المركزي. كل الحقوق محفوظة ©2023

هذه المعلومات سرية ومملوكة لمصرف ليبيا المركزي. يتم توزيعها على برامج المشاركين في شبكة الدفع المحلية. لا يجب نسخ أو نشر أو توزيع أو الكشف عن هذه المعلومات، كلياً أو جزئياً، للتجار أو حاملي البطاقات أو أي شخص آخر دون إذن كتابي مسبق من مصرف ليبيا المركزي أو مشغل شبكة الدفع المحلية.

الشعارات والأسماء التجارية والعلامات التجارية وعلامات الخدمة داخل ليبيا، سواء كانت مسجلة أو غير مسجلة هي علامات تجارية مملوكة لمصرف ليبيا المركزي.

ملاحظة:

جميع القيم الغير معرفة المرموز لها بالرمز X أو تعدده سيتم تحديدها لاحقاً من الإدارات المختصة بمصرف ليبيا المركزي.

Table of Contents

Chapter 1 Regulatory Rules of Libyan National Payment Scheme.....25

Introduction.....25

1.1 The Purpose of this Document 25

1.2 Terms and Definitions 27

1.3 Scope of Regulation Rules and Instruction 31

1.4 Supervisory Power 31

1.5 National Scheme Operator and other Entities Role.....31

1.6 Methodology Followed for Rules and Regulations 33

1.7 Discrepancies 33

1.8 Membership & Types of Membership 35

1.8.1 Members and Participants Obligations 35

1.8.2 Classification of the Participants 37

1.8.3 Participants Management 37

1.8.4 Procedures for obtaining license 37

1.8.5 Service Provision Contract / Service Request Form.....37

1.9 Relevant Parties 37

1.9.1 Roles and Responsibilities of the Relevant Parties.....39

1.9.2 Obligations of the Relevant Parties 39

1.9.3 Termination of Relevant Parties 39

1.10 Intellectual Property and Ownership 41

1.10.1 Ownership and Privacy of the Rules and Regulations 41

1.10.2 Right to Manage and to Operate the National Scheme Operator 41

1.11 The Use and Implementation of Rules and Regulations 41

1.11.1 Products Management 41

1.11.2 Rules of Co-badging.....41

1.11.3 Rules of Brand Usage 43

1.11.4 Rules for clearing, settlement and acceptance of electronic transaction 43

1.11.5 Pricing and Interchange Rule 43

1.12 Fraud & Risk Management 43

1.12.1 Detection of Unusual Activities 45

1.12.2 Customers Awareness and Data Security 45

1.12.3 System Applications Security 45

1.12.4 Securing Information Confidentiality 45

1.13 Compliance with Rules & Regulations 47

1.14 Exceptions and Waivers 49

1.15 Rules of Handling Exceptions and Waivers 49

1.16 Work Flows 49

1.16.1 Purchasing Authorization Flow 49

جدول المحتويات

الفصل 1 - القواعد التنظيمية شبكة الدفع المحلية الليبية.....24

المقدمة: 24

1.1 الغرض من هذه الوثيقة: 24

2.1 المصطلحات والتعريفات: 26

3.1 مجال اختصاص القواعد التنظيمية والتعليمات: 30

4.1 السلطة الإشرافية: 30

5.1 اختصاصات مشغل شبكة الدفع المحلية والاعضاء الأخرى: 30

6.1 المنهجية المتبعة في إصدار القواعد واللوائح 32

7.1 التناقضات: 32

8.1 العضوية وأنواعها. 34

1.8.1 التزامات الأعضاء والمشاركين: 34

2.8.1 تصنيف المشاركين: 36

3.8.1 إدارة الاعضاء المشاركين: 36

4.8.1 إجراءات الحصول على التراخيص: 36

5.8.1 عقد تقديم الخدمة/ نموذج طلب الخدمة: 36

9.1 الأطراف المعنية: 36

1.9.1 أدوار ومسؤوليات الأطراف المعنية: 38

2.9.1 التزامات الأطراف المعنية: 38

3.9.1 إنهاء الأطراف المعنية: 38

10.1 حقوق الملكية الفكرية: 40

1.10.1 ملكية وخصوصية القواعد واللوائح: 40

2.10.1 الحق في إدارة وتشغيل مشغل شبكة الدفع المحلية: 40

11.1 استخدام وتطبيق القواعد واللوائح.....40

1.11.1 إدارة المنتجات.....40

2.11.1 قواعد العلامة المشتركة.....40

3.11.1 قواعد استخدام العلامة التجارية 42

4.11.1 قواعد المقاصة والتسوية وقبول المعاملات الإلكترونية 42

5.11.1 قواعد التسعير والتبادل.....42

12.1 إدارة الاحتيال والمخاطر.....42

1.12.1 الكشف عن الأنشطة الضارة 44

2.12.1 توعية العملاء وأمن البيانات 44

3.12.1 نظام أمن التطبيقات.....44

4.12.1 تأمين سرية المعلومات 44

13.1 الامتثال للقواعد واللوائح 46

14.1 الاستثناءات والتنازلات.....48

15.1 قواعد التعامل مع الاستثناءات والتنازلات.....48

1 سير العمل 48

1.16.1 سير تفويض الشراء 48

1.16.2 ATM Authorization Flow (off-us)	49
1.16.3 Clearing and Settlement Flow	49
1.16.4 Chargeback Flow	49
1.16.5 eCommerce 3DS 2.0 Flow	49
Chapter 2 - Members Compliance	51
2.1 Standards	51
2.2 Variances	51
2.3 Failure to Comply with a Standard	51
2.4 Conduct of Activity	53
2.5 Obligations of a Sponsor	53
2.6 Payment Service Providers	53
2.7 Financial Health	55
2.8 Compliance	55
2.9 Indemnity and Liability Limitations	55
2.10 Legal Jurisdiction	59
2.11 Scheme Right to Investigate and Audit	59
2.12 Member Rights and Obligations	61
2.12.1 Fees Payment	61
2.12.2 Taxes and Other Charges	63
2.12.3 Transactions Responsibility	63
2.12.4 Unbiased—POS Transactions	63
2.12.5 Unbiased—ATM and Bank Branch Terminal Transactions	63
2.12.6 Cooperation and Good Coexistences to Other Scheme Members and the National Scheme Operator	65
2.12.7 Prevention of Unjustifiable Enrichment	65
2.12.8 Transaction Queries and Disputes	65
2.13 Violations and Penalties – General	65
2.14 Violations and Penalties – Process	67
2.15 Persistent and Intentional Violations	67
2.16 Certification of Compliance	67
2.17 Appeals	67
2.18 Resolution of Appeal	69
2.19 Provision and Use of Information	69
2.19.1 Member Obligation to Provide Data	69
2.19.2 Confidential Information of Members	69
2.19.3 Member Use of Scheme Information	73
2.19.4 Confidentiality of Scheme Information	73
2.20 Data Security	73
2.20.1 Processing of Transaction-Related Personal Data	73
2.20.2 Data Subject Notice and Consent	75

2.16.1 سير تفويض أجهزة الصراف الآلي (off-us)	48
3.16.1 سير المقاصة والتسوية	48
4.16.1 سير تحميل التكاليف	48
5.16.1 سير التجارة الإلكترونية DS 3 2.0	48
الفصل 2 – امتثال الأعضاء	50
1.2 المعايير	50
2.2 الاختلاف	50
3.2 عدم الامتثال للمعيار	50
4.2 القيام بالنشاط	52
5.2 التزامات الراعي	52
6.2 مقدمي خدمة الدفع	52
7.2 المطابقة المالية	54
8.2 الامتثال	54
9.2 تحديد المسؤولية والتعويض	54
10.2 الولاية القانونية	58
11.2 حق النظام في التحقيق والتدقيق	58
12.2 حقوق الأعضاء والتزاماتهم	60
1.12.2 دفع الرسوم	60
2.12.2 الضرائب والرسوم الأخرى	62
3.12.2 مسؤولية المعاملات	62
4.12.2 معاملات الحيادية لنقاط البيع	62
5.12.2 المعاملات الحيادية لأجهزة الصراف الآلي وفروع المصرف	62
6.12.2 التعاون وحسن التعايش مع أعضاء النظام الآخرين ومشغل شبكة الدفع المحلية	64
7.12.2 منع الإثراء غير المشروع	64
8.12.2 الاستفسارات والنزاعات الخاصة بالمعاملات	64
13.2 المخالفات والجزاءات العامة	64
14.2 المخالفات والجزاءات العملية	66
15.2 المخالفات المستمرة والمتعمدة	66
16.2 شهادة الامتثال	66
17.2 الاستئناف	66
18.2 قرار الاستئناف	68
19.2 توفير واستخدام المعلومات	68
1.19.2 التزام العضو بتوفير البيانات	68
2.19.2 المعلومات السرية للأعضاء	68
3.19.2 استخدام الأعضاء لمعلومات النظام	72
4.19.2 سرية معلومات النظام	72
20.2 أمن البيانات	72
1.20.2 معالجة البيانات الشخصية ذات الصلة بالمعاملات	72
2.20.2 إشعار وموافقة موضوع البيانات	74

2.20.3 Data Subject Access to Personal Data	75
2.20.4 Integrity of Personal Data	75
2.21 Quarterly Submitted Report	75
2.21.1 Report Not Received	75
2.21.2 Incomplete or Erroneous Reports	77
2.21.3 Overpayment Claim/Refund of Fees	77
2.22 Transaction Requirements	77
2.23 Payment Authorization Service	79
2.24 Integrity of Brand and Network	79
Chapter 3 – Issuing	79
3.1 Issuer Requirements	79
3.1.1 Card Issuance - General requirements	79
3.1.2 Credit Card Issuance	81
3.1.3 Debit & Prepaid Card Issuance	81
3.1.3.1 Eligible Accounts – Debit	81
3.1.3.2 Ineligible Accounts	83
3.1.4 Appeals and Marketing - Linked Card Programs	83
3.1.5 Selective Authorization	83
3.1.6 Information to Cardholders	83
3.1.7 Limitation of Liability of Cardholders for Unauthorized Use (Zero Liability)	85
3.1.8 Lost or Stolen Card Reporting	85
3.1.9 Emergency Card Replacement	85
3.1.10 Emergency Request – Fines and Penalties	85
3.1.11 Proprietary Scheme Cardholder Loyalty Programs	87
3.1.12 ATM Usage	87
3.1.13 ATM Issuer Requirements	87
3.1.14 ATM Balance Inquiry Service	87
3.1.15 Tokenization of Accounts	87
3.1.16 Stand-in Processing	89
3.1.17 Chip Issuer Liability	89
3.1.18 EMV Liability Shift	89
3.1.19 Address Verification Service (AVS)	89
3.1.20 3-D Secure Participation Requirements	89
3.1.21 3-D Secure Participation Non-Compliance Penalties	89
3.1.22 Cardholder Authentication	89
3.1.23 Membership Management	91
3.1.24 Client Portfolio Management Self-Service Tools Requirements	91
3.1.25 Data Retention and Transmission	91
3.1.26 Card Shipping Requirements	91

3.20.2 وصول موضوع البيانات إلى البيانات الشخصية	74
4.20.2 سلامة البيانات الشخصية	74
21.2 التقرير المقدم ربع سنوي	74
1.21.2 تقارير لم يتم استلامها	74
2.21.2 تقارير غير كاملة أو خاطئة	76
3.21.2 مطالبة المدفوعات الزائدة/ استرداد الرسوم	76
22.2 متطلبات المعاملة	76
23.2 خدمة تفويض الدفع	78
24.2 سلامة العلامة التجارية والشبكة	78
الفصل 3 – الإصدار	78
1.3 متطلبات جهة الإصدار	78
1.1.3 إصدار البطاقة - القواعد العامة	78
2.1.3 إصدار بطاقة الائتمان	80
3.1.3 إصدار بطاقة الخصم والدفع المسبق	80
1.3.1.3 الحسابات المؤهلة – الخصم	80
2.3.1.3 الحسابات غير المؤهلة	82
4.1.3 التفعيل والتسويق - برامج البطاقات المرتبطة	82
5.1.3 التفويض الانتقائي	82
6.1.3 معلومات لحاملي البطاقات	82
7.1.3 تحديد مسؤولية حاملي البطاقات عن الاستخدام غير المصرح به (الإعفاء من المسؤولية)	84
8.1.3 الإبلاغ عن البطاقة الضائعة أو المسروقة	84
9.1.3 الاستبدال الطارئ للبطاقة	84
10.1.3 طلب الطوارئ - الغرامات والعقوبات	84
11.1.3 برامج ولاء حامل بطاقة لنظام الملكية	86
12.1.3 استخدام أجهزة الصراف الآلي	86
13.1.3 قواعد جهة إصدار أجهزة الصراف الآلي	86
14.1.3 خدمة الاستعلام عن الرصيد عن طريق أجهزة الصراف الآلي	86
15.1.3 ترميز الحسابات	86
16.1.3 المعالجة الاحتياطية:	88
17.1.3 مسؤولية جهة إصدار الشريحة	88
18.1.3 انتقال مسؤولية EMV	88
19.1.3 خدمة التحقق من العنوان (AVS)	88
20.1.3 متطلبات المشاركة الآمنة ثلاثية الأبعاد	88
21.1.3 عقوبات عدم الامتثال للمشاركة الآمنة ثلاثية الأبعاد	88
22.1.3 مصادقة حامل البطاقة	88
23.1.3 إدارة العضوية	90
24.1.3 متطلبات أدوات الخدمة الذاتية لإدارة محفظة العميل	90
25.1.3 حفظ ونقل البيانات	90
26.1.3 قواعد شحن البطاقة	90

3.2 Product Types	93
3.2.1 Consumer	93
3.2.2 Commercial.....	93
3.2.3 Governmental.....	95
3.3 Prepaid Cards	95
3.3.1 Prior Consent of the National Scheme Operator	95
3.3.2 Reservation of rights.....	95
3.3.3 Responsibility for the Prepaid Card Program.....	95
3.3.4 Categories of Prepaid Card Program	97
3.3.5 Return of Unspent Value.....	97
3.3.6 Value loading.....	99
3.3.7 Automatic Value Loads from Payment Cards.....	99
3.3.8 Communication and Marketing Materials	99
3.4 Non-Personalized Prepaid Card Programs	101
3.4.1 Ownership and Control of the Co-brand Program	101
3.4.2 Use of the Acceptance Brand Logos.....	103
3.5 Proprietary Accounts	103
3.5.1 Proprietary Account Access.....	103
3.5.2 Proprietary Account Types.....	103
3.5.3 Fees and Reporting Requirements.....	105
3.6 Virtual Accounts	105
3.7 Youth Card Programs	105
3.7.1 Appeal and Disclosure Requirements	107
3.8 Card Requirements.....	107
3.8.1 Principles of Standardization	107
3.8.2 Account Range and BIN Use.....	109
3.8.3 Primary Account Number.....	109
3.8.4 Signature Panel	109
3.8.5 Magnetic Stripe Encoding.....	109
3.9 Chip Cards	113
3.9.1 Chip Card Applications	113
3.9.2 Integrated Circuit Chip Providers	115
3.9.3 Multiple Application Chip Cards	115
3.10 Contactless Cards and Payment Devices	115
3.11 Contactless Cards and Mobile Payment Devices	115
3.12 Cardholder Verification Method	117
3.12.1 CVM Fallback (PIN Bypass)	119
3.13 Consumer Device Cardholder Verification Method (CDCVM).....	119
3.14 Card Verification Value	119

2.3 أنواع المنتجات	92
1.2.3 المستهلك	92
2.2.3 تجاري	92
3.2.3 حكومية	94
3.3 بطاقات الدفع المسبق	94
1.3.3 الموافقة المسبقة لمشغل شبكة الدفع المحلية.....	94
2.3.3 حفظ الحقوق	94
3.3.3 المسؤولية عن برنامج بطاقات الدفع المسبق.....	94
4.3.3 فئات برامج بطاقات الدفع المسبق.....	96
5.3.3 إرجاع قيمة الرصيد الباقي في الحساب.....	96
6.3.3 تحميل القيمة	98
7.3.3 تحميل القيمة تلقائياً من بطاقات الدفع.....	98
8.3.3 مواد الاتصال والتسويق	98
4.3 برامج بطاقات الدفع المسبق غير المخصصة	100
1.4.3 الملكية والتحكم في برنامج العلامة التجارية المشتركة	100
2.4.3 استخدام شعارات العلامات التجارية المقبولة	102
5.3 حسابات الملكية	102
1.5.3 الوصول إلى حساب الملكية	102
2.5.3 أنواع حسابات الملكية	102
3.5.3 الرسوم ومتطلبات الإبلاغ	104
6.3 الحسابات الافتراضية.....	104
7.3 برامج بطاقات الشباب	104
1.7.3 متطلبات الاستثناء والإفصاح	106
8.3 متطلبات البطاقة	106
1.8.3 مبادئ التوحيد القياسي.....	106
2.8.3 نطاق الحساب واستخدام رقم التعريف المصرفية	108
3.8.3 رقم الحساب الأساسي	108
4.8.3 لوحة التوقيع.....	108
5.8.3 ترميز الشريط المغناطيسي	108
9.3 بطاقات الشريحة	112
1.9.3 تطبيقات بطاقة الشريحة.....	112
2.9.3 مزودي شرائح الدوائر المتكاملة.....	114
3.9.3 بطاقات الشرائح متعددة التطبيقات	114
10.3 بطاقات وأجهزة الدفع عن بعد	114
11.3 بطاقات الخدمة عن بعد وأجهزة الدفع عبر الهاتف المحمول.....	114
12.3 طريقة التحقق من حامل البطاقة	116
1.12.3 نموذج التحقق من البطاقة الاحتياطية (تجاوز رقم التعريف الشخصي.....	118
13.3 إجراءات التحقق من حامل بطاقة جهاز المستهلك (CDCVM)	118
14.3 قيمة التحقق من البطاقة.....	118

3.14.1 Issuer Requirements for CVV	121
3.14.2 Issuer Requirements for CVV	121
3.14.3 CVV Calculation Methods	123
3.15 Service Codes	125
3.15.1 Valid Service Codes	127
3.15.2 Additional Service Code Information	127
3.16 Card Authentication Method	127
3.16.1 Additional Information	129
3.17 Chip Card Post-Issuance Updates	129
Chapter 4 - Payments Acceptance	129
4.1 Requirements of the Acquirer	129
4.1.1 Acquirer Jurisdiction	129
4.1.2 Acquirer Onboarding	135
4.1.3 The Merchant Agreements; Aggregated Transactions	135
4.1.4 Merchant Compliance with the Standard	137
4.1.5 Display of NUMO Logo	139
4.1.6 Transaction Message Data	139
4.1.7 Presentment of Transaction Record	141
4.1.8 Retention of Transaction Record	141
4.1.9 PCI DSS Certification for Acquirers, PSPs and Merchant	143
4.1.10 NUMO Token	143
4.1.11 Acquirer Obligations with Respect to Merchant	143
4.2 ATM and Other Cash Transaction	145
4.2.1 Display of NUMO Logo at ATM	145
4.2.2 ATM Network Requirement	145
4.2.3 ATM and Bank Branch Terminal Requirement	145
4.2.4 Use of a PIN for Transactions at ATMs and Bank Branch Terminal	147
4.2.5 ATM Decline	147
4.2.6 ATM Dispense Error	147
4.2.7 ATM Transaction Restrictions	147
4.2.8 ATM Balance Inquiry Service	147
4.2.9 ATM Access Fees	149
4.2.10 Manual Cash Disbursement Transactions	151
4.3 Merchant Requirements	159
4.3.1 The Usage of Numo Brand	159
4.3.2 Merchant Location	159
4.3.3 Agent Location	161
4.3.4 Responsibility for Transactions	161
4.3.5 Merchant Obligations for Card Acceptance	161

1.14.3 قواعد جهات الإصدار لقيمة التحقق من البطاقة 1	120
2.14.3 قواعد جهات الإصدار لقيمة التحقق من البطاقة 2	120
3.14.3 طرق حساب قيمة التحقق من البطاقة	122
15.3 رموز الخدمة	124
1.15.3 رموز الخدمة الصالحة	126
2.15.3 معلومات رمز الخدمة الإضافية	126
16.3 طريقة مصادقة البطاقة	126
1.16.3 معلومات إضافية	128
17.3 تحديثات ما بعد الإصدار لبطاقة الشريحة	128
الفصل 4 - قبول المدفوعات	128
1.4 متطلبات جهة القبول	128
1.1.4 اختصاص جهة القبول	128
2.1.4 إعداد جهة القبول	134
3.1.4 اتفاقيات التاجر؛ المعاملات المجمعة	134
4.1.4 امتثال التاجر للمعايير	136
5.1.4 عرض شعار علامة نمو	138
6.1.4 بيانات رسالة المعاملة	138
7.1.4 تقديم سجلات المعاملات	140
8.1.4 الاحتفاظ بسجلات المعاملات	140
9.1.4 شهادة PCI DSS للقبولين و مقدمي خدمات الدفع والتجار	142
10.1.4 رموز نمو	142
11.1.4 التزامات القابل فيما يتعلق بالتجار	142
2.4 أجهزة الصراف الآلي والمعاملات النقدية الأخرى	144
1.2.4 عرض علامة نمو على أجهزة الصراف الآلي	144
2.2.4 متطلبات شبكة أجهزة الصراف الآلي	144
3.2.4 متطلبات أجهزة الصراف الآلي و محطات فروع المصرف	144
4.2.4 استخدام رقم التعريف الشخصي للمعاملات في أجهزة الصراف الآلي ومحطات فرع المصرف	146
5.2.4 رفض أجهزة الصراف الآلي	146
6.2.4 خطأ صرف أجهزة الصراف الآلي	146
7.2.4 قيود معاملات أجهزة الصراف الآلي	146
8.2.4 خدمة الاستعلام عن رصيد أجهزة الصراف الآلي	146
9.2.4 رسوم الدخول إلى أجهزة الصراف الآلي	148
10.2.4 معاملات الصرف النقدي اليدوية	150
3.4 متطلبات التاجر	158
1.3.4 استخدام علامة نمو التجارية	158
2.3.4 موقع التاجر	158
3.3.4 موقع الوكيل	160
4.3.4 المسؤولية عن المعاملات	160
5.3.4 التزامات التاجر لقبول البطاقة	160

4.3.6 Partial Payment	169
4.3.7 Specific Terms of a Transaction	169
4.3.8 Floor Limit	171
4.3.9 Returned Products and Canceled Services	171
4.3.10 Refund Transactions	171
4.3.11 Transaction Records	171
4.4 Card Present Environment	173
4.4.1 Chip Card Acceptance – General Requirements	173
4.4.2 Contactless Chip Transaction	173
4.4.3 Magnetic Stripe Transaction	173
4.4.4 Merchant Procedures – Card-Present Transactions.....	175
4.4.5 Purchase with Cash Back Transactions.....	175
4.5 Card-Not-Present Environment	177
4.5.1 E-Commerce Transactions	177
4.5.2 Key-Entered Transactions	179
4.5.3 Mail Order and Telephone Order (MO/TO) Transactions	181
4.5.4 Credential-On-File Transactions	181
4.5.5 Recurring Payment Transactions	181
4.6 Specific Transaction Types	181
4.6.1 T&E Charges	181
4.6.2 General T&E	183
4.6.3 T&E Authorizations – Exemptions	183
4.6.4 Car Rental Merchants	183
4.6.5 Charges for Loss, Theft, or Damage	183
4.6.6 Delayed or Amended Charges	183
4.6.7 Car Rental Advance Deposit	185
4.6.8 Hotel Guaranteed Reservations	185
4.6.9 Timeshare Merchants	185
4.6.10 Education Payments	185
4.6.11 Tax and Other Government Payments	187
4.6.12 Government Payment Requirements	187
4.6.13 Unattended Fuel Dispensers and Other Unattended Terminals	187
4.6.14 Terminal Eligibility	187
4.6.15 Terminal Requirements	187
4.6.16 Terminal Function Keys	189
4.6.17 Terminal Responses	189
4.6.18 Terminal Transaction Log	189
4.6.19 POS Terminal Requirements	191
4.6.20 Hybrid Terminal Requirements	191

6.3.4 السداد الجزئي	168
7.3.4 الشروط المحددة للمعاملة	168
8.3.4 الحد الأدنى	170
9.3.4 المنتجات المرتجعة، والخدمات الملغاة	170
10.3.4 معاملات الاسترداد	170
11.3.4 سجلات المعاملات	170
4.4 حالة البطاقة الموجودة	172
1.4.4 قبول بطاقة الشريحة - المتطلبات العامة	172
2.4.4 معاملة الشريحة غير المتصلة	172
3.4.4 معاملة الشريط المغناطيسي	172
4.4.4 إجراءات التاجر - معاملات البطاقة الموجودة	174
5.4.4 الشراء باستخدام طريقة معاملات الاسترداد النقدي	174
5.4 حالة البطاقة غير الموجودة	176
1.5.4 معاملات التجارة الإلكترونية	176
2.5.4 المعاملات المدخلة بالمفتاح	178
3.5.4 معاملات الطلبات عبر البريد والطلبات عبر الهاتف	180
4.5.4 معاملات الاعتماد في الملف	180
5.5.4 معاملات الدفع المتكررة	180
6.4 أنواع المعاملات المحددة	180
1.6.4 رسوم السفر والترفيه	180
2.6.4 السفر والترفيه العام	182
3.6.4 تفويضات السفر والترفيه - الإعفاءات	182
4.6.4 تجار تأجير السيارات	182
5.6.4 رسوم الفقد أو السرقة أو التلف	182
6.6.4 الرسوم المتأخرة أو المعدلة	182
7.6.4 الإيداع المسبق لتأجير السيارات.....	184
8.6.4 حجوزات فندقية مضمونة	184
9.6.4 تجار المشاركة بالوقت.....	184
10.6.4 مدفوعات التعليم	184
11.6.4 الضرائب والمدفوعات الحكومية الأخرى	186
12.6.4 متطلبات الدفع الحكومية	186
13.6.4 محطات الوقود غير المراقبة، والمحطات الأخرى غير المراقبة	186
14.6.4 جهوزية المحطة	186
15.6.4 متطلبات المحطة	186
16.6.4 مفاتيح وظيفة المحطة	188
17.6.4 استجابات المحطة	188
18.6.4 سجل معاملات المحطة	188
19.6.4 متطلبات محطة نقاط البيع	190
20.6.4 متطلبات المحطة الهيئية	190

4.6.21 Contactless-enabled POS Terminals	193
4.6.22 Contactless-only POS Terminals	193
4.6.23 Mobile POS (MPOS) Terminals	195
4.6.24 Terminals without a Printer	195
4.7 Transaction Receipts	195
4.7.1 General Requirements	195
4.7.2 Transaction Receipt Contents	199
4.7.3 Transaction Receipts - CNP Transactions	201
4.7.4 Delayed Delivery Transaction Receipt Requirement	203
Chapter 5- Authorization – Clearing & Settlement Management	203
5.1 The Authorization Platform	203
5.1.2 Message Types: Dual Message System and Single Message System	205
5.1.3 Authorization Processing Functionality	219
5.1.4 Authorization Processing Flows	221
5.2 The Clearing System	227
5.2.1 Participation in the Clearing System	227
5.2.2 Clearing Messages	229
5.2.3 Clearing System Functionality	233
5.3 The Settlement System	235
5.3.1 Participation in the Settlement System	237
5.3.2 General Settlement Obligations	237
5.3.3 Settlement Best Practices	239
5.3.4 Interchange and Service Fees	241
5.3.5 Settlement Funds Transfer Obligations	241
5.3.6 Indemnification and Limitation of Liability of National Scheme Operator	243
5.3.7 Failure of a Principal Member to Discharge a Settlement Obligation	245
5.3.8 System Liquidity	247
5.3.9 Liability for Owned or Controlled Entities	247
5.3.10 Risk of Loss	249
5.3.11 Adjustment of Settlement Positions—Loss Allocation Among Members	251
5.3.12 Settlement Noncompliance - Cost Reimbursement, Noncompliance Assessments, and Compensation	253
5.4 Transaction Requirements and Processing Procedures	255
5.4.1 Authorization Service	255
5.4.2 Connecting to the Interchange System	259
5.4.3 Authorization Routing	259
5.4.4 Stand-In Processing Service	261
5.4.5 Obtaining an Authorization	261
5.4.6 Authorization Responses	263

21.6.4 محطات نقاط البيع غير المتصلة	192
22.6.4 محطات نقاط البيع الغير متصلة فقط	192
23.6.4 محطات نقاط البيع المتنقلة (MPOS)	194
24.6.4 المحطات الطرفية بدون طابعة	194
7.4 إيصالات المعاملات	194
1.7.4 المتطلبات العامة	194
2.7.4 محتويات إيصال المعاملة	198
3.7.4 إيصالات المعاملات - معاملات البطاقة غير الموجودة CNP	200
4.7.4 متطلبات استلام معاملات التسليم المتأخر	202
الفصل 5- التفويض - إدارة المقاصة والتسوية	202
1.5 منصة التفويض	202
2.1.5 أنواع الرسائل: نظام الرسائل المزدوجة ونظام الرسائل الواحدة	204
3.1.5 وظيفة معالجة التفويض	218
4.1.5 تدفقات معالجة التفويض	220
2.5 نظام المقاصة	226
1.2.5 المشاركة في نظام المقاصة	226
2.2.5 رسائل المقاصة	228
3.2.5 وظائف نظام المقاصة	232
3.5 نظام التسوية	234
1.3.5 المشاركة في نظام التسوية	236
2.3.5 التزامات التسوية العامة	236
3.3.5 أفضل ممارسات التسوية	238
4.3.5 رسوم التبادل والخدمة	240
5.3.5 التزامات تحويل أموال التسوية	240
6.3.5 تعويض وحدود مسؤولية مشغل شبكة الدفع المحلية	242
7.3.5 فشل العضو الرئيسي في إبراء الذمة من التزام التسوية	244
8.3.5 سيولة النظام	246
9.3.5 المسؤولية عن الكيانات المملوكة أو الخاضعة للسيطرة	246
10.3.5 مخاطر الخسارة	248
11.3.5 تعديل أوضاع التسوية - تخصيص الخسارة بين الأعضاء	250
12.3.5 عدم الامتثال للتسوية - سداد التكاليف، تقييمات عدم الامتثال والتعويضات	252
4.5 متطلبات المعاملات وإجراءات المعالجة	254
1.4.5 خدمة التفويض	254
2.4.5 التوصيل بنظام التبادل	258
3.4.5 توجيه التفويض	258
4.4.5 خدمة المعالجة الاحتياطية	260
5.4.5 الحصول على تفويض	260
6.4.5 استجابات التفويض	262

5.4.7 Pre-authorizations	267
5.4.8 Final Authorizations	269
5.4.9 Multiple Incremental Authorizations	269
5.4.10 Full Approvals	269
5.4.11 Full and Partial Reversals	271
5.4.12 ATM Transactions	273
5.4.13 Transaction Records	273
5.4.14 Transaction Queries and Disputes	275
5.4.15 Correction of Errors	275
Chapter 6 - Fraud & Risk Management	279
6.1 Payment System Integrity Standards	279
6.1.1 Connecting to the Network—Physical and Logical Security Requirements	279
6.1.2 Integrity of NUMO Brand and Network	281
6.1.3 CBL Anti-Money Laundering and Sanctions Requirements	281
6.1.4 Satisfaction of Minimum Financial Requirements	283
6.2 Scheme Risk Management Program	283
6.2.1 Scheme Risk Management Review Levels	283
6.2.2 Scheme Risk Management Program Review Topics	287
6.2.3 Scheme Risk Management Program Reports	289
6.2.4 Member Scheme Review Conditions	289
6.3 Fraud Loss Control Standards	291
6.3.1 Issuer Fraud Loss Control Programs	291
6.3.2 Acquirer Fraud Loss Control Programs	297
6.3.3 Noncompliance with Fraud Loss Control Standards	305
6.3.4 Counterfeit Card Fraud Loss Control Standards	305
6.4 Information Security Program—Personal Data	311
6.4.1 Protection of Personal Data	313
6.5 Information Security Program—Confidential Information and Account Data	315
6.5.1 Payment Card Industry (PCI) Security Standards	317
6.5.2 Cybersecurity Incentive Program	319
6.5.3 Account Data Compromise Events	323
6.6 Fraud Reporting Standards	347
6.6.1 Reporting Lost and Stolen Cards	349
6.6.2 Fraud and Loss Database Reporting Requirements	351
6.6.3 Criminal and Counterfeit Investigations	353
6.7 Merchant and Agent Screening and Monitoring Standards	355
6.7.1 Screening New Merchants and Agents	355
6.7.2 Terminated Merchant File	359
6.7.3 Ongoing Monitoring	361

7.4.5. التفويضات المسبقة	266
8.4.5. التفويضات النهائية	268
9.4.5. التفويضات الإضافية المتعددة	268
10.4.5. الموافقات الكاملة	268
11.4.5. العمليات العكسية الكاملة والجزئية	270
12.4.5. معاملات أجهزة الصراف الآلي	272
13.4.5. سجلات المعاملات	272
14.4.5. استفسارات ونزاعات المعاملات	274
15.4.5. تصحيح الأخطاء	274
الفصل 6 – مكافحة عمليات الاحتيال وإدارة المخاطر	278
1.6. معايير سلامة نظام الدفع	278
1.1.6. الاتصال بالشبكة - متطلبات الأمان المادية والمعنوية	278
2.1.6. سلامة العلامة التجارية وشبكة نمو	280
3.1.6. متطلبات مصرف ليبيا المركزي لمكافحة غسل الأموال والعقوبات	280
4.1.6. استيفاء الحد الأدنى من المتطلبات المالية	282
2.6. برنامج إدارة مخاطر النظام	282
1.2.6. مستويات مراجعة إدارة مخاطر النظام	282
2.2.6. موضوعات مراجعة برنامج إدارة مخاطر النظام	286
3.2.5. تقارير برنامج إدارة مخاطر النظام	288
4.2.6. شروط مراجعة نظام الأعضاء	288
3.6. معايير التحكم في خسائر الاحتيال	290
1.3.6. برامج التحكم في خسائر الاحتيال لجهة الإصدار	290
2.3.6. برامج التحكم في خسائر الاحتيال لجهة القبول	296
3.3.6. عدم الامتثال لمعايير التحكم في خسائر الاحتيال	304
4.3.6. معايير التحكم في خسائر احتيال البطاقات المزورة	304
4.6. برنامج أمن المعلومات - البيانات الشخصية	310
1.4.6. حماية البيانات الشخصية	312
5.6. برنامج أمن المعلومات - المعلومات السرية وبيانات الحساب	314
1.5.6. معايير الأمان الخاصة بصناعة بطاقات الدفع	316
2.5.6. برنامج حوافز الأمن السيبراني	318
3.5.6. حالات المساومة في بيانات الحساب	322
6.6. معايير الإبلاغ عن الاحتيال	346
1.6.6. الإبلاغ عن البطاقات المفقودة والمسرقة	348
2.6.6. متطلبات الإبلاغ عن قاعدة بيانات المزورة والمفقودة	350
3.6.6. التحقيقات الجنائية والاحتياطية	352
7.6. معايير فحص ومراقبة التاجر والوكيل	354
1.7.6. فحص التاجر والوكلاء الجدد	354
2.7.6. ملف التاجر الذي فسخت العلاقة معه	358
3.7.6. المراقبة المستمرة	360

6.7.4 Merchant Education and Behavior	361
6.7.5 High-Risk Merchants	363
6.7.6 Reporting Suspected Merchant Fraud	373
6.7.7 Chargeback Monitoring Program	373
6.7.8 Reporting Terminated Merchants	379
6.8 Card Validation Number and Service Code Data	379
6.8.1 Card Validation Number (CVV)	379
6.8.2 Service Codes	387
6.9 Card Recovery and Return	389
6.9.1 Merchant Card Retention and Return	389
6.9.2 ATM Card Retention and Return	391
6.9.3 Payment of Rewards	393
6.10 PIN Security Standards	395
6.10.1 PIN Entry Devices (PEDs) and Encrypting PIN Pads (EPPs)	397
6.10.2 Software-based PIN Entry using PIN CVM Applications	399
6.10.3 PIN Verification	401
6.10.4 PIN Encipherment	405
6.10.5 PIN Key Management	405
6.11 Terminal Security Standards	407
6.11.1 Hybrid Terminal Security Standards	407
6.11.2 Triple DES Standards	407
Appendix number (1)	409
Appendix number (2)	411
Appendix number (3)	411
Appendix number (4)	413
Appendix number (5)	413
Appendix number (6)	414
Appendix number (7)	415
Appendix number (8)	415
Appendix number (9)	417
Appendix number (10)	417
Appendix number (11)	417
Appendix number (12)	417
Appendix number (13)	417
Appendix number (14)	419
Appendix number (15)	419
Appendix number (16)	419
Appendix number (17)	419
Appendix number (18)	419

4.7.6. تعليم وسلوك التاجر	360
5.7.6. التجار ذوي المخاطر العالية	362
6.7.6. الإبلاغ عن احتيال تاجر مشتببه به	372
7.7.6. برنامج مراقبة رد المبالغ المدفوعة	372
8.7.6. الإبلاغ عن التجار الذين فسخت العلاقة معهم	378
8.6. رقم التحقق من البطاقة، وبيانات رمز الخدمة	378
1.8.6. رقم التحقق من البطاقة (CVV)	378
2.8.6. رموز الخدمة	386
9.6. استرداد وإعادة البطاقة	388
1.9.6. الاحتفاظ وإعادة بطاقة التاجر	388
2.9.6. الاحتفاظ وإعادة بطاقة جهاز الصراف الآلي	390
3.9.6. دفع المكافآت	392
10.6. معايير أمان رقم التعريف الشخصي	394
1.10.6. أجهزة إدخال أرقام التعريف الشخصية (PEDs) ولوحات تشفير أرقام التعريف الشخصية (EPPs)	396
2.10.6. إدخال رقم التعريف الشخصي المستند إلى البرامج باستخدام تطبيقات أرقام التعريف الشخصية وطريقة التحقق من البطاقة	398
3.10.6. التحقق من رقم التعريف الشخصي	400
4.10.6. تشفير رقم التعريف الشخصي	404
5.10.6. إدارة مفتاح رقم التعريف الشخصي	404
11.6. معايير أمن الطرفيات	406
1.11.6. معايير أمن الطرفيات الهجينة	406
2.11.6. معايير تشفير البيانات الثلاثي DES	406
الملحق رقم (1)	408
الملحق رقم (2)	410
الملحق رقم (3)	410
الملحق رقم (4)	411
الملحق رقم (5)	411
الملحق رقم (6)	413
الملحق رقم (7)	414
الملحق رقم (8)	414
الملحق رقم (9)	416
الملحق رقم (10)	416
الملحق رقم (11)	416
الملحق رقم (12)	416
الملحق رقم (13)	416
الملحق رقم (14)	418
الملحق رقم (15)	418
الملحق رقم (16)	418
الملحق رقم (17)	418
الملحق رقم (18)	418

Appendix number (19) 419

Appendix number (20) 421

Appendix number (21) 421

Appendix number (22) 421

Appendix number (23) 421

Appendix number (24) 421

Appendix number (25) 421

Appendix number (26) 423

Appendix number (27) 423

Appendix number (28).....423

Appendix number (29) 423

Appendix number (30) 423

Appendix number (31) 423

Appendix number (32) 423

Appendix number (33) 425

Appendix number (34) 425

Appendix number (35) 425

Appendix number (36) 425

Appendix number (37) 427

Appendix number (38) 427

Appendix number (39) 427

Appendix number (40) 427

Appendix number (41) 429

Appendix number (42) 429

Appendix number (43) 429

Appendix number (44) 429

Appendix number (45) 429

Appendix number (46) 431

Appendix number (47) 433

Appendix number (48) 433

Appendix number (49) 433

Appendix number (50) 435

Appendix number (51) 435

Appendix number (52) 435

الملحق رقم (19) 418

الملحق رقم (20) 420

الملحق رقم (21) 420

الملحق رقم (22) 420

الملحق رقم (23) 420

الملحق رقم (24) 420

الملحق رقم (25) 420

الملحق رقم (26) 422

الملحق رقم (27) 422

الملحق رقم (28) 422

الملحق رقم (29) 422

الملحق رقم (30) 422

الملحق رقم (31) 422

الملحق رقم (32) 422

الملحق رقم (33) 424

الملحق رقم (34) 424

الملحق رقم (35) 424

الملحق رقم (36) 424

الملحق رقم (37) 426

الملحق رقم (38) 426

الملحق رقم (39) 426

الملحق رقم (40) 426

الملحق رقم (41) 428

الملحق رقم (42) 428

الملحق رقم (43) 428

الملحق رقم (44) 428

الملحق رقم (45) 428

الملحق رقم (46) 430

الملحق رقم (47) 432

الملحق رقم (48) 432

الملحق رقم (49) 432

الملحق رقم (50) 434

الملحق رقم (51) 434

الملحق رقم (52) 434

Chapter 1 Rules and Regulations of Libyan National Payment Scheme

The National Scheme Operator represents the centralized system -under the supervision of CBL-that binds up and links all Member banks and other members lying under the umbrella of National Payment Scheme of Libya with the different parties that participate in a payment transaction.

The Central Bank of Libya have the full authority of delegation of any of the administrative, regulation and oversight to the National Scheme Operator or any other parties it deems eligible for such a role.

The National Scheme Operator, with its technical and human capabilities and competencies, performs the management and operations and sets the rules that are in line with the operating conditions as well as the controls required for the work of the national payment system.

In a manner that does not conflict with any of the controls and regulations established by the Central Bank of Libya and in line with the generally accepted terms, principles and rules of payment systems, the National Scheme Operator sets the necessary instructions and rules for the operation and management of the system, which represents an obligatory reference for all members participating in the system.

This book interprets and explains the different sections within the National Payment Scheme network systems, being classified with accordance to its' function the nature of tasks related to it.

1.1 The Purpose of this Document:

The established rules and conditions aim to lay the foundations for the operations related to the issuance and acceptance of cards as well as the different types of modern payment methods while they are available through the national payment system.

They represent the standard rules and terms of reference for banks participating in the national payment system, as well as the basics that must be adhered to by any bank wishing to join the system.

These rules and conditions operate within Libya in a manner that does not contravene or contradict any of the rules or conditions set by the Central Bank of Libya.

The National Scheme Operator is obligated to perform the necessary updates and to ensure that the operating instructions include the latest update while informing all participants in the system in a way that does not affect the nature of business and daily operations, bearing in mind that any technical modifications require changes in the nature of the technology used or operating applications, taking into account the time required to modify applications in line with the new system requirements.

الفصل 1 - القواعد التنظيمية لشبكة الدفع المحلية الليبية

يمثل مصرف ليبيا المركزي عن طريق مشغل شبكة الدفع المحلية؛ السلطة المركزية التي تنظم علاقته بجميع المصارف، وعلاقة المصارف فيما بينها المتمتعين بالعضوية في هذا النظام، وكذلك الأعضاء الآخرين المشاركون في شبكة الدفع المحلية.

ويملك مصرف ليبيا المركزي السلطة الكاملة في تفويض مشغل شبكة الدفع المحلية أو أي جهات أخرى في اتخاذ الإجراءات الإدارية والتنظيمية والرقابية، المتعلقة بهذا البرنامج.

يتولى مشغل شبكة الدفع المحلية، بما لديه من قدرات فنية وكفاءات بشرية، القيام بوظيفة الإدارة والتشغيل، ووضع القواعد والضوابط التي تتناسب مع ظروف التشغيل، والالتزام للعمل بشبكة الدفع المحلية، والتي تعد مرجعاً إلزامياً لجميع الأعضاء المشاركون في هذا النظام.

ويتقيد مشغل شبكة الدفع المحلية عند وضعه للقواعد والتعليمات المنظمة للتشغيل والإدارية بأن لا تتعارض مع الضوابط واللوائح التي يضعها مصرف ليبيا المركزي، وأن تتماشى مع الشروط والمبادئ والقواعد المقبولة عمومًا لأنظمة الدفع، والتي تعد مرجعاً ملزماً لأي عضو مشارك في نظام الدفع.

يعد هذا الكتاب دليلًا لتفسير وبيان الأقسام المختلفة داخل أنظمة شبكة الدفع المحلية، حيث يتم تصنيفها وفقًا لوظيفتها وطبيعة المهام المتعلقة بها.

1.1 الغرض من هذه الوثيقة:

هو بيان القواعد والشروط الموضوعية والتي تهدف إلى إرساء أسس العمليات المتعلقة بإصدار وقبول البطاقات، إضافة إلى مختلف أنواع طرق الدفع الحديثة أثناء تفعيلها من قبل مشغل شبكة الدفع المحلية.

كما تمثل هذه الوثيقة القواعد والمعايير التي تلتزم بها المصارف المشاركة في شبكة الدفع المحلية، وكذلك الأسس التي يجب على أي مصرف الالتزام بها عندما يرغب في الانضمام إلى شبكة الدفع المحلية.

هذه القواعد والمعايير والشروط تكون واجبة التطبيق داخل ليبيا، وبما لا يتعارض مع أي من القواعد أو الشروط التي يضعها مصرف ليبيا المركزي.

يلتزم مشغل شبكة الدفع المحلية بإدخال التحديثات اللازمة، والتي تضمن أن تعليمات التشغيل تتم وفقاً لها، وإعلام جميع الأعضاء المشاركين في النظام بأنها يجب ألا تؤثر على طبيعة الأعمال أو العمليات اليومية، أخذاً في الاعتبار أن إدخال هذه التحديثات الفنية تتطلب تغييرات في طبيعة ونوع التكنولوجيا المستخدمة أو تطبيقات التشغيل، وهو ما يستلزم منح المدة الكافية لتعديل التطبيقات بما يتوافق مع متطلبات النظام الجديد.

1.2 Terms and Definitions:

Term \Definition

The Acquirer: The licensed entity by the central bank to accept payments.

JAC (Joint Acquirer Center): Joint Acquirer Center.

Aggregated Transactions: Set of transactions been linked or segregated.

AID (Application ID): A unique Identification value represents the Scheme and exists on all its’ branded chip cards.

Applicable Data Protection Law: The applicable laws, rules, regulations, directives and governmental requirements in Libya relating in any way to the privacy, protection and security of Personal Data, as amended from time to time.

ATM: Automated Teller Machine.

BIN: Bank Identification Number.

CDCVM: Customer Device Cardholder Verification Method .

Clearing: The process of clearing transactions. between acquirers, payment scheme and issuers.

CNP: Card Not Present.

CVM: Cardholder Verification Method.

Data Subject: A Cardholder or Merchant or other natural person whose Personal Data is collected, used or disclosed by the National Scheme Operator or the Member.

e-Commerce: Electronic Commerce.

Floor Limit: Minimum limit to use for off-line transaction.

ICT: Instant Credit Transaction.

IIN (Issuer Identification Number): Usually presented by the first 6 or 8 digits of PAN.

Issuer: Meant to be Cards Issuing Entities.

KYC: Know Your Customer.

Member: A Licensed bank accredited by the National Payment Scheme to perform financial and payment services within National Payment network.

MCC: Merchant Category Code.

MPOS: Mobile Point of Sale.

PAN: Primary Account Number.

Participant: Party been sublicensed through a licensed member to perform payment services and other related transactions.

PCI DSS Payment Card Industry Data Security Standard.

Personal Data: Any information or opinion, whether true or not, about an identified individual or an individual who can be identified or is reasonably identifiable from that information or opinion.

2.1 المصطلحات والتعريفات:

المصطلحات/ التعريفات

القابل: الكيان المرخص له من قبل المصرف المركزي لقبول المدفوعات.

JAC (مركز القبول المشترك): مركز القبول المشترك.

المعاملات المجمعة: مجموعة المعاملات التي تم ربطها أو فصلها.

AID (معرف التطبيق): تمثل القيمة التعريفية الفريدة للشبكة والتي تكون موجودة في جميع بطاقات الشرائح ذات العلامات التجارية الخاصة به.

قانون حماية البيانات المعمول به: يشمل القوانين واللوائح والتوجيهات الحكومية المعمول بها في ليبيا والمتعلقة بأي شكل من أشكال حماية الخصوصية كالبيانات الشخصية وحمايتها وأمنها، بصيغتها المعدلة من وقت لآخر.

ATM: جهاز الصراف الآلي.

BIN: رقم التعريف المصرفي.

CDCVM: طريقة التحقق من هوية حامل بطاقة جهاز العميل.

التصفية: عملية تصفية المعاملات بين التاجر والمصرف.

CNP: البطاقة غير الموجودة.

CVM: طريقة التحقق من هوية حامل البطاقة.

موضوع البيانات: حامل البطاقة أو التاجر أو أي شخص طبيعي آخر يتم جمع بياناته الشخصية أو استخدامها أو الكشف عنها بواسطة مشغل شبكة الدفع المحلية أو العضو.

e-Commerce: التجارة الإلكترونية

الحد الأدنى: الحد الأدنى لاستخدام المعاملات خارج الإنترنت.

ICT: معاملة ائتمانية فورية

INN (رقم تعريف جهة الإصدار): يتم تقديمه عادةً بواسطة أول 6 أو 8 أرقام من رقم الحساب الأساسي.

جهة الإصدار: المصارف المصدرة للبطاقات.

KYC: تعرف على عميلك.

العضو: مصرف مرخص ومعتمد من قبل شبكة الدفع المحلية لأداء الخدمات المالية وخدمات الدفع.

MCC: رمز فئة التاجر.

MPOS: نقاط البيع المتنقلة.

PAN: رقم الحساب الأساسي.

المشارك: هو طرف تم الترخيص له من قبل عضو مرخص له لأداء خدمات الدفع والمعاملات الأخرى ذات الصلة.

PCI DSS: معايير صناعة بطاقات الدفع لأمن البيانات. البيانات الشخصية: أي معلومات أو رأي، سواء كان صحيحًا أم لا حول شخص محدد أو شخص يمكن تحديد هويته أو يمكن التعرف عليه بشكل معقول من تلك المعلومات أو الرأي.

PF (Payment Facilitator): It is a solvent company that:

Providing financial and technological services to sub-companies contracting with it on behalf of the bank for electronic collection, including, but not limited to:

- Establishing technology platforms for subsidiary companies with linking them to electronic collection services.
- Establishing intermediary systems that provide additional services to subsidiary companies, while linking them to electronic collection services.
- Providing the bank with the data of the subsidiary companies that will be collected.
- Contracting with companies on behalf of the bank to provide electronic collection services.
- Receiving financial settlements from the contracting bank on behalf of its listed companies.
- Carrying out financial settlements and providing the necessary technical support to the companies listed with it on behalf of the bank.
- Providing all the necessary reports for its listed companies regarding all the financial operations that were carried out through it.

PIN: Personal Identification Number.

POI: Point of Interaction.

POS: Point of Sale.

Processing of Personal Data: The carrying out of any operation or set of operations in relation to Personal Data, including recording, holding, organization, adaptation or alteration, retrieval, combination, transmission and erasure or destruction.

Profile: The set of rules which forms actions to be followed by the card and controls the card behavior across points of acceptance.

PSP: Payment Service Provider.

Settlement: The process of reconciliation between banks and it is considered the role of Central Bank. Tokenization: Replacement of card sensitive data as the card number, expiry date, the CVV – by a token representing such values which been kept in a tokenization vault.

TPP: Third Party Processor.

Transaction-related Personal Data: Personal Data required for authorizing, recording, settling and clearing a Transaction processed by the National Scheme Operator.

Sponsors: External parties out of payment ecosystem and join in with issuers or acquirers for promotional purposes as printing their logos or brands over cards and payment devices.

National Scheme Operator: The delegated Company/Organization/Authority from CBL to manage NPS in part or whole.

National Payment Council: The legislature that will adopt the rules and regulatory instructions and any future update on them.

PF (ميسر الدفع): شركة القائمة:

تقديم خدمات مالية وتكنولوجية للشركات الفرعية المتعاقدة معها نيابة عن المصرف للحصول الإلكتروني ، بما في ذلك على سبيل المثال لا الحصر:

- إنشاء منصات تقنية للشركات التابعة مع ربطها بخدمات التحصيل الإلكتروني.
- إنشاء أنظمة وسيطة تقدم خدمات إضافية للشركات التابعة مع ربطها بخدمات التحصيل الإلكتروني.
- تزويد المصرف ببيانات الشركات التابعة التي سيتم تحصيلها
- التعاقد مع شركات نيابة عن المصرف لتقديم خدمات التحصيل الإلكتروني.
- استلام التسويات المالية من المصرف المتعاقد نيابة عن شركائه المدرجة.
- إجراء التسويات المالية وتقديم الدعم الفني اللازم للشركات المقيدة لديه نيابة عن المصرف.
- تقديم كافة التقارير اللازمة لشركاتها المدرجة عن كافة العمليات المالية التي تمت من خلالها.

PIN: رقم التعريف الشخصي.

POI: نقطة التفاعل.

POS: نقطة البيع.

معالجة البيانات الشخصية: تنفيذ أي عملية أو مجموعة من العمليات المتعلقة بالبيانات الشخصية، بما في ذلك التسجيل، والاحتفاظ، والتنظيم، والتكيف أو التغيير، والاسترجاع، والجمع، والنقل، والمسح أو التدمير.

حساب تعريف: مجموعة القواعد التي تشكل الإجراءات التي يجب أن تتبعها البطاقة وتتحكم في سلوكها عبر نقاط القبول.

PSP: مقدم خدمة الدفع.

التسوية: عملية حل النزاع بين المصارف ويقوم بها مصرف ليبيا المركزي.

الترميز: استبدال البيانات الحساسة للبطاقة كرقم البطاقة ، وتاريخ انتهاء الصلاحية ، و CVV - عن طريق رمز مميز يمثل هذه القيم التي تم الاحتفاظ بها في قبو الترميز.

TPP: معالج طرف ثالث.

البيانات الشخصية ذات الصلة بالمعاملات: البيانات الشخصية المطلوبة للمصادقة و للتفويض والتسجيل والتسوية وتصفية المعاملات التي تمت معالجتها بواسطة مشغل شبكة الدفع المحلية.

الرعاة: هم الأطراف خارج النظام البيئي للدفع وانضمامهم إلى جهات الإصدار أو القابلين يكون لأغراض ترويجية مثل طباعة شعاراتهم أو علاماتهم التجارية على البطاقات وأجهزة الدفع.

مشغل شبكة الدفع المحلية: الشركة / المنظمة / السلطة المفوضة من مصرف ليبيا المركزي لإدارة شبكة الدفع المحلية NPS جزئياً أو كلياً.

مجلس الدفع المحلي: الهيئة التشريعية التي ستتبنى القواعد والتعليمات التنظيمية وأي تحديث مستقبلي لها.

National Payment System: The whole of the services that are associated with sending, receiving and processing orders of payment or transfers of money in domestic or foreign currencies, the issuance and management of payment instruments, payment, clearing and settlement systems, including those processing securities, arrangements and procedures associated with those systems and services, and payment service providers, including an operator of a system, participants, and any third party acting on behalf of them, either as an agent or by way of outsourcing agreements, whether operating entirely or partially. This process includes all the tools, systems, mechanisms, institutions, agreements, procedures, rules or laws.

1.3 Scope of Regulation Rules and Instructions:

The Regulation rules covers all the procedures and instructions that must be followed to implement the operations related to National payment Scheme, including the rules for the functions related to those operations, within the framework of the governing laws and established as general frameworks by the Central Bank of Libya.

These rules and controls are the minimum threshold for all participants in the national payment system, and all banks must ensure that all necessary measures are taken towards managing the risks associated with providing all necessary for the management of banking payment services, and these rules are also applicable without prejudice to the controls of operations may previously issued by the Central Bank of Libya, as well as instructions and rules for the implementation of banking operations.

The National Scheme Operator is responsible for supervising the implementation of the aforementioned instructions, as well as making the necessary updates in a timely manner, and taking the necessary measures to ensure how they are implemented while setting determinants and standards in case of violations and non-compliance.

1.4 Supervisory Power:

- (1) CBL has a general right for supervision and that
- (2) In discrete high-level rules set forth the national scheme operator (NSO) has the right to supervise the conditions for membership on the national scheme (NS)

1.5 National Scheme Operator and other Entities Role:

The National Scheme Operator represents the body entrusted with setting procedures, instructions and rules of compliance in light of the role assigned to it by the Central Bank of Libya.

All banks and participating entities in the national payment system in the state of Libya must follow the established rules and instructions and review the national distributor in any development that might affect the payment operations that the national distributor manages or passes through the local network.

The role of the National Scheme Operator is not limited to setting instructions and monitoring the implementation only, but the role of the national distributor extends to setting the technical details as well as choosing the technical methods compatible with implementation and compatible with the national network.

شبكة الدفع المحلية: جميع الخدمات المرتبطة بإرسال واستلام ومعالجة أوامر الدفع أو تحويل الأموال بالعملة المحلية أو الأجنبية، وإصدار وإدارة أدوات الدفع، وأنظمة الدفع والمقاصة والتسوية، بما في ذلك تلك المتعلقة بمعالجة الأوراق المالية والترتيبات والإجراءات المرتبطة بتلك الأنظمة والخدمات، ومقدمي خدمات الدفع، بما في ذلك مشغل النظام، والمشاركين، وأي طرف ثالث يتصرف نيابة عنهم، إما كوكيل أو عن طريق اتفاقيات الاستعانة بمصادر خارجية، سواء كانت تعمل كليًا أو جزئيًا. تشمل هذه العملية جميع الأدوات والأنظمة والآليات والمؤسسات والاتفاقيات والإجراءات والقواعد أو القوانين.

3.1 مجال اختصاص القواعد التنظيمية والتعليمات:

تنطبق قواعد هذه اللائحة على جميع الإجراءات والتعليمات التي يجب اتباعها لتنفيذ العمليات المتعلقة بشبكة الدفع المحلية، بما في ذلك القواعد الخاصة بالوظائف المتعلقة بتلك العمليات، في إطار اللوائح والمعايير المنظمة لها من قبل مصرف ليبيا المركزي.

تمثل هذه القواعد الحد الأدنى الذي يجب على جميع المشاركين في شبكة الدفع المحلية الالتزام بها، ويجب على جميع المصارف التحقق من اتخاذ جميع التدابير اللازمة لإدارة المخاطر المرتبطة بتوفير كل ما يلزم لإدارة خدمات الدفع المصرفية، وتكون هذه القواعد واجبة التطبيق، وذلك دون الإخلال بالقواعد الخاصة والمعايير المتعلقة بتنفيذ العمليات المصرفية والتي سبق وأن أصدرها مصرف ليبيا المركزي، بالإضافة إلى التعليمات والقواعد المتعلقة بتنفيذ العمليات البنكية.

يتحمل مشغل شبكة الدفع المحلية مسؤولية الإشراف على تنفيذ التعليمات المذكورة أعلاه، بالإضافة إلى إدخال التحديثات اللازمة على التكنولوجيا المستخدمة في الوقت المناسب واتخاذ الإجراءات اللازمة لضمان كيفية تنفيذها ووضع المحددات والمعايير في حالة حدوث انتهاكات وغير أمثال.

4.1 السلطة الإشرافية:

- (1) مصرف ليبيا المركزي له حق عام في الإشراف.
- (2) في القواعد المنفصلة رفيعة المستوى المحددة يحق لمشغل شبكة الدفع المحلية (NSO) الإشراف على شروط العضوية في الشبكة المحلية (NS)

5.1 اختصاصات مشغل شبكة الدفع المحلية والاعضاء الأخرى:

مشغل شبكة الدفع المحلية هي الجهة المخولة بوضع القواعد والإجراءات ومعايير الامتثال بعد تفويضه على ضوء الدور المناط به من قبل مصرف ليبيا المركزي.

يجب على جميع المصارف والاعضاء المشاركون في شبكة الدفع المحلية بدولة ليبيا اتباع القواعد والمعايير المعمول بها، ومراجعة مشغل شبكة الدفع المحلية في إدخال أي تطوير من شأنه أن يؤثر على عمليات الدفع التي يديرها مشغل شبكة الدفع المحلية أو يمر عبر الشبكة المحلية.

لا يقتصر اختصاص مشغل شبكة الدفع المحلية على وضع القواعد والمعايير، والإشراف على تنفيذها، بل يشمل اختصاص مشغل شبكة الدفع المحلية وضع وتحديد التفاصيل والأساليب الفنية وكذلك اختيار الطرق الفنية المتوافقة مع عمليات التنفيذ داخل الشبكة المحلية.

Among the duties and powers of the National Distributor is to set the necessary frameworks for managing the system, as well as laying the foundations and applications, and choosing the appropriate means of application and different technological systems, in the event of multiple means or methods of application.

1.6 Methodology Followed for Rules and Regulations:

When setting the rules and standards, consideration was given to providing the elements of integration and reliability on instruction books, and categorized them according to the nature of each of the activities of the integrated payments process.

Classification was done on a functional basis so that each book can be used by specialized elements within the organizational structure of the banks and to facilitate the implementation process and reference use for each activity specialist separately.

The Rules and Regulations of The Libyan National Payment Scheme included the rules and standards for implementation in relation to the following basic operations and functions:

Book 1 Organization Principals

- Chapter 1.1: General Rules & Regulations
- Chapter 1.2: Members Compliance
- Chapter 1.3: Issuing
- Chapter 1.4: Payments Acceptance
- Chapter 1.5: Authorization – Clearing & Settlement Management
- Chapter 1.6: Fraud & Risk Management

Book 2 Technical Legal Standards

- Chapter 2.1: Membership
- Chapter 2.2: NUMO Brand Usage
- Chapter 2.3: NUMO Products Guide

Book 3 Technical Operational Standards

- Chapter 3.1: Card Specifications, Terms And Designing Standards
- Chapter 3.2: Chargeback Rules
- Chapter 3.3: Interchange and Pricing
- Chapter 3.4: eCommerce & Digital Services

1.7 Discrepancies:

Document should not present any discrepancies or contradictions in the presence of rules and instructions during the application process, but some participants may request the existence of some exceptions to be compatible with the existing systems and the work in progress, which would cause some discrepancies from what is presented.

يختص مشغل شبكة الدفع المحلية بوضع اللائحة الإدارية لإدارة شبكة الدفع المحلية، وكذلك وضع الأسس والتطبيقات، واختيار وسائل التطبيقات المناسبة والأنظمة التكنولوجية المختلفة، في حالة تعدد هذه التطبيقات وتلك الأنظمة.

6.1 المنهجية المتبعة في إصدار القواعد واللوائح:

عند وضع القواعد والمعايير المنظمة لشبكة الدفع المحلية، يجب أن تكون هذه القواعد والمعايير متكاملة ومتوافقة مع دليل التعليمات، وأن يتم تصنيفها حسب طبيعة كل نشاط من عمليات المدفوعات المتكاملة.

يجب أن يتم تصنيف القواعد والمعايير على أساس وظيفي، بحيث يمكن تسهيل استخدام كل كتاب بواسطة عناصر متخصصة ضمن الهيكل التنظيمي للمصارف وتسهيل القيام بعملية التنفيذ والاستخدام المرجعي لكل نشاط متخصص على حدى.

تتضمن قواعد ولوائح شبكة الدفع المحلية الليبية قواعد ومعايير التنفيذ فيما يتعلق بالعمليات والوظائف الأساسية التالية:

كتاب 1: مبادئ المنظمة

- الفصل 1.1: القواعد واللوائح العامة.
- الفصل 2.1: امتثال الأعضاء
- الفصل 3.1: الإصدار
- الفصل 4.1: قبول المدفوعات
- الفصل 5.1: التفويض - إدارة المقاصة والتسوية
- الفصل 6.1: إدارة الاحتيال والمخاطر

الكتاب 2: المعايير القانونية الفنية

- الفصل 1.2: العضوية
- الفصل 2.2: استخدام علامة نموالتجارية
- الفصل 3.2: دليل منتجات نمو

الكتاب 3: معايير التشغيل الفنية

- الفصل 1.3: مواصفات البطاقة وشروطها ومعايير التصميم
- الفصل 2.3: قواعد رد المبالغ المدفوعة
- الفصل 3.3: التبادل والتسعير
- الفصل 4.3: التجارة الإلكترونية والخدمات الرقمية

7.1 التناقضات:

يجب ألا يحتوي المستند على أي تناقض أو تعارض مع القواعد والمعايير أثناء عملية التقديم، وإذا طلب أحد المشاركين وجود بعض الاستثناءات لتكون متوافقة مع الأنظمة القائمة والعمل الجاري، مما قد يتسبب في حدوث التعارض مع القواعد والمعايير الحالية. في مثل هذه الحالات، يمكن تقديم طلب للحصول على موافقة على هذه الاستثناءات، وبطريقة لا

In such cases, a petition can be submitted for the purpose of obtaining approval to implement these exceptions in a manner that does not contradict or require any additional technical or administrative efforts that need special care from the national distributor and that does not cause major differences that would disrupt or stop payment services.

And each of the participants must ensure compliance with the rules and conditions set by the national distributor and use them as a reference for the application and ensure that the national distributor is notified of the conflict in the application, if any.

1.8 Membership & Types of Membership:

All banks operating in Libya that are licensed by the Central Bank of Libya automatically acquire the right to membership in the National Payments System, and other parties eligible to be participants may take the procedures of applying to become a member. No entity may participate in the activity until this entity is approved to be a member, and it has obtained the applicable licenses for the proposed activity in a form acceptable to the national distributor, and has paid all fees and other related costs.

1.8.1 Members and Participants Obligations:

At All times, each member must:

1. be fully responsible for all aspects of its activities including its digital activities that it controls and have the ability to establish and enforce all management policies and implement operating terms and instructions on all of its payment transaction activities, and in accordance with the Standards;
2. Not to transfer or waive some or all liability, delegate control or limit responsibilities in any way;
3. Ensure that all policies applicable to its financial and digital activities comply with the Standards and comply with all applicable governmental laws and regulations, including AMLCFT law and relevant regulations;
4. Carry out purposeful and continuous monitoring to ensure compliance with all responsibilities stipulated in this rule, and to be able to demonstrate such monitoring and compliance at the request of the national distributor operator in accordance with the Standards;
5. Ensure that both subcontractors and employees comply with all anti-bribery and anti-corruption laws applicable to commercial transactions and any implementing regulations in relation to any such laws. The Member shall not, in connection with its business activities in connection with the Payment System Operator: (1) make, promise or offer to make any payment or transfer of anything of value or any other privilege directly or indirectly through a representative, intermediary or agent, or in any manner other to any government official or other person for the purpose of improperly influencing any act or inaction or decision of such official or individual or securing improper privileges to assist the Member and/or the National Distributor Operator in acquiring or retaining business; (2) It shall not accept anything of value from any third party seeking to influence any action or decision of the Member or to secure inappropriate privileges for that third party; or (3) A politically exposed person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is or has been entrusted with a prominent public function

تتعارض أو تتطلب أي جهود فنية أو إدارية إضافية، أو تحتاج إلى عناية خاصة من مشغل شبكة الدفع المحلية، ولا تسبب اختلافات كبيرة من شأنها أن تعطل أو توقف خدمات الدفع. ويجب على كل مشارك (عضو) التحقق من الامتثال للقواعد والمعايير التي يضعها مشغل شبكة الدفع المحلية، واستخدامها في التطبيق العملي، والتحقق من إخطار مشغل شبكة الدفع المحلية بالتعارض في الممارسة العملية، إن وجد.

8.1 العضوية وأنواعها:

تتصل جميع المصارف العاملة في ليبيا، والمرخص لها من قبل مصرف ليبيا المركزي بطريقة تلقائية على حق العضوية في نظام شبكة الدفع المحلية، ويجوز للأطراف الآخرين والمؤهلين للعضوية في هذا النظام اتخاذ إجراءات تقديم الحصول على العضوية. لا يجوز لأي طرف المشاركة في هذا النظام إلا بعد دفع جميع الرسوم والتكاليف الأخرى المطلوبة، والحصول على الموافقة المكتوبة بقبول عضويته، والترخيص المعمول بها للدخول في هذا النظام من قبل مشغل شبكة الدفع المحلية.

1.8.1 التزامات الأعضاء والمشاركين:

يجب على كل عضو الالتزام بالآتي:

- (1) أن يكون مسؤولاً ومسؤولية كاملة على جميع جوانب أنشطته؛ بما في ذلك أنشطته الرقمية التي يديرها، والتي يملك القدرة على تنفيذ شروط وتعليمات التشغيل على جميع أنشطة معاملات الدفع الخاصة به، ووفقاً للمعايير المعمول بها.
- (2) عدم الاتفاق على تحويل المسؤولية، أو الإعفاء منها و جزء منها أو تفويض السيطرة وتحديد المسؤوليات.
- (3) التحقق من أن جميع السياسات المطبقة على أنشطته المالية والرقمية تتوافق مع القواعد والمعايير الموضوعة من قبل مشغل شبكة الدفع المحلية، أو مصرف ليبيا المركزي، ومع جميع القوانين واللوائح المعمول بها، بما في ذلك قانون مكافحة غسل الأموال / مكافحة تمويل الإرهاب واللوائح ذات الصلة؛
- (4) طبقاً للقواعد والمعايير المعمول بها يجب إجراء مراقبة هادفة ومستمرة لضمان الامتثال لجميع المسؤوليات المنصوص عليها، ولا يجوز القيام بهذه المراقبة ألا بناءً على طلب مشغل شبكة الدفع المحلية وفقاً للمعايير.
- (5) التحقق من أن كلا من العاملين والمقاولين من الباطن يمثلون لجميع القوانين واللوائح التنفيذية المجرمة للرشوة والفساد المتعلقة بالمعاملات التجارية. فيما يتعلق بتنفيذ أنشطته، لا يجوز للعضو القيام بالأعمال التالية: (1) إجراء أي دفعة أو نقل أي شيء ذي قيمة أو أي امتياز آخر أو الوعد به أو عرضه بشكل مباشر أو غير مباشر من خلال ممثل أو وسيط أو وكيل ، أو بأي طريقة أخرى إلى أي مسؤول حكومي أو أي شخص آخر بغرض التأثير بشكل غير لائق على أي عمل أو عدم اتخاذ أي إجراء أو قرار من هذا المسؤول أو الفرد أو تأمين امتيازات غير لائقة لمساعدة العضو و / أو مشغل الموزع الوطني في قبول الأعمال أو الاحتفاظ بها، (2) قبول أي شيء ذي قيمة من الغير، من أجل التأثير على أي إجراء أو قرار للعضو أو لتأمين امتيازات غير قانونية لذلك الغير.(3) يتم تعريف الشخص البارز سياسياً(PEP) من قبل فريق العمل المالي (FATF)على أنه شخص بارز أو تم تكليفه بوظيفة عامة بارزة.

6. Outsourced services rules are covered by the announced and released circulars been released by CBL. For the purposes of this rule, a “government official” is defined as any employee or official of the Government of Libya or a subdivision thereof, including any federal, provincial or local government, department, agency, or agency, or corporation owned or controlled by such government; any official of a political party; and any official or employee of a public enterprise; It also includes any person acting in an official capacity for or on behalf of such entities; Any candidate for political office.

1.8.2 Classification of the Participants:

There are two types of participants with the national distributor:

The first is the main participants and holders of a license from the Central Bank of Libya to practice banking activity within the State of Libya and to deal with the public and the eligibility to issue or accept cards. The second is the participating parties by delegating financial or derivative powers and under one of the banks that have obtained a license to engage in banking activity.

1.8.3 Participants Management

The National Scheme Operator shall, in accordance with its powers, undertake the management of participants, set standards and administrative and technical bases for operation, and how to carry out issuance and acceptance processes, as well as in the event of any activity of issuance or acceptance on behalf of the participant and in accordance with the licenses obtained from the Central Bank of Libya.

Under no circumstances may the license or the powers granted to one of the participants be transferred, transferred or transferred to another party without referring to the national distributor before starting these procedures.

1.8.4 Procedures for obtaining licenses

Banking license must first be obtained through the Central Bank of Libya for working within the Libyan territory, followed by signing an agreement with the National Scheme Operator and specifying the role and activity required to be performed.

1.8.5 Service Provision Contract / Service Request Form

Each participant tends to join as a member of the national payments network must sign a service provision contract before the system of the network is linked to the national distributor and the systems of the person wishing to participate.

The subscriber is obligated to carry out all the necessary technical work to connect and comply with the network system, which is managed by the national distributor, and to agree to the terms of the contractual conditions mentioned in the agreement.

The service provision contract governs the relationship between the national distributor and all participants who are subject to the standards, rules and conditions of operation set for the services of the national network.

1.9 Relevant Parties

The relevant parties are defined for the nature of their role in making the payments process and according to what is authorized by the Central Bank of Libya for their respective roles,

6) قواعد خدمات التعهد تنظمها التعميمات المعلنة والصادرة عن مصرف ليبيا المركزي. لأغراض هذه القاعدة ، يُعرّف “المسؤول الحكومي” بأنه أي موظف أو مسؤول في الحكومة الليبية أو أحد الجهات التابعة لها، بما في ذلك الحكومة المركزية أو الحكومة المحلية التابعة لها، إدارة أو وكالة أو شركة تملكها أو تسيطر عليها هذه الحكومة؛ أي مسؤول في حزب سياسي ؛ وأي مسؤول أو موظف في مؤسسة عامة؛ ويشمل أيضًا أي شخص يتصرف بصفة رسمية لصالح هذه الكيانات أو بالنيابة عنها ؛ أي مرشح لمنصب سياسي.

2.8.1 تصنيف المشاركين:

هناك نوعان من الاعضاء المشاركين مع مشغل شبكة الدفع المحلية:

النوع الأول: هم الاعضاء الرئيسيون: وهم الذين تم منحهم ترخيص من قبل مصرف ليبيا المركزي لممارسة النشاط المصرفي للتعامل مع الجمهور وإصدار البطاقات وقبولها داخل الدولة الليبية. النوع الثاني: الاعضاء المشاركون وهم: الذين تم منحهم تفويض الصلاحيات المالية، من أحد المصارف الحاصلة على ترخيص لمزاولة العمل المصرفي في ليبيا.

3.8.1 إدارة الاعضاء المشاركين

يتولى مشغل شبكة الدفع المحلية، طبقاً لاختصاصاته، إدارة الاعضاء المشاركين في هذا النظام، ووضع المعايير والأسس الإدارية والفنية اللازمة للتشغيل، وكيفية تنفيذ عمليات الإصدار والقبول ووفقاً للتراخيص الممنوحة من مصرف ليبيا المركزي.

في جميع الاحوال لا يجوز نقل الترخيص أو الاختصاصات الممنوحة لأحد الاعضاء المشتركين إلى طرف آخر بدون الرجوع إلي المشغل الوطني قبل البدء في هذه الإجراءات.

4.8.1 إجراءات الحصول على التراخيص

يجب الحصول أولاً على ترخيص ممارسة العمل المصرفي من قبل مصرف ليبيا المركزي للعمل داخل إقليم الدولة الليبية، ثم توقيع اتفاقية مع مشغل شبكة الدفع المحلية، وتحديد الدور والنشاط المطلوب أدائه.

5.8.1 عقد تقديم الخدمة/ نموذج طلب الخدمة

كل مشارك يرغب في الانضمام كعضو في شبكة الدفع المحلية، يجب عليه التوقيع على عقد تقديم الخدمة قبل ربط نظام الشبكة بين مشغل شبكة الدفع المحلية و أنظمة الشخص الراغب في العضوية.

يلتزم كل عضو مشارك بتنفيذ جميع الأعمال الفنية اللازمة للتوصيل بنظام الشبكة الذي يديره مشغل شبكة الدفع المحلية والامتثال لها ، والموافقة على الشروط التعاقدية المذكورة في العقد.

عقد تقديم الخدمة هو الذي ينظم العلاقة بين مشغل شبكة الدفع المحلية، وجميع المشاركين الخاضعين لقواعد ومعايير وشروط التشغيل المحددة لخدمات الشبكة المحلية.

9.1 الأطراف المعنية

يتم تحديد الأطراف المعنية بنظام المدفوعات، عن طريق مصرف ليبيا المركزي، وهو الذي يحدد طبيعة دورها في إجراء عملية المدفوعات، وتطبق هذه القاعدة على مقدمي خدمات الدفع ((PSP المفوضة صلاحياتهم من قبل المصارف الدائنة والمصارف التي لديها تفويض وموافقة مسبقة من مصرف ليبيا المركزي.

and this applies to PSP (Payment Service Providers) with their delegated powers by the payable banks with prior notification and approval of a bank Central Libya.

The same applies to PF Payment Facilitators. Independent PSP may exist, subject to licensing of CBL, and that they must comply with all the provisions of the rule books. A specific guarantee should be included on the insurance (cash deposit or letter of guarantee) that they must have.

1.9.1 Roles and Responsibilities of the Relevant Parties

All the issued rules and instructions must be adhered to by all parties participating in the payments system based on the operation of the national distributor, and it becomes binding on all relevant parties, and those in charge of contracting with these parties must ensure implementation and are considered obligated to do so before The National Scheme Operator.

1.9.2 Obligations of the Relevant Parties

The relevant parties shall abide by all the rules and instructions related to securing the payments process and maintaining the confidentiality of data and information related to customers and users in accordance with the CBL circular on licensing. It would be exposed to risks specific to the payments process, and compliance with the security and data protection standards in the card and electronic payment Card industry PCI Standards must be reviewed.

Under the circular fore set in this regard by the CBL, the directors and the persons responsible for the management of the payment institution must be of good repute and possess appropriate knowledge and experience to perform payment services, regardless of the institution's size, internal organization and the nature, scope and complexity of its activities and the duties and responsibilities of the specific position.

1.9.3 Termination of Relevant Parties

Transactions with related parties are terminated in one of two ways:

The first is voluntarily based on the desire to liquidate, end of business, or any other reasons. In this case, the contracting authority must be notified of the practice of the activity 90 days before the desire to do so, in order to make appropriate precautions for settlements and any process that may involve any of the disputes related to transactions through clients with Ensure that the national distributor is informed as soon as he becomes aware of the relevant party's desire to do so.

The second occurs forcibly through the National Scheme Operator -under delegated rights from CBL- as a result of bypassing or performing an act that contradicts the rules of the agreement to perform the service or breach the terms of the contract, and the implementation is carried out immediately with notifications to the national distributor as soon as the decision is made to stop the transactions and accept the payments through the relevant party while taking the necessary financial precautions to secure any of the settlement operations. This party shall not be released until after all settlements and pending clearing operations have been implemented.

قد يوجد PSP مستقلين ، يخضعوا لترخيص من مصرف ليبيا المركزي، ويجب أن يلتزموا بجميع القواعد المنصوص عليها في كتاب القواعد. كما يجب تقديم ضمان محدد في التأمين (إيداع نقدي أو خطاب الضمان) الذي يجب أن يكون لديهم.

1.9.1 أدوار ومسؤوليات الأطراف المعنية

يجب التزام جميع الأطراف المعنية المشاركة في نظام المدفوعات بالقواعد والتعليمات الصادرة من مشغل شبكة الدفع المحلية، والتي تكون ملزمة أيضاً لجميع الأطراف ذات الصلة، ويجب على المسؤولين عن التعاقد مع هذه الأطراف، التحقق من تنفيذها.

2.9.1 التزامات الأطراف المعنية

تلتزم الأطراف المعنية بجميع القواعد والتعليمات المتعلقة بتأمين عملية المدفوعات، والحفاظ على سرية البيانات والمعلومات المتعلقة بالعملاء والمستخدمين وفقاً لتعميم مصرف ليبيا المركزي بشأن الترخيص. ستتعرض لمخاطر خاصة بعملية المدفوعات ، ويجب مراجعة الامتثال لمعايير الأمان وحماية البيانات في معايير PCI الخاصة بصناعة البطاقات وبطاقات الدفع الإلكترونية.

بموجب التعميم المقدم من قبل مصرف ليبيا المركزي، يجب أن يتمتع المديرون، والأشخاص المسؤولون عن إدارة مؤسسة الدفع، بسيرة حسنة، وأن تكون لديهم المعرفة والخبرة المهنية لتقديم خدمات الدفع، وذلك بصرف النظر عن حجم المؤسسة وتنظيمها الداخلي، وطبيعة ونطاق أنشطتها، وواجبات ومسؤوليات الوظيفة المحددة.

3.9.1 إنهاء الأطراف المعنية

يتم إنهاء المعاملات مع الأطراف المعنية بإحدى طريقتين:

الأولى: أن يقوم باختياره بالإعلان عن رغبته في تصفية نشاطه أو إنهاء العمل أو أي طريقة أخرى. وفي هذه الحالة ، يجب تقديم إخطار إلى الجهة المتعاقدة قبل 90 يومًا من تاريخ إعلان هذه الرغبة في إنهاء النشاط، وذلك من أجل اتخاذ التدابير المناسبة لإجراءات التسويات، وتفادي حدوث منازعات مع العملاء حول معاملاتهم. مع الالتزام بأن يتم إخطار مشغل شبكة الدفع المحلية بذلك حال معرفة رغبة الطرف المعني.

الثانية: فسخ التعاقد بالقوة من خلال السلطة التقديرية مشغل شبكة الدفع المحلية - بموجب الحقوق المفوضة من مصرف ليبيا المركزي - بسبب تجاوزاته أو إخلاله بالتزاماته التعاقدية أو خرق لبنود العقد. ويجب إخطار مشغل شبكة الدفع المحلية بمجرد اتخاذ قرار الفسخ لوقف العمليات وقبول المدفوعات من الطرف المعني مع اتخاذ التدابير المالية اللازمة لتأمين عمليات التسوية، ويجب عدم أعفاء هذا الطرف من التزاماته إلا بعد إجراء كل التسويات، وتنفيذ عمليات المقاصة المعلقة.

1.10 Intellectual Property and Ownership

1.10.1 Ownership and Privacy of the Rules and Regulations

The Central Bank of Libya retains all Intellectual property and privacy rights for all instructions and rules issued and related to National Payment Scheme and all relevant operating rules and publishing it, in addition it is considered the single entity that has the right to delegate or to authorize any other entity to apply any amendments or additions to these instructions.

1.10.2 Right to Manage and to Operate the National Scheme Operator

The National Scheme Operator Under his delegated authority through the Central Bank of Libya, and within its' accordance the National Scheme Operator retains the rights to take the role of managing and operating the system as well as carry out the operations entrusted to it according to the authorization granted to it by the Central Bank of Libya.

1.11 The Use and Implementation of Rules and Regulations.

1.11.1 Products Management

The National Scheme Operator is the only authorized entity through the Central Bank of Libya to manage and operate the Scheme systems as well as products related to National Payment Scheme within the Libyan territory.

1.11.2 Rules of Co-badging

Under certain limitations, an issuer may request to be licensed for co-badging with international networks from CBL and it must be under the following rules:

1. The requested co-badging must be chip-based product within the known EMVco, approved and published Kernels.
2. The National Scheme application will be the primary application and will always have the priority in acceptance within Libya at all points of acceptance.
3. The used BIN range shall be accepted domestically and a routing mandate for transactions within the country will be solely managed by the National Scheme operator and all the regulations and rules published by CBL shall be applied for domestic based transactions, only for the usage outside Libya the co-badged ICS rules shall be applied.
4. Card profile provided for co-badged product must be arranged with the National Scheme Operator in order to get the required profile that will be personalized.
5. The Issuer must ensure that the sublicensed kernel for co-badging is applicable for acceptance across all points of acceptance within the country.
6. Issuer banks must obtain the right to sublicense the provided kernel technology for NUMO profile designing to keep the international and local profile consistency for smooth acceptance.
7. During the card design process, the Issuer bank must ensure that NUMO logo is within the design of the plastic card and displacement is done with accordance to card design and specifications published by the Central Bank of Libya.
8. National Scheme Operator must conduct the required PVT (Personalization Validation Test) similar to the ICS using a personalized test card prior rolling out and printing cards for Issuer customers.

10.1 حقوق الملكية الفكرية:

1.10.1 ملكية وخصوصية القواعد واللوائح:

يتمتع مصرف ليبيا المركزي بكافة حقوق الملكية الفكرية على جميع القواعد والمعايير والتعليمات الصادرة والمتعلقة بشبكة الدفع المحلية، بالإضافة إلى أنه يعتبر السلطة الوحيدة التي تملك الحق في تفويض أي جهة أخرى لإجراء أي تعديلات أو إضافات على تلك التعليمات.

2.10.1 الحق في إدارة وتشغيل مشغل شبكة الدفع المحلية:

يختص مشغل شبكة الدفع المحلية وفي حدود التفويض الممنوح له من مصرف ليبيا المركزي ، بإدارة وتشغيل نظام المدفوعات، وإضافة إلى تنفيذ العمليات الموكلة إليه وفقاً للتفويض الممنوح لها من مصرف ليبيا المركزي.

11.1 استخدام وتطبيق القواعد واللوائح

1.11.1 إدارة المنتجات

يعد مشغل شبكة الدفع المحلية هو الجهة المرخص لها من مصرف ليبيا المركزي، لإدارة وتشغيل أنظمة الشبكة، بالإضافة إلى إدارة المنتجات المتعلقة بشبكة الدفع المحلية داخل الأراضي الليبية.

2.11.1 قواعد العلامة التجارية المشتركة

في ظل قيود معينة، قد تطلب جهة الإصدار الحصول على ترخيص من مصرف ليبيا المركزي من أجل المشاركة مع شبكات دولية ويجب أن يخضع ذلك للقواعد التالية:

- (1) يجب أن يكون العلامة التجارية المشتركة المطلوبة منتجاً يعتمد على شريحة ضمن EMVco المعروفة والمعتمدة والمنشورة.
- (2) سيكون تطبيق الشبكة المحلية هو التطبيق الأساسي وسيكون له الأولوية دائماً في القبول داخل ليبيا في جميع نقاط القبول.
- (3) يتم قبول نطاق BIN المستخدم محلياً وسيتم إدارة تفويض التوجيه للمعاملات داخل ليبيا فقط بواسطة مشغل شبكة الدفع المحلية وسيتم تطبيق جميع اللوائح والقواعد التي ينشرها مصرف ليبيا على المعاملات المحلية، فقط عند الاستخدام خارج ليبيا يجب تطبيق قواعد ICS ذات الشارة المشتركة.
- (4) يجب ترتيب ملف تعريف البطاقة المقدم للمنتج الذي يحمل شارة مشتركة مع مشغل شبكة الدفع المحلية من أجل الحصول على الملف الشخصي المطلوب الذي سيتم تخصيصه.
- (5) يجب على جهة الإصدار التأكد من أن النواة kernel المرخصة من الباطن للعلامة المشتركة قابلة للقبول عبر جميع نقاط القبول داخل الدولة.
- (6) يجب أن تحصل مصارف جهة الإصدار على الحق في ترخيص تقنية النواة kernel المقدمة من الباطن لتصميم ملف تعريف (نمو) للحفاظ على اتساق الملف الشخصي الدولي والمحلي من أجل القبول السلس.
- (7) أثناء عملية تصميم البطاقة ، يجب على مصرف جهة الإصدار التأكد من أن شعار (نمو) ضمن تصميم البطاقة البلاستيكية وأن الإزاحة تتم وفقاً لتصميم البطاقة والمواصفات التي ينشرها مصرف ليبيا المركزي.
- (8) يجب على مشغل شبكة الدفع المحلية إجراء PVT (اختبار التحقق من التخصيص) المطلوب على غرار اختبار ICS باستخدام بطاقة اختبار شخصية قبل طرح البطاقات وطباعتها لعملاء جهة الإصدار.

1.11.3 Rules of Brand Usage

The right to use the Brand of the National Scheme/Network is granted only under a written permission from the National Scheme Operator. The National Scheme Operator logos must not be used in any way or form prior to a permission granted by the respective owner (CBL or National Payment Scheme/ Network Operator).

No additional interest or return is given for the right to use the National Scheme/Network logo. The Licensee is also responsible for all costs and obligations arising out of or related to its use of the National Payments Network's logo.

The license is non-exclusive and non-transferable. Licensee permits sublicense of the right to use the National Payment Scheme Mark to any Sublicense only in accordance with the Standards or with the express written consent of the Payment System Operator. A Member or other licensee who is permitted to license the use of the National Payments Scheme Mark to a sublicensee shall ensure, as long as the sub-license is in effect, that the National Payment Scheme Mark is used by the Sublicensee in accordance with the Standards. and/or other additional terms of such use required by the payment system operator.

The right to use the National Payments Mark may not be sublicensed or assigned, whether by sale, merger, merger, acquisition, law enforcement or otherwise, without the prior written consent of the payment system operator.

The national scheme operator does not make any representations or warranties, express or implied, regarding the national payment network logo (its role is limited to carrying out the management and operation process) and the payment system operator does not specifically hold the payment system operator accountable for any of these representations and guarantees, if any.

1.11.4 Rules for clearing, settlement and acceptance of electronic transactions

Not within the scope of the instructions mentioned here and it is referenced to what was previously set by the Central Bank of Libya, being the party responsible for clearing operations.

1.11.5 Pricing and Interchange Rules

Refer to book 3 Chapter 3 in this set of regulations.

1.12 Fraud & Risk Management

The Central Bank of Libya sets a set of rules and conditions that must be available for monitoring, follow-up, avoiding financial risks, and monitoring any attempts that would discredit financial transactions. Participating banks are responsible for protecting their customers and compensating them in case of breach of any of these functions.

Further is detailed in Chapter 6 of this book.

3.11.1 قواعد استخدام العلامة التجارية

يُمنح الحق في استخدام العلامة التجارية لشبكة الدفع المحلية، بموجب ترخيص من مشغل شبكة الدفع المحلية. لا يجوز استخدام شعار مشغل شبكة الدفع المحلية بأي شكل من الأشكال قبل منح الترخيص من قبل المالك المعني (مصرف ليبيا المركزي أو مشغل شبكة الدفع المحلية).

لا يجوز منح فائدة أو أي عائد إضافي كان، مقابل الحق في استخدام شعار الشبكة المحلية. يتحمل المرخص له المسؤولية عن جميع التكاليف والالتزامات المتعلقة باستخدامه لشعار شبكة الدفع المحلية.

التراخيص غير حصرية وغير قابلة للتنازل عنها، ولكن يجوز للمرخص له الترخيص من الباطن لمنح الحق في استخدام علامة شبكة الدفع المحلية لأي مرخص له من الباطن طبقاً للقواعد والمعايير المعمول بها، وبعد الحصول على الموافقة المكتوبة المسبقة من مشغل شبكة الدفع المحلية. يجب على العضو أو المرخص له الذي يجوز له منح ترخيص استخدام علامة شبكة الدفع المحلية إلى المرخص له من الباطن، أن يضمن أن شبكة الدفع المحلية يتم استخدامها بواسطة المرخص له من الباطن طبقاً للقواعد والمعايير الذي يطلبها مشغل شبكة الدفع المحلية لهذا الاستخدام.

لا يجوز ترخيص أو التنازل عن الحق في استخدام شعار شبكة الدفع المحلية، سواء عن طريق البيع أو الدمج أو الاندماج أو القبول أو إنفاذ القانون أو غير ذلك، دون موافقة كتابية مسبقة من مشغل نظام الدفع.

لا يلتزم مشغل شبكة الدفع المحلية بتقديم أي تعهدات أو ضمانات، سواء كانت صريحة أو ضمنية، تتعلق باستخدام شبكة الدفع المحلية (يقتصر دوره على تنفيذ عملية الإدارة والتشغيل) ولا يقوم مشغل شبكة الدفع المحلية على وجه التحديد بمسألة مشغل شبكة الدفع المحلية لأي من هذه التأكيدات والضمانات، إن وجدت.

4.11.1 قواعد المقاصة والتسوية وقبول المعاملات الإلكترونية

لا تدخل في نطاق التعليمات المذكورة هنا ويتم الإشارة إلى ما سبق وضعه من قبل مصرف ليبيا المركزي بصفته الجهة المسؤولة عن عمليات المقاصة.

5.11.1 قواعد التسعير والتبادل

الرجوع إلى الكتاب 3 الفصل 3 في هذه المجموعة من اللوائح.

12.1 إدارة الاحتيال والمخاطر

يختص مصرف ليبيا المركزي بوضع القواعد والمعايير التي يجب توافرها للرقابة والمتابعة وتجنب المخاطر المالية ومراقبة أي محاولات من شأنها أن تسبب ضرراً للمعاملات المالية. وتعد المصارف المشاركة هي المسؤولة عن حماية عملائها، وتلتزم بتعويضهم في حالة الإخلال بواجب الحماية. تم تفصيل المزيد في الفصل 6 من هذا الكتاب.

1.12.1 Detection of Unusual Activities

All card-issuing banks must provide monitoring and follow-up systems to monitor unusual activities in transactions, such as a change in the nature of use or the usual rate of spending in purchase or withdrawal transactions, as well as the number of repeated failed attempts for the card holder's personal identification number, which may create the impression that the user is not the actual holder of those card and it is preferable to have systems for immediate monitoring and act of refusal to protect the card in cases of suspicious transaction.

Banks and accepting parties are responsible for suspicious transactions executed by merchants or their agents contracting with those banks. Also, banks and accepting agencies bear all responsibilities and risks arising from payment service facilitators and service providers contracting with them, and accordingly, selective measures must be taken with an emphasis on the reputation of the contractors. So that these banks are not exposed to losses as a result of fraudulent transactions.

1.12.2 Customers Awareness and Data Security

Issuing Banks are committed to preserving all data related to customers, and are also fully responsible for securing the data and making sure that it is only accessed by employees with appropriate powers to their job roles.

Banks also bear the responsibility of raising awareness of card holders and users of the system, and clarifying the necessity of using secured transactions that require entering the personal identification number, as well as not sharing the personal identification number and card number with anyone, and immediately reporting to the issuing bank in the event of discovering the loss of the card.

1.12.3 System Applications Security

All applications and systems used to pass transactions through all parties participating in the transaction (whether by passing or settlement), must provide the necessary procedures for protection and insurance, as well as all parties to ensure the use of encryption methods for the data that is passed through networks and means of communication, as well as Encryption methods should be used for customer data and transaction records kept with issuing banks and accepting banks.

1.12.4 Securing Information Confidentiality

All parties involved in the system of financial transactions and payments operations in all its forms are obligated to maintain the confidentiality of information related to customers and card holders, as well as the confidentiality of transactions and the content of card data and everything that falls under customer data and accounts.

All banks must ensure that the systems and networks related to them are approved through the PCI DSS Payment Card Industry Data Security Standard in accordance with the latest update and rules established by that participating entity.

All banks must ensure that all employees of the parties participating in the payments system follow the conditions of not disclosing any data or transactions made available to them through their positions or roles in the payment system.

1.12.1 الكشف عن الأنشطة الضارة

يجب على جميع المصارف المصدرة للبطاقات، ان تقيم أنظمة مراقبة ومتابعة للكشف عن الأنشطة الضارة للمعاملات، مثل التغيير في طبيعة الاستخدام أو التغيير في معدل الإنفاق المعتاد في عمليات الشراء أو السحب، وكذلك عدد المحاولات الفاشلة المتكررة بالنسبة لرقم التعريف الشخصي لحامل البطاقة مما قد يعطي انطباعاً بأن المستخدم ليس هو المالك الفعلي لتلك البطاقة، ويستحسن أن تكون لديها أنظمة للمراقبة الفورية، واستخدام أمر الرفض لحماية البطاقة في حالات المعاملات المقترنة بشبهة الاحتيال.

تعتبر المصارف والوكالات المقبولة مسؤولة (تجاه العملاء) عن المعاملات المقترنة بشبهة الاحتيال والتي قد ينفذها التجار أو وكلائهم المتعاقدون مع تلك المصارف. كما تتحمل المصارف والوكالات المقبولة جميع المسؤوليات والمخاطر الناشئة عن ميسري خدمات الدفع ومقدمي الخدمات المتعاقدين معهم، ولذلك يجب اتخاذ إجراءات احترازية، التحقق من سمعة هؤلاء المتعاقدون، حتى لا تتعرض هذه المصارف للخسائر نتيجة التعويض عن المعاملات الاحتيالية.

2.12.1 توعية العملاء وأمن البيانات

تلتزم المصارف المصدرة للبطاقات بحفظ جميع البيانات المتعلقة بالعملاء، كما أنها مسؤولة مسؤولية كاملة عن تأمين البيانات والتحقق من أن إمكانية الوصول للبيانات يقتصر فقط على الموظفين المختصين على استعمال تلك البيانات حسب الغرض المخصصة له.

كما تلتزم المصارف بتوعية حاملي البطاقات ومستخدمي النظام، على ضرورة استخدام المعاملات الآمنة التي تتطلب إدخال رقم التعريف الشخصي، وكذلك عدم مشاركة رقم التعريف الشخصي ورقم البطاقة مع أي شخص، ويجب عليهم إعلام المصرف المصدر وبشكل فوري في حالة اكتشاف ضياع البطاقة، أو سرقتها.

3.12.1 نظام أمن التطبيقات

جميع التطبيقات والأنظمة المستخدمة لتنفيذ المعاملات بواسطة جميع الأطراف المشاركة في المعاملة (سواء بالمرور أو التسوية)، يجب أن تحتوي على الإجراءات اللازمة للحماية والتأمين، وذلك لضمان استخدام طرق التشفير للبيانات التي يتم تمريرها عبر الشبكات ووسائل الاتصال، وكما يجب استخدام طرق التشفير لبيانات العملاء وسجلات المعاملات المحفوظة لدى المصارف المصدرة للبطاقات والمصارف التي تقبل البطاقات.

4.12.1 تأمين سرية المعلومات

تلتزم جميع الأطراف المشاركة في نظام المعاملات المالية وعمليات الدفع بجميع أشكالها بالحفاظ على سرية المعلومات والبيانات والمعاملات المتعلقة بالعملاء وحاملي البطاقات.

يجب على جميع المصارف التحقق من أن الأنظمة والشبكات المتعلقة بها قد تمت الموافقة عليها من قبل معيار أمن بيانات صناعة بطاقات الدفع PCI DSS وفقاً لآخر تحديث، إضافة إلى القواعد التي وضعتها الكيان المشارك.

يجب على جميع المصارف التحقق من أن جميع موظفي الأطراف المشاركة في نظام المدفوعات يلتزمون بشروط عدم الإفصاح (السرية) عن أي بيانات أو معلومات أو معاملات تتعلق بالعملاء كانت متاحة لهم من خلال عملهم في نظام الدفع.

1.13 Compliance with Rules & Regulations

Failure to comply with any standard adversely affects subscribed members and their customers and undermines the integrity of the national payments network. Accordingly, a Participant who fails to comply with any Standard shall be subject to assessments (“Non-Compliance Ratings”) as stated in the Standards.

From time to time, a national distributor creates programs that address cases of non-compliance with certain standards. Each case of non-compliance pertains to a standard not implemented by the participant that falls into at least one of the following three categories of compliance:

(Category A) Integrity of Payment Services

Category A incompliance affects the integrity of the payment system. The National Scheme Operator has the authority to impose monetary non-compliance assessments in the event of category A incompliance. Violations of Payment System Integrity include, but are not limited to, implied non-compliance with licensing requirements, signature and monitoring requirements for the merchant and ATM owner, and protection of card, account or transaction information.

(Category B) Interacting with Customers

Category B incompliance deals with visible irregularities, particularly by customers of issuing banks and/or Acquiring banks.

The National Scheme Operator has the power to impose monetary non-compliance penalties in the event of Category B non-compliance or, alternatively, may allow (alternatively) to provide notice and a stated undertaking of time to address the incompliance before the imposition of monetary fines.

Violations that are visible, which include violations - but not limited to - incompliance involving the use of the National Payments Network logo in violation of license terms, the application of selective approvals for transactions, or the identification of the merchant in the POI, or the override of minimum and maximum transaction amounts, and payment Additional amounts for merchants and providers of transactions, or failure to apply the conditions to be met in the transaction receipt, or notices of fees for the right to use ATMs.

(Category C) Efficiency and Performance

Category C incompliance deals with operational efficiency and performance. The National Scheme operator has the power to impose monetary fines in the event of incompliance with this category, or in return a notification is given by the violator, including a limitation of the time required to remedy the non-compliance that exists before imposing monetary fines.

“Efficiency and Operational Performance” Breach of performance includes, but is not limited to, incompliance that involves operating transactions within the stipulated time frame, providing merchants with materials required to process transactions, holding the Card at ATMs, card fees and reporting procedures, and the obligation to provide National distributor with the required information.

13.1 الامتثال للقواعد واللوائح

يرتب عدم الامتثال للقواعد واللوائح والمعايير، تأثيراً سلباً على الأعضاء المشتركين وعملائهم، ويخفض من درجة سلامة شبكة الدفع المحلية. وعليه، يجب أن يخضع المشارك الذي لا يلتزم بأي معيار، لعمليات التقييم (“تقييمات عدم الامتثال”) كما هو مذكور في المعايير.

من وقت لآخر يقوم مشغل شبكة الدفع المحلية، بإنشاء برامج تعالج حالات عدم الامتثال لمعايير معينة. بحيث تتعلق كل حالة من حالات عدم الامتثال بمعيار لم يتم تنفيذه من قبل المشارك والتي يكون ضمن واحد على الأقل من فئات الامتثال الثلاث التالية:

(الفئة أ) سلامة خدمات الدفع

يؤثر عدم الامتثال للفئة أ على سلامة نظام الدفع. ويتمتع مشغل شبكة الدفع المحلية في هذه الحالة، بسلطة فرض ضمانات نقدية في حالة عدم الامتثال للفئة “أ”. يشمل الإخلال بسلامة نظام الدفع، على سبيل المثال ليس الحصر، عدم الامتثال الضمني لقواعد الترخيص، وقواعد التوقيع والمراقبة للتاجر ومالك أجهزة الصراف الآلي، وحماية معلومات البطاقة أو الحساب أو المعاملة.

(الفئة ب) التعامل مع العملاء

عدم الامتثال وفقاً (للفئة ب) يعد مخالفة مرئية خاصة من قبل عملاء المصارف المصدرة أو المصارف القابلة

يتمتع مشغل شبكة الدفع المحلية بسلطة فرض غرامات مالية في حالة عدم الامتثال (للفئة ب)، ويجوز له بدلا من ذلك، الاكتفاء بتقديم إشعار وتعهّد محدد المدة لمعالجة حالة عدم الامتثال قبل فرض الغرامات المالية.

الانتهاكات المرئية، والتي تشمل الانتهاكات، على سبيل المثال لا الحصر، عدم الامتثال الذي يتضمن استخدام شعار شبكة الدفع المحلية بما يخالف شروط الترخيص: تطبيق الموافقات الانتقائية للمعاملات، أو تحديد التاجر POI، أو تجاوز الحد الأدنى والحد الأقصى لمبالغ المعاملات، ودفع مبالغ إضافية للتجار ومقدمي الخدمات، أو عدم تطبيق الشروط الواجب توافرها في إيصال المعاملة أو الاخطارات برسوم الحق في استخدام أجهزة الصراف الآلي.

الفئة (ج) الكفاءة والأداء

يرتبط عدم الامتثال (للفئة ج) مع الكفاءة التشغيلية وجودة الأداء. وعليه، يتمتع مشغل شبكة الدفع المحلية بسلطة فرض غرامات مالية في حالة عدم الامتثال لهذه الفئة، ويجوز له بدلا من ذلك، الاكتفاء بتقديم إشعار وتعهّد محدد المدة لمعالجة حالة عدم الامتثال قبل فرض الغرامات المالية. “الكفاءة وجودة الأداء التشغيلي” يشمل خرق الأداء، على سبيل المثال لا الحصر، عدم الامتثال الذي يتضمن تشغيل المعاملات ضمن الوقت الزمني المحدد، وتزويد التجار بالمواد المطلوبة لمعالجة المعاملات، وحمل البطاقة في أجهزة الصراف الآلي، ورسوم البطاقة وإجراءات الإبلاغ، والالتزام بتزويد مشغل شبكة الدفع المحلية بالمعلومات المطلوبة.

Compliance Procedures

- 1. Auditing missions shall be conducted through the NSO auditing team through delegation granted by the CBL, through such mission it should vit through internal auditing tasks performed internally by the participant member and a health check on a random basis to assure that it is made in right way
- 2. The CBL through its’ own verification and auditing missions would set the rules and basis of verification and would conduct a random check on the above-mentioned task performed by the NSO.
- 3. The auditing tasks should not be limited to the operational tasks but should include those parts relevant to AML/CFT rules implemented under the early published laws by CBL and to assure that no deviations of such rules in its related bulletins published by the CBL.

1.14 Exceptions and Waivers

There are no exceptions to any rule of compliance or what is included in the operating instructions. However, there may be compatibility and harmonization in some items and implementation modalities through the main parties participating in the National payment Network.

This exception may be needed to address some technical issues related to the operating systems or to the presence of technical limitations that prevent implementation as required.

1.15 Rules of Handling Exceptions and Waivers

That the party requesting the exception submits to the National Scheme Operator a request for an appeal explaining the rules in which an exception is requested, with an explanation of the technical reason that led to the inability to comply and implement, and it must also provide alternatives for implementation to return to achieve the same goal of the job in which it is desired to obtain an exception.

Bearing in mind that submitting the appeal in and of itself does not mean approval, and that the national distributor should not bear any additional costs or burdens as a result of achieving the required exception

1.16 Work Flows

1.16.1 Purchasing Authorization Flow

(See appendix number1)

1.16.2 ATM Authorization Flow (off-us)

(See appendix number2)

1.16.3 Clearing and Settlement Flow

(See appendix number3)

1.16.4 Chargeback Flow

(See appendix number4)

1.16.5eCommerce 3DS 2.0 Flow

(See appendix number5)

إجراءات الامتثال

1- تتم مهام التدقيق من خلال فريق التدقيق التابع لمشغل شبكة الدفع المحلية من خلال التفويض الممنوح لهم من قبل مصرف ليبيا المركزي. يجب على فريق التدقيق أن يقوم بإجراء مهام التدقيق الداخلي بواسطة العضو المشارك، والقيام بعملية الفحص الدقيق على أساس غير رسمي للتحقق من أنه يتم بالطريقة الصحيحة.

2- يضع مصرف ليبيا المركزي من خلال فرق التحقق والتدقيق الخاصة به قواعد وأسس القيام بعملية التدقيق، ويجري فحصًا عشوائيًا للعملية المذكورة أعلاه التي يؤديها مشغل شبكة الدفع المحلية.

3- لا تقتصر مهام فرق التدقيق على التدقيق على المهام التشغيلية، بل يجب أن تشمل مدى الالتزام بتطبيق القواعد المتعلقة بمكافحة غسيل الأموال وتمويل الإرهاب وفقا للقوانين النافذة، إضافة إلى التحقق من عدم وجود انحرافات عن هذه القواعد في النشرات ذات الصلة التي نشرها مصرف ليبيا المركزي.

14.1 الاستثناءات والتنازلات

لا توجد استثناءات على تطبيق أي قاعدة من قواعد الامتثال، أو ما هو مدرج في تعليمات التشغيل. ومع ذلك، قد يكون هناك توافق وتناسق بين بعض البنود وطرق التنفيذ من خلال الأطراف الرئيسية المشاركة في شبكة الدفع المحلية.

وقد تكون هناك حاجة إلى هذا الاستثناء لمعالجة بعض المشكلات الفنية المتعلقة بأنظمة التشغيل أو لوجود عقبات فنية تمنع التنفيذ كما هو مطلوب.

15.1 قواعد التعامل مع الاستثناءات والتنازلات

يجب على الطرف الذي يطلب الاستثناء أن يقدم طلباً بذلك إلى مشغل شبكة الدفع المحلية، يبين فيه القواعد التي يُطلب فيها منحه استثناءً على الامتثال لها، مقترناً بتوضيح السبب الفني الذي أدى إلى عدم قدرته على الامتثال لها وتنفيذها، ويجب عليه أيضًا توفير البدائل، من أجل أن يكون التنفيذ محققا لجودة الوظيفة المطلوب الحصول على استثناء فيها.

16.1 سير العمل

1.16.1 سير تفويض الشراء

(انظر الملحق رقم 1)

2.16.1 سير تفويض أجهزة الصراف الآلي (off-us)

(انظر الملحق رقم 2)

3.16.1 سير المقاصة والتسوية

(انظر الملحق رقم 3)

4.16.1 سير تحميل التكاليف

(انظر الملحق رقم 4)

5.16.1 سير التجارة الإلكترونية DS 3 2.0

(انظر الملحق رقم 5)

Rules and Regulations of The Libyan National Payment Scheme

Chapter 2 - Members Compliance

This Chapter contains the Standards relating to general Member obligations, variances, violations of the Standards, penalties, confidential information and data protection.

2.1 Standards

From time to time, aligned with CBL strategy and standards the National Scheme Operator announce Standards governing the conduct of Members and Activity or Digital Activity.

The National Scheme Operator has the sole right to interpret and enforce the Standards Without prejudice to art 11 of the CBL high level regulation.

The National Scheme Operator has the right, but not the obligation, to resolve any dispute between or among Members including, but not limited to, any dispute involving the National Scheme Operator, the Standards, or the Members' respective Activities or Digital Activities, and any such resolution by the National Scheme Operator is final and not subject to appeal, review, or other challenge.

In resolving disputes between or among Members, or in applying its Standards to Members, the National Payment Scheme has the right to deviate from any process in the Standards or that the National Scheme Operator otherwise applies, and to implement an alternative process, if an event, including, without limitation, an account data compromise event, is, in the sole judgment of the National Scheme Operator, of sufficient scope, complexity and/or magnitude to warrant such deviation.

The National Scheme Operator will exercise its discretion to deviate from its Standards only in circumstances the National Scheme Operator determines to be extraordinary. Any decision to alter or suspend the application of any process will not be subject to appeal, review, or other challenge.

2.2 Variances

A variance is the consent by the National Scheme Operator for a Member to act other than in accordance with a Standard. Only a member has the right to request a variance. Any such request must specify the Rules or other Standards for which a variance is sought. The request must be submitted to the National Scheme Operator in writing, together with a statement of the reason for the request. If the request is approved, the National Scheme Operator has the right to determine the period for which the variance is granted. The Member must achieve compliance by the date specified.

2.3 Failure to Comply with a Standard

Any failure to comply with any of the Standards would adversely affects the National Scheme Operator and its Members and undermines the integrity of the National Scheme Operator system. Accordingly, a member that who does not comply with any Standard is therefore subject to assessments ("Non-Compliance Ratings") as described in the Standards.

قواعد ولوائح شبكة الدفع المحلية الليبية

الفصل 2 – امتثال الأعضاء

يحتوي هذا الفصل على المعايير المتعلقة بالتزامات الأعضاء العامة، والفروق، والإخلال بالمعايير، والجزاءات، والمعلومات السرية، وحماية البيانات.

1.2 المعايير

يجب على مشغل شبكة الدفع المحلية، وتماشياً مع استراتيجية ومعايير مصرف ليبيا المركزي أن يعلن بشكل دوري، عن المعايير التي تحكم سلوك الأعضاء، وتنفيذ الأنشطة الرقمية وغير الرقمية.

لمشغل شبكة الدفع المحلية وحده الحق في تفسير المعايير وتنفيذها دون الإخلال بالمادة 11 من اللائحة العليا لمصرف ليبيا المركزي.

يجوز لمشغل شبكة الدفع المحلية ، حل أي نزاع بين الأعضاء بما في ذلك، على سبيل المثال لا الحصر، أي نزاع يتعلق بتنفيذ المعايير أو الأنشطة أو الأنشطة الرقمية الخاصة بالأعضاء، و يعد القرار الذي يصدره مشغل شبكة الدفع المحلية قراراً نهائياً، ولا يجوز التظلم منه، أو الطعن فيه.

في حالة قيامه بحل المنازعات بين الأعضاء، أو في مدى التزامهم بتطبيق القواعد والمعايير والتعليمات الصادرة منه، يحق مشغل شبكة الدفع المحلية، الانحراف عن المعايير التي يطبقها عند قيامه بأي عملية وتنفيذها بطريقة بديلة، إذا كان هناك خرق في تطبيقها، مثال ذلك حدث اختراق في بيانات الحساب، ويتمتع مشغل شبكة الدفع المحلية وحده بالسلطة التقديرية، لتقرير مدى التعقيد الذي يبرر هذا الانحراف.

يمارس مشغل شبكة الدفع المحلية سلطته التقديرية في الخروج عن معاييره فقط في الظروف الاستثنائية التي يقدرها. لا يجوز التظلم أو الطعن في القرار التي يتخذها مشغل شبكة الدفع المحلية والتي يترتب عليه تغيير أو تعديل أو تعليق تنفيذ التطبيقات في أي عملية من العمليات.

2.2 الاختلاف

الاختلاف هو موافقة مشغل شبكة الدفع المحلية لنظام الدفع على أن يتصرف العضو بخلاف ما توجبه المعايير. يجوز للعضو فقط أن يتقدم بطلب مكتوب، مبينا فيه السبب ، ومحددأ فيه القواعد أو المعايير الأخرى المطلوب تغييرها. وإذا تمت الموافقة على هذا الطلب، يجوز لمشغل شبكة الدفع المحلية تحديد المدة الزمنية التي يتم فيها الخروج عن القواعد والمعايير. يجب على العضو تحقيق الامتثال بحلول الأجل المحدد.

3.2 عدم الامتثال لأي معيار

أي فشل في الامتثال لأي من المعايير سيؤثر سلباً على مشغل شبكة الدفع المحلية وأعضائه، ويؤثر على نزاهته. وبناءً على ذلك، فإن العضو الذي لا يمثل لأي معيار يخضع بالتالي لإجراءات ("تصنيفات عدم الامتثال") كما هو موضح في المعايير.

In addition to, the imposition of a noncompliance ratings, the National Scheme Operator, as per given delegation from CBL, has the right to require a member to take such action and the National Scheme Operator itself has the right to take such action as the National Scheme Operator deems necessary or appropriate to ensure compliance with the Standards and secure the integrity of the National Scheme Operator system. In the exercise of such discretion, the National Scheme Operator (As per given delegation from Central Bank of Libya) has the right to consider the nature, fluffiness, number and frequency of occurrences and possible consequences resulting from a failure to comply with any Standard. The National Scheme Operator has the right, but not the obligation, to provide notice and limited time to cure such noncompliance before imposing a noncompliance assessment.

The National Scheme Operator reserves the right to limit, suspend a Member's Participation and/or Licenses or to amend the rights, obligations, or both of the Member, whether set forth in a License or otherwise, if that Member does not comply with any Standards or with any decision of the National Scheme Operator with regard to the interpretation and enforcement of any Standards.

2.4 Conduct of Activity

(Category A)

Each Member at all times must conduct Activity and Digital Activity in compliance with the Standards and with all applicable laws and regulations. A Member is not required to undertake any act that is unambiguously prohibited by applicable law or regulation. If a Member is unable to comply with a Standard because of applicable law or regulation, then the National Scheme Operator has the right to require that such Member undertake some other form of permissible Activity.

If a party other than a Member files a claim against a Member concerning the Member's Activity or Digital Activity, the National Scheme Operator must be informed thereof by the Member. The National Scheme Operator is entitled but not obliged to intervene in the case.

2.5 Obligations of a Sponsor

(Category A)

Each Member that Sponsors one or more Payment Service Providers must cause each such Payment Service Provider to comply with all Standards applicable to the Activity of that Payment Service Provider. Each Sponsor is liable to the National Scheme Operator and to all other Members for all Activities of each of its Sponsored Payment Service Providers and for any failure by any such Sponsored Payment Service Provider to comply with a Standard or with applicable law or regulation.

2.6 Payment Service Providers

(Category A)

Except to the extent any liability or obligation arising under a Standard has been satisfied by a Sponsor, each Payment Service Provider is responsible for the liabilities and obligations arising out of or in connection with its Activities, regardless of any:

1. Action taken by such Payment Service Provider to satisfy such liability or obligation with, through or by a Sponsor or former Sponsor of such Payment Service Provider, or
2. Agreement between any Sponsor and such Payment Service Provider.

بالإضافة إلى فرض تصنيفات عدم الامتثال، يجوز لمشغل شبكة الدفع المحلية، وفقًا لتفويض معين من مصرف ليبيا المركزي، أن يطلب من أحد الأعضاء اتخاذ مثل هذا الإجراء، ويجوز له من تلقاء نفسه، وبناءً على سلطته التقديرية، اتخاذ مثل هذه الإجراءات متى رأى إنها ضرورية لضمان الامتثال للمعايير وتأمين سلامة نظام مشغل الشبكة المحلية. ويجوز لمشغل شبكة الدفع المحلية (وفقًا لتفويض خاص من مصرف ليبيا المركزي) الأخذ بعين الاعتبار المسؤولية المترتبة عن طبيعة وتضم وعدد وتكرار المخالفات، والعواقب المحتملة الناتجة عن عدم الامتثال لأي معيار. يحق لمشغل شبكة الدفع المحلية، ولكنه غير ملزم، بتقديم إشعار للعضو في حالة عدم الامتثال، متضمن المدة الزمنية اللازمة لتطبيق معايير الامتثال على نشاطه.

وفي جميع الأحوال، يحتفظ مشغل شبكة الدفع المحلية بالحق في تقييد أو تعليق مشاركة العضو أو إلغاء تراخيصه أو تعديل حقوقه أو التزاماته، إذا كان العضو لا يمثل لأي معايير أو لا يلتزم بتطبيق القرارات الصادرة عن مشغل شبكة الدفع المحلية فيما يتعلق بتفسير وتنفيذ أي المعايير.

4.2 القيام بالنشاط

(الفئة أ)

يجب على كل عضو، وفي جميع الأوقات، القيام بالنشاط والنشاط الرقمي وفقًا للمعايير، وجميع القوانين واللوائح المعمول بها. لا يُطلب من العضو القيام بعمل مخالف أو ممنوع بموجب القانون أو اللوائح المعمول بها. إذا كان العضو غير قادر على الامتثال لمعيار بسبب القانون أو اللوائح المعمول بها، فعندئذٍ يحق لمشغل شبكة الدفع المحلية مطالبته بالقيام به بشكل آخر من أشكال النشاط المسموح بها.

إذا قام طرف آخر غير العضو بتقديم دعوى قضائية ضد عضو آخر، تتعلق بنشاطه أو النشاط الرقمي، فيجب إعلام مشغل شبكة الدفع المحلية بذلك من قبل العضو. ويجوز لمشغل شبكة الدفع المحلية في هذه الحالة التدخل في الدعوى ولكنه غير ملزم بذلك.

5.2 التزامات الراعي

(الفئة أ)

يجب على كل عضو يرعى واحدًا أو أكثر من مقدمي خدمات الدفع أن يجعل كل مقدم خدمة دفع يلتزم بجميع المعايير المطبقة على نشاط مقدم خدمة الدفع هذا. كل راعي مسؤول أمام مشغل شبكة الدفع المحلية وأمام جميع الأعضاء الآخرين عن جميع أنشطة كل من مقدمي خدمة الدفع المكفول وعن أي فشل من قبل أي مقدم خدمة دفع مكفول في الامتثال لمعيار أو مع القانون أو اللوائح المعمول بها.

6.2 مقدمي خدمة الدفع

(الفئة أ)

باستثناء الحد الذي يتم فيه الوفاء بالالتزامات الناشئة من قبل الرعاة، يكون مقدمي خدمة الدفع مسؤولين عن الوفاء بالالتزامات المتعلقة بأنشطتهم، بصرف النظر عن أي منها:

1. الإجراءات التي يتخذها مقدمي خدمة الدفع للوفاء بالتزاماتهم أو عن طريق الراعي أو الراعي السابق لمقدم خدمة الدفع.
2. اتفاق بين أي راعي ومقدم خدمة الدفع.

In accordance with the Standards and in compliance with all applicable laws and regulations, each Sponsor will have access to and is permitted to use or otherwise process its Sponsored Payment Service Providers' Confidential Information and Confidential Transaction Data in connection with authorization, settlement, clearing, fraud reporting, chargebacks, billing, and other related activities.

2.7 Financial Health

(Category A)

Each Member must conduct all Activity and otherwise operate in a manner that is financially sound and so as to avoid risk to the National Scheme Operator and to other Members.

A Member must promptly report to the National Scheme Operator any materially adverse financial condition or discrepancy or suspected materially adverse financial condition or discrepancy relating to the Member or, in the case of a Principal or Association, any Sponsored Payment Service Provider.

The Member must refer or, if applicable, cause the Payment Service Provider to refer such condition or discrepancy to independent certified public accountants or another person or firm satisfactory to the National Scheme Operator for evaluation and recommendation as to remedial action, and promptly provide to the National Scheme Operator a copy of such evaluation and recommendation after receipt thereof.

2.8 Compliance

From time to time, the National Scheme Operator has the right to develop means and apply criteria to evaluate a Member's compliance with Rule 2.4. Each Member must fully cooperate with any effort by the National Scheme Operator and the National Scheme Operator's representatives to evaluate a Member's compliance with Rule 2.4.

In the event that the National Scheme Operator determines that a Member is not complying or may not on an ongoing basis comply with the requirements of Rule 2.4, the National Scheme Operator has the right to:

1. Impose special terms upon the Member as the National Scheme Operator deems necessary or appropriate until each condition or discrepancy is resolved to the National Scheme Operator's satisfaction so as to enable the Member to be and to remain in full compliance with Rule 2.4, or
2. Withdraw the Member's Participation.

As granted by CBL the NSO has the right to supervision and audit the banks to insure the execution and compliance with regulations in terms of the listed rules mentioned within the document

2.9 Indemnity and Liability Limitations

Each Member (each, for the purposes of this Rule, an "Indemnifying Member") must protect, indemnify, and hold harmless the National Scheme Operator and the National Scheme Operator's parent and subsidiaries and Payment Service Provider entities, and each of the directors, officers, employees and Payment System Providers of the National Scheme Operator and the National Scheme Operator's parent and subsidiaries and Payment Service Provider entities from any actual or threatened claim, demand, obligation, loss, cost, liability and/or expense (including, without limitation, actual attorneys' fees, costs of

وفقًا للمعايير وامثالًا لجميع القوانين واللوائح المعمول بها، يكون لكل راعي الحق في الوصول إلى المعلومات السرية وبيانات المعاملات السرية الخاصة بمقدمي خدمة الدفع المكفولة، ويسمح لهم باستخدامها أو معالجتها بطريقة أخرى فيما يتعلق بالتفويض والتسوية والتصفية، والإبلاغ عن شبهات الاحتيال وعمليات رد المبالغ المدفوعة والفواتير والأنشطة الأخرى ذات الصلة.

7.2 المطابقة المالية

(الفئة أ)

يلتزم كل عضو بإجراء جميع الأنشطة بطريقة تتطابق مع النظم المالية المعمول بها، وذلك لتجنب المخاطر التي قد يتعرض لها مشغل شبكة الدفع المحلية والأعضاء الآخرين.

يلتزم كل عضو بتقديم تقريره فوراً إلى مشغل شبكة الدفع المحلية عن أي حالة مالية معاكسة أو متناقضة أو مشتبه فيها، تتعلق بالعضو، أو في حالة المسؤول أو المؤسسة، مزود خدمة الدفع المكفول.

يلتزم كل عضو بالرجوع، إن كان ذلك ممكناً، إلى سبب القيام بخدمة الدفع، ويكون تقييم التعارض والتناقض والاشارة إلى الشرط أو التناقض عن طريق محاسبين قانونيين مستقلين أو أي جهة يوافق عليها مشغل شبكة الدفع المحلية، ويجب على من تم اختياره للقيام بعملية التقييم تزويد مشغل شبكة الدفع المحلية فور انتهاء عمله بنسخة من تقريره والتوصية بالإجراءات التصحيحية التي يجب اتباعها.

8.2 الامتثال

يجوز لمشغل شبكة الدفع المحلية، وبشكل دوري تطوير الوسائل وتطبيق المعايير لتقييم امتثال العضو للقاعدة 2.4. يلتزم كل عضو بالتعاون بشكل كامل مع أي جهد يبذله مشغل شبكة الدفع المحلية وممثلوه، لتقييم امتثال العضو للقاعدة 2.4.

في حالة ما إذا قرر مشغل شبكة الدفع المحلية أن أحد الأعضاء لا يمثل، أو قد لا يمثل على أساس مستمر لمتطلبات القاعدة 2.4، فإنه يجوز لمشغل شبكة الدفع المحلية اتخاذ الإجراءات التالية:

1. فرض شروط خاصة على العضو يقدر مشغل شبكة الدفع المحلية إنها ضرورية لحل كل حالة أو تناقض، وذلك لتمكين العضو من الالتزام التام بالقاعدة 2.4 ،
2. سحب مشاركة العضو.

كما أن مصرف ليبيا المركزي منح مشغل شبكة الدفع المحلية ممارسة سلطة الإشراف والتدقيق على المصارف لضمان عمليات التنفيذ، والامتثال للوائح من حيث القواعد المدرجة في الوثيقة.

9.2 تحديد المسؤولية والتعويض

يجب على كل عضو (لأغراض هذه القاعدة ، "عضو الذي يقوم بالتعويض") حماية وتعويض وإبعاد الضرر عن مشغل شبكة الدفع المحلية والجهات الأم والشركات التابعة لمشغل شبكة الدفع المحلية وكيانات مقدم خدمة الدفع، وكل من المديرين، الضباط والموظفون ومقدمي نظام الدفع مشغل شبكة الدفع المحلية والجهة الأم مشغل شبكة الدفع المحلية والشركات التابعة لها وكيانات مقدم خدمة الدفع من أي مطالبة أو طلب أو التزام أو خسارة أو تكلفة أو مسؤولية و/ أو مصروفات فعلية أو مهددة (بما في ذلك ، على سبيل المثال لا الحصر ، أتعاب المحاماة الفعلية ، وتكاليف التحقيق ،

investigation, and disbursements) resulting from and/or arising in connection with, any act or omission of the Indemnifying Member, its subsidiaries, or any person associated with the Indemnifying Member or its subsidiaries (including, without limitation, such Indemnifying Member's directors, officers, employees and Payment System Providers, all direct parents, subsidiaries, and Payment Service Providers of the Indemnifying Member, the Indemnifying Member's customers in connection with issuing and/or acquiring Activity and/or Digital Activity and/or other business, and the Indemnifying Member's suppliers, including, without limitation, Service Providers, Card production vendors, and other persons acting for, or in connection with, the Indemnifying Member or a Merchant or other entity for which the Indemnifying Member acquires Transactions, or any such Merchant's or entity's employees, representatives, Payment System Providers, suppliers or Members, including any Data Storage Entity) with respect to, or relating to:

1. Any Programs and/or other Activities and/or Digital Activities of the Indemnifying Member;
2. Any programs and/or activities of any person associated with the Indemnifying Member and/or its subsidiaries;
3. The compliance or noncompliance with the Standards by the Indemnifying Member;
4. The compliance or noncompliance with the Standards by any person associated with the Indemnifying Member and its subsidiaries;
5. Any other activity of the Indemnifying Member;
6. Direct or indirect access to and/or use of the Network (it being understood that the National Scheme Operator does not represent or warrant that the Network or any part thereof is or will be defect-free or error-free and that each Member chooses to access and use the Network at the Member's sole risk and at no risk to the National Scheme Operator);
7. Any other activity and any omission of the Indemnifying Member and any activity and any omission of any person associated with the Indemnifying Member, its subsidiaries, or both, including but not limited to any activity that used and/or otherwise involved any of the Marks or other assets; or
8. The National Scheme Operator's interpretation, enforcement, or failure to enforce any Standards.

The National Scheme Operator does not represent or warrant that the Network or any other system, process or activity administered, operated, controlled or provided by or on behalf of the National Scheme Operator (collectively, for purposes of this section, the "Systems") is free of defect and/or mistake and, unless otherwise specifically stated in the Standards or in a writing executed by and between the National Scheme Operator and a Member, the Systems are provided on an "as-is" basis and without any express or implied warranty of any type, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose or non-infringement of third party intellectual property rights.

Under no circumstance will the national scheme operator be liable for any indirect, incidental, special or consequential damages, for loss of profits, or any other cost or expense incurred by a member or any third party arising from or related to use or receipt of the systems, whether in an action in contract or in tort, and even if the member or any third party has been advised of the possibility of such damages. each member assumes the entire risk of use or receipt of the systems.

والمصروفات) الناتجة عن و/ أو الناشئة فيما يتعلق بأي فعل أو إغفال للعضو المُعوض ، أو الشركات التابعة له ، أو أي شخص مرتبط بالعضو المُعوض أو الشركات التابعة له (بما في ذلك، بدون القيود ، مثل أعضاء مجلس الإدارة والمسؤولين والموظفين ومقدمي نظام الدفع التابعين للعضو، وجميع الجهات الأم المباشرة، والشركات التابعة، و مقدم خدمات الدفع التابعون للعضو المُعوض، وعملاء العضو المُعوض فيما يتعلق بإصدار و/ أو قبول نشاط و/ أو نشاط رقمي و/ أو أعمال أخرى، وموردي العضو المُعوض، بما في ذلك ، على سبيل المثال لا الحصر، مقدمي الخدمة، وموردي إنتاج البطاقات، والأشخاص الآخرون الذين يعملون لصالح، أو يرتبطون، بالعضو المُعوض أو تاجر أو كيان آخر يكتسب العضو المُعوض المعاملات من أجله ، أو أي من موظفي التاجر أو الكيان أو الممثلين أو مقدمي نظام الدفع أو الموردين أو الأعضاء، بما في ذلك أي كيان لتخزين البيانات) فيما يتعلق أو تتعلق بما يلي:

1. أي برامج أو أنشطة رقمية أو غير رقمية للعضو المُعوض.
2. البرامج أو الأنشطة لشخص مرتبط بالعضو المُعوض أو الشركات التابعة له.
3. الامتثال أو عدم الامتثال للمعايير من قبل العضو المُعوض.
4. الامتثال أو عدم الامتثال للمعايير من قبل الشخص المرتبط بالعضو المُعوض والشركات التابعة له.
5. أي نشاط آخر للعضو المُعوض.
6. الوصول المباشر أو غير المباشر للشبكة أو استخدامها (مع العلم أن مشغل شبكة الدفع المحلية لا يقر أو يضمن أن الشبكة أو أي جزء منها سيكون خاليًا من العيوب أو خالي من الأخطاء، وأن كل عضو يختار الوصول إلى الشبكة واستخدامها على مسؤوليته وحده ودون تحميل مشغل شبكة الدفع المحلية بأي مسؤولية.
7. أي نشاط آخر أو أي خطأ للعضو المُعوض، أو للعضو المرتبط به، أو الشركات التابعة له، أو كليهما، بما في ذلك على سبيل المثال، أي نشاط استخدم أو شارك بطريقة أخرى في أي من العلامات أو الأصول الأخرى.
8. تفسير مشغل شبكة الدفع المحلية وتطبيقه، أو الفشل في تطبيق معايير.

لا يقر مشغل شبكة الدفع المحلية ولا يضمن أن الشبكة أو أي نظام آخر أو عملية أو نشاط يتم إدارته أو تشغيله أو التحكم فيه أو توفيره بواسطة، أو نيابة عنه (مجتمعين، لأغراض هذا القسم، "الأنظمة") خالية من العيوب أو الأخطاء، ما لم ينص على خلاف ذلك، كتابة، أو في المعايير. يتم توفير الأنظمة على أساس "كما هي" وبدون تقديم أي ضمان، بما في ذلك، على سبيل المثال وليس الحصر، الضمانات الخاصة بالتسويق والملاءمة لغرض معين، أو عدم التعدي على حقوق الملكية الفكرية لطرف ثالث.

في جميع الأحوال، لا يتحمل مشغل شبكة الدفع المحلية أي مسؤولية عن الأضرار سواء كانت غير مباشرة أو عرضية أو خاصة أو تبعية، أو خسارة الأرباح، أو أي تكاليف أخرى يتكبدها العضو أو أي طرف ثالث تتعلق باستخدام أو استلام الأنظمة، سواء كانت طبقاً لقواعد المسؤولية العقدية، ولو تم إخطار العضو أو الطرف ثالث بإمكانية حدوث مثل هذه الأضرار. وعليه، يتحمل كل عضو مسؤولية مخاطر استخدام أو استلام الأنظمة.

Only in the event the limitation of liability set forth in the immediately preceding paragraph is deemed by a court of competent jurisdiction to be contrary to applicable law, the total liability, in aggregate, of the National Scheme Operator to a Member and anyone claiming by or through the Member, for any and all claims, losses, costs or damages, including attorneys' fees and costs and expert-witness fees and costs of any nature whatsoever or claims expenses resulting from or in any way related to the Systems shall not exceed the total compensation received by the National Scheme Operator from the Member for the particular use or receipt of the Systems during the 12 months ending on the date that the National Scheme Operator was advised by the Member of the Systems concern or the total amount of LDY 4,319,775, whichever is less. It is intended that this limitation apply to any and all liability or cause of action however alleged or arising; to the fullest extent permitted by law; unless otherwise prohibited by law; and notwithstanding any other provision of the Standards.

A payment or credit by the National Scheme Operator to or for the benefit of a Member that is not required to be made by the Standards will not be construed to be a waiver or modification of any Standard by the National Scheme Operator. A failure or delay by the National Scheme Operator to enforce any Standard or exercise any right of the National Scheme Operator set forth in the Standards will not be construed to be a waiver or modification of the Standard or of any of the National Scheme Operator's rights therein.

2.10 Legal Jurisdiction

The laws of Libya govern all disputes involving the National Scheme Operator, the Standards, and/or Members and Activity and Digital Activity without regard to conflicts-of-law provisions. Any action initiated by a Member regarding and/or involving the National Scheme Operator, the Standards and/or any Member and Activity and Digital Activity must be brought, if at all, only in the courts of Libya, and any Member involved in an action hereby submits to the jurisdiction of such courts.

This provision in no way limits or otherwise impacts the National Scheme Operator's authority described in Rule 2.1. Each Member agrees that the Standards are construed under, and governed by, the substantive laws of Libya without regard to conflicts-of-law provisions.

2.11 Scheme Right to Investigate and Audit

(Category A)

The National Scheme Operator reserves the right to conduct an examination or audit, including the right to conduct on-site visits, of any Member, and to require a Member to provide any reports or other information necessary to ensure full compliance with the Standards, Without prejudice of the provisions of the high-level regulation on supervision.

Any such examination or audit is at the expense of the Member, and a copy of the examination or audit results must be provided promptly to the National Scheme Operator upon request.

Further, the National Scheme Operator, at any time and whether or not a Member is subject to periodic examination or audit or other oversight by banking regulatory authorities, and at the Member's sole expense, has the right to require that Member to be subjected to an examination and/or audit and/or periodic examination and/or periodic audit by a firm

فقط في حالة اعتبار حدود المسؤولية المنصوص عليها في الفقرة السابقة مباشرة من قبل محكمة ذات اختصاص قضائي مخالفًا للقانون المعمول به، فإن المسؤولية الإجمالية، بشكل إجمالي، لمشغل شبكة الدفع المحلية تجاه عضو وأي شخص يدعي من قبل أو من خلال العضو، بالنسبة لأي وجميع المطالبات أو الخسائر أو التكاليف أو الأضرار، بما في ذلك أتعاب المحاماة والتكاليف وأتعاب الشهود الخبراء والتكاليف من أي نوع كانت أو نفقات المطالبات الناتجة عن أو بأي شكل من الأشكال المتعلقة بالأنظمة يجب ألا تتجاوز إجمالي التعويض الذي حصل عليه مشغل شبكة الدفع المحلية من العضو للاستخدام أو استلام الأنظمة خلال الـ 12 شهرًا المنتهية في التاريخ الذي تم فيه إبلاغ مشغل شبكة الدفع المحلية من قبل عضو عن الأنظمة أو المبلغ الإجمالي البالغ 4,319,775 دينار ليبي، أيهما أقل. من المقصود أن ينطبق هذا القيد على أي وجميع المسؤوليات أو سبب الدعوى مهما كان مزعومًا أو ناشئًا؛ إلى أقصى حد يسمح به القانون؛ ما لم يحظر القانون خلاف ذلك؛ وبغض النظر عن أي أحكام أخرى في المعايير.

لا يعد تقديم مدفوعات أو ائتمانات (لا تتطلبه المعايير) من قبل مشغل شبكة الدفع المحلية لصالح أحد الأعضاء على أنه تنازل أو تعديل لأي معيار من قبل مشغل شبكة الدفع المحلية. لا يجب أن يُفسر التراجع أو التأخير من قبل مشغل شبكة الدفع المحلية في تنفيذ أي معيار، أو ممارسة حقوقه المنصوص عليه، على أنه تنازل عن حقوقه، أو تنازل عن تنفيذ المعيار أو تعديل له، من قبل مشغل شبكة الدفع المحلية.

10.2 الولاية القانونية

القانون الليبي هو القانون الواجب التطبيق على جميع العلاقات التي تربط مشغل شبكة الدفع المحلية بالأعضاء، والمتعلقة بالأنشطة الرقمية وغير الرقمية. ويختص القضاء الليبي بالفصل في جميع المنازعات المتعلقة بمشغل شبكة الدفع المحلية.

ولا يحد هذا الحكم بأي شكل من الأشكال ولا يؤثر على سلطة مشغل شبكة الدفع المحلية الموضحة في القاعدة 2.1. ويقر كل عضو على أن المعايير يتم تفسيرها، بموجب القانون الليبي، بغض النظر عن أحكام تنازع القوانين.

11.2 حق النظام في التحقيق والتدقيق

(الفئة أ)

يحتفظ مشغل شبكة الدفع المحلية بالحق في إجراء عمليات الفحص والتدقيق، بما في ذلك القيام بالزيارات الميدانية للعضو، ومطالبته بتقديم التقارير أو معلومات أخرى ضرورية لضمان الامتثال الكامل للمعايير، ودون الإخلال بأحكام اللائحة الأعلى الخاصة بالرقابة.

وتكون تكاليف عملية الفحص والتدقيق على حساب نفقة العضو. ويجب تقديم نسخة من نتائج الفحص أو المراجعة إلى مشغل شبكة الدفع المحلية عند طلبه لها فوراً.

يجوز لمشغل شبكة الدفع المحلية ، في أي وقت، وحتى لو كان العضو يخضع لفحص دوري أو تدقيق أو رقابة أخرى من قبل السلطات التنظيمية المصرفية، وعلى نفقة العضو وحده، أن يطلب منه الخضوع لفحص دوري أو تدقيق أو رقابة آخر. قد يقوم بعملية الفحص أو المراجعة أو الفحص الدوري أو المراجعة

of independent certified accountants or by any other person or entity satisfactory to the National Scheme Operator.

A Member must not engage in any conduct that could or would impair the completeness, accuracy or objectivity of any aspect of such an examination or audit and must not engage in any conduct that could or would influence or undermine the independence, reliability or integrity of the examination or audit. A Member must cooperate fully and promptly in and with the examination or audit and must consent to unimpeded disclosure of information to the National Scheme Operator by the auditor.

2.12 Member Rights and Obligations

2.12.1 Fees Payment

(Category A)

Each member is considered responsible to timely pay to the National Payment Scheme and its' Operator all fees, charges, assessments and the like applicable to Activity as may be in effect from time to time, including those mentioned in the applicable National Scheme Operator billing manual.

If a Member does not timely pay the National Scheme Operator or any other person any amount due under the Standards, then the National Scheme Operator has the right, immediately and without providing prior notice to the Member, to assess and collect from that Member, on a current basis as the National Scheme Operator deems necessary or appropriate, such amount, as well as the actual attorneys' fees and other costs incurred by the National Scheme Operator in connection with any effort to collect such amount from that Member.

The National Scheme Operator has the right to assess and collect such amount at any time after the applicable amount becomes due, by any means available to the National Scheme Operator, which shall specifically include, by way of example and not limitation:

1. The taking or setoff of funds or other assets of the Member held by the National Scheme Operator;
2. The taking or setoff of funds from any account of the Member upon which the National Scheme Operator is authorized to draw;
3. The taking of funds being paid by the Member to any other Member; and
4. The taking of funds due to the Member from any other Member.

Each Member expressly authorizes the National Scheme Operator to take the Member's funds and other assets as authorized by this Rule, and to apply such funds and other assets to any obligation of the Member to the National Scheme Operator or any other person under the Standards, and no Member shall have any claim against the National Scheme Operator or any other person in respect of such conduct by the National Scheme Operator. Each Member agrees upon demand to promptly execute, acknowledge and deliver to the National Scheme Operator such instruments, agreements, lien waivers, releases, and other documents as the National Scheme Operator shall, from time to time, request in order to exercise its rights under this Rule.

الدورية من قبل محاسبين معتمدين مستقلين، أو من قبل شخص أو كيان آخر، يثق مشغل شبكة الدفع المحلية في قدراته على تنفيذ هذه العملية.

يجب على العضو أن لا يرتكب عملاً يكون من شأنه أن يؤثر على عملية الفحص والتدقيق أو موضوعيتها، أو يقوض عمل فرق الفحص والتدقيق، أو يؤثر في استقلاليتها أو نزاهتها. يجب على العضو أن يتعاون مع فريق الفحص أو المراجعة و أن يوافق على الكشف عن المعلومات دون عوائق، لفريق الفحص والتدقيق، المكلف من قبل مشغل شبكة الدفع المحلية.

12.2 حقوق الأعضاء والتزاماتهم

2.12.1 دفع الرسوم

(الفئة أ)

يلتزم كل عضو، في الوقت المحدد، بدفع جميع الرسوم والتكاليف المطلوبة منه من قبل مشغل شبكة الدفع المحلية والجهات التابع له، بما في ذلك الرسوم والتكاليف الأخرى المذكورة في دليل فوترة مشغل شبكة الدفع المحلية المعمول به.

وإذا أخل العضو بهذا الالتزام، كان لمشغل شبكة الدفع المحلية، أن يقوم فوراً، ودون تقديم إخطار مسبق إلى العضو، بعملية التقييم والتحصيل من ذلك العضو، من التاريخ الذي يحدده مشغل شبكة الدفع المحلية، مثال ذلك، تحصيل أتعاب المحاماة، والتكاليف الأخرى التي يتكبدها مشغل شبكة الدفع المحلية فيما يتعلق بأي جهد لجمع هذا المبلغ من ذلك العضو.

يجوز لمشغل شبكة الدفع المحلية تقييم وتحصيل هذا المبالغ مستحقة الأداء، وبأي وسيلة، والتي يجب أن تتضمن على وجه التحديد، على سبيل المثال وليس الحصر، الوسائل التالية:

1. أخذ أو مقاصة الأموال أو الأصول الأخرى للعضو التي يحتفظ بها مشغل شبكة الدفع المحلية.
2. سحب أو مقاصة الأموال من حسابات العضو والتي يجوز مشغل شبكة الدفع المحلية السحب منه.
3. أخذ الأموال التي يدفعها العضو إلى أي عضو آخر.
4. أخذ الأموال المستحقة للعضو من أي عضو آخر.

يلتزم كل عضو بأن يمنح صراحة مشغل شبكة الدفع المحلية تفويضاً بأخذ أموال العضو والأصول الأخرى، في الحالات التي يخل فيها العضو بالتزاماته المتعلقة بتطبيق هذه القاعدة، وتنطبق هذه القاعدة أيضاً على أي التزام للعضو تجاه مشغل شبكة الدفع المحلية أو أي شخص آخر بموجب المعايير، و لا يجوز للعضو أن يقوم برفع دعوى ضد مشغل شبكة الدفع المحلية أو أي شخص آخر فيما يتعلق بتطبيق هذه القاعدة من مشغل شبكة الدفع المحلية.

يلتزم كل عضو أن يقوم بشكل فوري بتقديم مثل هذه الأدوات والاتفاقيات وإعفاءات الامتياز والإصدارات والمستندات الأخرى التي يطلبها مشغل شبكة الدفع المحلية، من وقت لآخر، من أجل ممارسة حقوقه بموجب هذه القاعدة.

2.12.2 Taxes and Other Charges

(Category A)

Each Member must pay when due all taxes charged by any jurisdiction in which the Member conducts Activity with respect to such Activity. In the event the National Scheme Operator is charged taxes or other charges by jurisdiction as a result of or otherwise directly or indirectly attributable to Activity, the Member is obligated to reimburse the National Scheme Operator the amount of such taxes or other charges. The National Scheme Operator has the right to collect such taxes or other charges from the settlement account of the Member responsible in accordance with the Standards for the Activity that gave rise to the charge.

2.12.3 Transactions Responsibility

(Category A)

Each Bank is responsible to the National Scheme Operator and to all other Members for Transactions arising from the use of the BINs that the National Scheme Operator assigns to the Member, and for any Cards that the Member or any of its Sponsored Payment Service Providers, if any, has issued.

Banks must use BINs only in accordance with the Standards.

Neither a Bank nor any of its Sponsored Payment Service Providers is permitted to use the Bank's BINs to issue Cards or acquire Transactions other than as specified by the National Scheme Operator.

2.12.4 Unbiased—POS Transactions

(Category A)

A Member must not be biased against any Merchant with regard to processing and authorizing POS Transactions received.

2.12.5 Unbiased—ATM and Bank Branch Terminal Transactions

(Category A)

Pursuant to the Standards, each Member must:

1. Honor all valid Cards at each ATM and Bank Branch Terminal for which it is responsible, in a manner that is no less favorable than the manner in which it honors the cards of any other ATM network in which the Member participates; and
2. Acquire and process all valid Transactions in a manner that is no less favorable than the manner in which it acquires and processes transactions of any other ATM network in which the Member takes part.

Except as the Standards permit, a Member must not be biased against other Members of the National Scheme Operator as to any of the terms or conditions upon which it honors Cards or acquires or processes Transactions.

If an Acquirer is expressly permitted by the National Scheme Operator or local law to block the use of its ATMs to Cards issued by a Member, the Acquirer must display notifications accompanying the Marks on or near such ATMs informing the affected Cardholders that their Cards are not accepted.

2.12.2 الضرائب والرسوم الأخرى

(الفئة أ)

يلتزم كل عضو أن يقوم بدفع استحقاقاته من الضرائب التي تفرضها القوانين المعمول بها. في حالة فرض ضرائب أو رسوم أخرى على مشغل شبكة الدفع المحلية سواء كانت بشكل مباشر أو غير مباشر، يكون العضو ملزمًا بسداد مبلغ هذه الضرائب أو الرسوم الأخرى لمشغل شبكة الدفع المحلية. يجوز لمشغل شبكة الدفع المحلية تحصيل هذه الضرائب أو الرسوم الأخرى من حساب التسوية للعضو المسؤول وفقًا لمعايير النشاط الذي أدى إلى فرض الرسوم.

3.12.2 مسؤولية المعاملات

(الفئة أ)

يكون كل مصرف مسؤولاً أمام مشغل شبكة الدفع المحلية وتجاه جميع الأعضاء الآخرين عن المعاملات الناشئة عن استخدام أرقام التعريف المصرفية التي يخصصها مشغل شبكة الدفع المحلية للعضو، وعن بطاقات التي يقوم العضو أو مقدمي خدمة الدفع المكفولين بها.

يجب على المصارف استخدام أرقام التعريف المصرفية فقط وفقًا للمعايير.

لا يجوز للمصارف ولا لمقدمي خدمة الدفع المكفولين، استخدام أرقام التعريف المصرفية الخاصة بالمصارف لإصدار بطاقات أو الحصول على معاملات بخلاف ما هو محدد من قبل مشغل شبكة الدفع المحلية.

4.12.2 معاملات الحيادية لنقاط البيع

(الفئة أ)

يجب ألا يكون العضو متحيزًا ضد تاجر فيما يتعلق بمعالجة وتفويض معاملات نقاط البيع المستلمة.

5.12.2 المعاملات الحيادية لأجهزة الصراف الآلي وفروع المصرف

(الفئة أ)

وفقًا للمعايير، يجب على كل عضو:

1. إنشاء جميع البطاقات الصالحة في كل جهاز صراف آلي، ويكون المصرف أو فروعه مسؤولًا عنها، بطريقة لا تقل أهمية عن الطريقة التي تنشأ بها بطاقات شبكة الصراف آلي الأخرى التي يشارك فيها العضو.
2. الحصول على جميع المعاملات الصحيحة ومعالجتها بطريقة لا تقل أهمية عن الطريقة التي يكتسب بها ويعالج معاملات أي شبكة أخرى من أجهزة الصراف الآلي التي يشارك فيها العضو.

باستثناء ما تسمح به المعايير، يجب ألا يكون العضو متحيزًا ضد أعضاء آخرين في مشغل شبكة الدفع المحلية، فيما يتعلق بالشروط التي تنشأ بموجبها البطاقات أو تكتسب أو تعالج المعاملات.

إذا فوض القابل صراحةً من قبل مشغل شبكة الدفع المحلية أو أباح له ذلك القانون الليبي، حظر استخدام أجهزة الصراف الآلي الخاصة به للبطاقات الصادرة عن أحد الأعضاء، فيجب على القابل عرض الإشعارات المصاحبة للعلامات الموجودة على أجهزة الصراف الآلي أو بالقرب منها لإعلام حاملي البطاقات بأن بطاقاتهم محظورة.

2.12.6 Cooperation and Good Coexistences to Other Scheme Members and the National Scheme Operator

(Category C)

Upon request, each Member shall provide assistance to other Members, for example in the context of requests for information from government authorities and investigations of possible criminal or fraudulent activities.

A Member must fully cooperate with the National Scheme Operator and all other Members in the resolution of Cardholder and settlement disputes.

A Member, to the best of its ability, must provide requested investigative assistance to any other Member. Each Member shall respond to requests for assistance from other Members with the same degree of respect and promptness as it would itself wish to receive.

2.12.7 Prevention of Unjustifiable Enrichment

(Category A)

A Member must in particular cooperate with the National Scheme Operator to prevent or resolve any case of unjustifiable enrichment.

If a member has been unjustly enriched because of an error, the Member must reimburse the amount with which it has been enriched to the Member or Members that have suffered the corresponding loss. The National Scheme Operator has the right to resolve the unjust enrichment by debiting any excess amount received from the settlement account of the unjustly enriched Member and crediting such amount to the settlement account of the Member that should have received it. The National Scheme Operator will inform each Member in writing before debiting/crediting its settlement account.

2.12.8 Transaction Queries and Disputes

(Category A)

A Member must have the facilities and ensure the support of processes to handle Transaction queries, disputes, documentation requests, and chargebacks.

Each Member must comply with the dispute resolution rules, timeframes and procedures set out in chapter 3 in book 3 of the present rules.

2.13 Violations and Penalties - General

From time to time, the National Scheme Operator shall establish programs that address instances of noncompliance with particular Standards. Every instance of noncompliance with a Standard not addressed by such a program falls into at least one of the following three compliance categories.

Category A—Payment System Integrity

Category A noncompliance affects payment system integrity. The National Scheme Operator has the authority to impose monetary noncompliance assessments for Category A noncompliance. “Payment system integrity” violations include, but are not limited to, noncompliance involving License requirements, Merchant signing and monitoring requirements, unauthorized disclosure of the National Scheme Operator’s confidential information, and the protection of Card, Account, and Transaction information.

6.12.2 التعاون وحسن التعايش مع أعضاء النظام الآخرين ومشغل شبكة الدفع المحلية

(الفئة ج)

بناءً على الطلب، يجب على كل عضو تقديم المساعدة للأعضاء الآخرين، على سبيل المثال في مجال طلبات الحصول على المعلومات من السلطات الحكومية والتحقيقات في الأنشطة الإجرامية أو الاحتمالية المحتملة.

يلتزم كل عضو بأن يتعاون بشكل كامل مع مشغل شبكة الدفع المحلية، وجميع الأعضاء الآخرين في تسوية المنازعات مع حاملي البطاقات.

يلتزم كل عضو، وفي حدود قدراته، بتقديم المساعدة في التحقيق مع عضو آخر. يجب على كل عضو أن يستجيب لطلبات المساعدة من الأعضاء الآخرين بنفس الدرجة والسرعة التي يرغب هو نفسه في تلقيها.

7.12.2 منع الإثراء غير المشروع

(الفئة أ)

يجب على العضو أن يتعاون بشكل خاص مع مشغل شبكة الدفع المحلية لمنع الوقوع في حالات الإثراء غير المشروع.

وإذا تم إثراء العضو بشكل غير مشروع، يجب على العضو سداد المبلغ الذي تم إثراءه به إلى العضو أو الأعضاء الذين لحقهم الافتقار. يجوز لمشغل شبكة الدفع المحلية تسوية حالة الإثراء غير المشروع عن طريق خصم أي مبلغ فائض يتم استلامه من حساب التسوية الخاص بالعضو الذي تم إثرائه بشكل غير مشروع، وإيداع هذا المبلغ في حساب التسوية الخاص بالعضو الذي كان ينبغي أن يحصل عليه. سيقوم مشغل شبكة الدفع المحلية بإبلاغ كل عضو كتابيًا قبل الخصم و الإيداع في حساب التسوية الخاص به.

8.12.2 الاستفسارات والنزاعات الخاصة بالمعاملات

يجب أن يمتلك العضو التسهيلات، ويضمن دعم العمليات للتعامل مع استفسارات المعاملات والمنازعات وطلبات التوثيق وعمليات رد المبالغ المدفوعة.

يجب على كل عضو الامتثال لقواعد تسوية المنازعات والمواعيد الزمنية والإجراءات المنصوص عليها في الفصل 3 في الكتاب 3 من هذه القواعد.

13.2 المخالفات والجزاءات العامة

يلتزم مشغل شبكة الدفع المحلية، وبشكل دوري، بإنشاء برامج تعالج حالات عدم الامتثال لمعايير معينة. تقع كل حالة من حالات عدم الامتثال لمعيار لم يتم تناولها بواسطة مثل هذا البرنامج في واحدة على الأقل من فئات الامتثال الثلاث التالية.

(الفئة أ) - سلامة نظام الدفع

يؤثر عدم الامتثال من (الفئة أ) على سلامة نظام الدفع. يتمتع مشغل شبكة الدفع المحلية بسلطة فرض تقييمات عدم الامتثال النقدية لعدم الامتثال من (الفئة أ). تشمل انتهاكات “سلامة نظام الدفع”، على سبيل المثال، عدم الامتثال الذي يتضمن قواعد الترخيص، وقواعد توقيع التاجر ومراقبته،

Category B—Visible to Customers

Category B noncompliance addresses conduct that is visible to Cardholders or Merchants. The National Scheme Operator has the authority to impose monetary noncompliance assessments for Category B noncompliance or, in the alternative, is permitted to provide notice and a limited time to cure such noncompliance before imposing monetary assessments. “Visible to Customers” violations include, but are not limited to, noncompliance involving the use of the Marks, the selective authorization of Transactions, identification of the Merchant at the POI, merchant surcharging, the setting of minimum and maximum Transaction amounts, the payment of Merchants and Sub-merchants for Transactions, Transaction receipt requirements, and ATM Access Fee notices.

Category C—Efficiency and Operational Performance

Category C noncompliance addresses efficiency and operational performance. The National Scheme Operator has the authority to impose monetary noncompliance assessments for Category C noncompliance or, in the alternative, provide notice and a limited time to cure such noncompliance before imposing monetary assessments. “Efficiency and operational performance” violations include, but are not limited to, noncompliance involving presentment of Transactions within the required time frame, supplying Merchants with materials required for Transaction processing, Card capture at the ATM, excessive authorization declines, Card fees and reporting procedures, and the obligation to provide the National Scheme Operator with the requested information.

2.14 Violations and Penalties - Process

The following schedule pertains to any Standard that does not have an established compliance program. subject to CBL approval The National Scheme Operator has the right to deviate from this schedule at any time.

In the below table, all days refer to calendar days and violations of a Standard are tracked on a rolling 12-month basis.

(See Appendix number 6)

The activation of the fees mentioned in the table above is subject to CBL directions

2.15 Persistent and Intentional Violations

The National Scheme Operator has the right to consider the nature, willfulness, number and frequency of occurrences and possible consequences resulting from a failure to comply with any Standard when it determines the measures to be taken to address a violation.

2.16 Certification of Compliance

(Category C)

A senior executive officer of each Member must, if requested by the National Scheme Operator, promptly certify in writing to the National Scheme Operator the status of compliance or noncompliance with any Standard by the Member or by any of its Sponsored Payment Service Providers.

2.17 Appeals

A Member may request that the designated officer of the National Scheme Operator review an assessment imposed by the National Scheme Operator for noncompliance with a Standard. Such a request must be submitted in writing and signed by the Member’s

والكشف غير المرفص به عن المعلومات السرية لمشغل شبكة الدفع المحلية، وحماية معلومات البطاقات، والحساب والمعاملات.

(الفئة ب) – ما هو ظاهر للعملاء

يؤثر عدم الامتثال من (الفئة ب) على السلوك الظاهر لحاملي البطاقات أو التجار. حيث يتمتع مشغل شبكة الدفع المحلية بسلطة فرض تقديرات عدم الامتثال النقدي لعدم الامتثال من (الفئة ب). ويجوز له أن يكفي بتقديم إشعار، وإلزام العضو خلال وقت محدود لمعالجة عدم الامتثال، هذا قبل فرض التقديرات النقدية. تشمل الأخطاء “الظاهرة للعملاء”، على سبيل المثال، عدم الامتثال الذي يتضمن استخدام العلامات، والتفويض الانتقائي للمعاملات، وتحديد التاجر في POI، والرسوم الإضافية للتاجر، وتحديد الحد الأدنى والحد الأقصى لمبالغ المعاملات، ودفع التجار والتجار من الباطن للمعاملات، ومتطلبات إيصال المعاملات، وإشعارات رسوم الوصول إلى أجهزة الصراف الآلي.

(الفئة ج) - الكفاءة والأداء التشغيلي:

يرتبط عدم الامتثال (للفئة ج) مع الكفاءة التشغيلية وجودة الأداء. وعليه، يتمتع مشغل شبكة الدفع المحلية بسلطة فرض غرامات مالية في حالة عدم الامتثال لهذه الفئة، ويجوز له بدلا من ذلك، الاكتفاء بتقديم إشعار وتعهد محدد المدة لمعالجة حالة عدم الامتثال قبل فرض الغرامات المالية. “الكفاءة وجودة الأداء التشغيلي” يشمل خرق الأداء، على سبيل المثال لا الحصر، عدم الامتثال الذي يتضمن تشغيل المعاملات ضمن الوقت الزمني المحدد، وتزويد التجار بالمواد المطلوبة لمعالجة المعاملات، وحمل البطاقة في أجهزة الصراف الآلي، ورسوم البطاقة وإجراءات الإبلاغ، والالتزام بتزويد مشغل شبكة الدفع المحلية بالمعلومات المطلوبة.

14.2 المخالفات والعقوبات - العملية

يتعلق الجدول التالي بأي معيار لا يحتوي على برنامج امتثال محدد. رهنآ بموافقة مصرف ليبيا المركزي يجوز مشغل شبكة الدفع المحلية الخروج عن هذا الجدول في أي وقت.

في الجدول أدناه، تشير جميع الأيام إلى أيام التقويم الميلادي، ويتم تتبع الإخلال بالمعيار على أساس 12 شهراً تتجدد تلقائياً.

(انظر الملحق رقم 6)

تفعيل الرسوم المذكورة في الجدول أعلاه تخضع لتوجيهات مصرف ليبيا المركزي.

15.2 المخالفات المستمرة والمتعمدة

لمشغل شبكة الدفع المحلية ، عندما يحدد التدابير التي يتعين اتخاذها لمعالجة آثار عدم الامتثال، أن يأخذ في الاعتبار طبيعة وقصد وعدد وتكرار المخالفات والعواقب المحتملة الناتجة عن عدم الامتثال لأي معيار.

16.2 شهادة الامتثال

(الفئة ج)

يجب على رئيس مجلس إدارة لكل العضو، إذا طلب منه مشغل شبكة الدفع المحلية، أن يقدم إفادته إليه عن حالة الامتثال أو عدم الامتثال لأي معيار من قبل العضو أو من قبل مقدمي خدمة الدفع المكفول.

17.2 الاستئناف

principal contact. The request must be postmarked no later than 30 days after the date of the disputed assessment.

The National Scheme Operator has the right to assess a fee to consider and act on a request for review of a noncompliance assessment.

2.18 Resolution of Appeal

When a Member requests review of an assessment for noncompliance with a Standard, the designated officer of the National Scheme Operator has the right to take such action as he or she deems necessary or appropriate, or may elect not to act. The designated officer has the right to delegate authority to act or not to act with respect to any particular matter or type of matter.

If the designated officer or his or her designee elects to conduct further inquiry into the matter, each Member must cooperate promptly and fully. If the designated officer or his or her designee makes a recommendation of action to resolve the matter, such recommendation is final and not subject to further review or other action.

2.19 Provision and Use of Information

The following sections relate to the provision and use of information.

2.19.1 Member Obligation to Provide Data

(Category C)

Upon request by the National Scheme Operator, and subject to applicable law or regulation, a Member must complete and timely deliver Member Reports to the National Scheme Operator or to the National Scheme Operator's designee, provided that compliance with the foregoing obligation does not require a Member to furnish any information, the disclosure of which, in the opinion of this National Scheme Operator's legal counsel, is likely to create a significant potential legal risk to this National Scheme Operator and/or its Members. To the extent that a Member is obligated to provide a Member Report to the National Scheme Operator that the Member deems to disclose proprietary information of the Member, such information will be treated by the National Scheme Operator with the degree of care deemed appropriate by the National Scheme Operator to maintain its confidentiality.

As an example of a Member Report, each Acquirer must provide Transaction Data to the National Scheme Operator in such form and manner as the National Scheme Operator may require. As used herein, "Transaction Data" means any data and/or data element or sub element that the Standards require to be used to authorize, clear and/or settle a Transaction (whether authorized, cleared and/or settled via the Network or otherwise) or that the National Scheme Operator requires to be provided.

Each Member must provide the National Scheme Operator with current Member contact information for itself and on behalf of its Sponsored Payment Service Providers, including mailing addresses, air express/hand delivery addresses, telephone numbers, fax numbers, and email addresses.

2.19.2 Confidential Information of Members

The National Scheme Operator and its parents, subsidiaries and Payment Service Providers (herein collectively referred to as National Scheme Operator) has the right to use and

يجوز للعضو أن يطلب من المسؤول المكلف من قبل مشغل شبكة الدفع المحلية، مراجعة التقييم الذي يفرضه مشغل شبكة الدفع المحلية لعدم الامتثال للمعيار. ويجب أن يقدم هذا الطلب كتابةً وموقعًا من جهة الاتصال الرئيسية للعضو. وأن يكون مرسلاً عن طريق البريد مصحوباً بعلم الوصول في موعد لا يتجاوز 30 يومًا من تاريخ التقييم المتنازع عليه.

وفي جميع الأحوال، يحق لمشغل شبكة الدفع المحلية تقييم الرسوم للنظر في طلب مراجعة تقييم عدم الامتثال والتصرف بناءً عليه.

18.2 قرار الاستئناف

عندما يطلب أحد الأعضاء مراجعة تقييم عدم الامتثال للمعايير، يجوز للشخص المكلف من مشغل شبكة الدفع المحلية اتخاذ الإجراءات الذي يراها مناسبة. وللشخص المكلف الحق في تفويض سلطة التصرف أو عدم التصرف فيما يتعلق بأي مسألة أو نوع معين من المسائل.

إذا قدر الشخص المكلف أو نائبه إجراء مزيداً من التحقيق في هذه المسألة، فإن يجب على كل عضو التعاون معه مباشرة. إذا قدم الشخص المكلف أو نائبه توصية باتخاذ إجراءات لمعالجة حالة عدم الامتثال، فإنها تعد توصية نهائية، ولا تخضع لمزيد من المراجعة.

19.2 توفير واستخدام المعلومات

تتعلق الأقسام التالية بتوفير المعلومات واستخدامها.

1.19.2 التزام العضو بتوفير البيانات

(الفئة ج)

بناءً على طلب مشغل شبكة الدفع المحلية، ووفقاً للقانون أو اللوائح المعمول بها، يجب على العضو إكمال تقارير العضوية وتسليمها في الوقت المحدد إلى مشغل شبكة الدفع المحلية أو من ينوب عنه، شريطة أن الامتثال للالتزام السابق لا يتطلب وجود عضو لتقديم أي معلومات، من المحتمل أن يؤدي الكشف عنها، في رأي المستشار القانوني لمشغل شبكة الدفع المحلية، إلى حدوث مخاطر قانونية محتملة كبيرة له، أو لأعضائه. إلى الحد الذي يكون فيه العضو ملزماً بتقديم تقرير إلى مشغل شبكة الدفع المحلية الذي يرى فيه العضو أنه يكشف عن معلومات ملكية خاصة بالعضو، فسوف يتم التعامل مع هذه المعلومات من قبل مشغل شبكة الدفع المحلية بدرجة العناية التي يراها مشغل شبكة الدفع المحلية مناسبة للحفاظ على سريته.

ومن أمثلة هذه التقارير، أنه يجب على كل قابل تقديم بيانات المعاملة إلى مشغل شبكة الدفع المحلية بالشكل والطريقة التي قد يطلبها مشغل شبكة الدفع المحلية. كما هو مستخدم هنا، تعني "بيانات المعاملة" أي بيانات أو عنصر بيانات أو عنصر فرعي تتطلب المعايير استخدامه لتفويض أو مسح أو تسوية معاملة (سواء كانت مصرح بها أو تمت الموافقة عليها أو تمت تسويتها عبر الشبكة أو غير ذلك) أو أن مشغل شبكة الدفع المحلية يطلب توفيره.

يجب على كل عضو تزويد مشغل شبكة الدفع المحلية بمعلومات اتصال العضو الحالية له، وبالنيابة عن مقدمي خدمة الدفع المكفولين، بما في ذلك عناوين البريد وعناوين التسليم السريع الجوي/ اليدوي وأرقام الهواتف وأرقام الفاكس وعناوين البريد الإلكتروني.

2.19.2 المعلومات السرية للأعضاء

disclose both Confidential Information and Confidential Transaction Data in compliance with applicable law and as provided herein.

The National Scheme Operator has the right to use or disclose Confidential Information and Confidential Transaction Data only as follows:

1. For the benefit of the Member supplying the information to support the Member's Program and/or Activities;
2. As may be appropriate to the National Scheme Operator's staff, accountants, auditors, or counsel;
3. As may be required or requested by any judicial process or governmental agency having or claiming jurisdiction over the National Scheme Operator;
4. As required for processing Transactions, including authorization, clearing, and settlement;
5. For accounting, auditing, billing, reconciliation, and collection activities;
6. For the purpose of processing and/or resolving chargebacks or other disputes;
7. For the purpose of protecting against or preventing actual or potential fraud, unauthorized transactions, claims, or other liability, including to third parties providing these services;
8. For the purpose of managing risk exposures, franchise quality, and compliance with the Standards;
9. For the purpose of providing products or services to Members or other third parties, except that any Confidential Transaction Data provided in such products or services will only be provided to a Member and will consist solely of Confidential Transaction Data provided to the National Scheme Operator by that Member;
10. For the purpose of administering sweepstakes, contests, or other marketing promotions;
11. For preparing internal reports for use by the National Scheme Operator's staff, management, and consultants for the purposes of operating, evaluating, and managing National Scheme Operator business;
12. For preparing and furnishing compilations, analyses, and other reports of aggregated information, and anonymizing Confidential Information and/or Confidential Transaction Data, provided that such compilations, analyses, or other reports do not identify any (i) Member other than the Member for which the National Scheme Operator prepares the compilation, analysis, or other report or (ii) Cardholder whose Transactions were involved in the preparation of any such compilation, analysis, or other report;
13. For the purpose of complying with applicable legal requirements; or
14. For other purposes for which consent has been provided by the individual to whom the Confidential Information and/or Confidential Transaction Data relates.

Each Member must ensure that it complies with the Standards and applicable laws and regulations in connection with disclosing any Confidential Transaction Data or Confidential Information to the National Scheme Operator to allow the uses and disclosures described herein, including any laws and regulations requiring the Member to provide notices to individuals about information practices or to obtain consent from individuals to such practices.

A Member must provide Confidential Transaction Data to the National Scheme Operator or through the National Scheme Operator's processes or systems solely as prescribed by the Standards or as otherwise required by the National Scheme Operator or applicable law. For example, an Account PAN or Token, when provided through the Network, must be submitted in accordance with the technical specifications or other Standards pertaining to the Network or a component thereof.

يجوز لمشغل شبكة الدفع المحلية، وشركته الام والشركات الفرعية ومقدمي خدمات الدفع (يشار إليهم مجتمعة باسم مشغل شبكة الدفع المحلية) استخدام وكشف كل من المعلومات السرية وبيانات المعاملات السرية بما يتوافق مع القانون المعمول به وكما هو منصوص عليه في هذه الوثيقة.

يجوز لمشغل شبكة الدفع المحلية استخدام أو الكشف عن المعلومات السرية وبيانات المعاملات السرية فقط على النحو التالي:

1. لصالح العضو الذي يقدم المعلومات لدعم برنامج العضو أو أنشطته.
2. لموظفي مشغل شبكة الدفع المحلية أو المحاسبين أو المراجعين أو المستشارين.
3. إذا كانت مطلوبة من قبل جهة تحقيق قضائي، أو من جهة حكومية لديها سلطة على مشغل شبكة الدفع المحلية.
4. إذا كانت مطلوبة لمعالجة المعاملات، بما في ذلك التفويض والمقاصة والتسوية.
5. لأنشطة المحاسبة والمراجعة والفواتير والتسوية والتحويل.
6. لغرض معالجة أو حل عمليات رد المبالغ المدفوعة أو النزاعات الأخرى.
7. لغرض الحماية من عمليات الاحتيال أو منعها أو المعاملات غير المصرح بها أو المطالبات أو المسؤولية الأخرى، بما في ذلك الأطراف الثالثة التي تقدم هذه الخدمات.
8. لغرض إدارة الوقاية من المخاطر، وجودة الامتياز، والامتثال للمعايير.
9. لغرض توفير المنتجات أو الخدمات للأعضاء أو لأطراف ثالثة أخرى، باستثناء أن بيانات المعاملات السرية التي يتم توفيرها في هذه المنتجات أو الخدمات، لن يتم تقديمها إلا إلى العضو وتتكون فقط من بيانات المعاملات السرية المقدمة إلى مشغل شبكة الدفع المحلية بواسطة ذلك العضو.
10. لغرض إدارة المسابقات أو العروض الترويجية الأخرى للتسويق.
11. لإعداد التقارير الداخلية لاستخدامها من قبل موظفي مشغل شبكة الدفع المحلية والإدارة والاستشاريين لأغراض تشغيل وتقييم وإدارة أعمال مشغل شبكة الدفع المحلية.
12. لإعداد وتقديم التقارير التجميعية والتحليلية، والتقارير الأخرى للمعلومات المجمعة وإخفاء هوية المعلومات السرية أو بيانات المعاملات السرية، شريطة ألا تحدد هذه التجميعات أو التحليلات أو التقارير الأخرى أي (1) عضو آخر غير العضو الذي من أجله يُعد مشغل شبكة الدفع المحلية التجميع أو التحليل أو أي تقرير آخر أو (2) حامل البطاقة الذي شاركت معاملاته في إعداد أي تقرير من هذا القبيل أو تحليل أو أي تقرير آخر.
13. لغرض الامتثال للقواعد، والمعايير القانونية المعمول بها.
14. للأغراض الأخرى التي تم تقديم الموافقة من قبل الشخص الذي تتعلق به المعلومات السرية أو بيانات المعاملة السرية.

يجب على كل عضو التحقق من امتثاله للمعايير والقوانين واللوائح المعمول بها فيما يتعلق بالكشف عن بيانات المعاملات السرية، أو المعلومات السرية لمشغل شبكة الدفع المحلية للسماح بالاستخدامات والإفصاحات الموضحة هنا، بما في ذلك القوانين واللوائح التي تتطلب من العضو تقديم إخطارات للأشخاص حول ممارسات المعلومات أو للحصول على موافقة من الأفراد على هذه الممارسات.

يلتزم العضو بتقديم بيانات المعاملة السرية إلى مشغل شبكة الدفع المحلية، وعلى النحو المنصوص عليه في المعايير من قبل مشغل شبكة الدفع المحلية أو القانون المعمول به. على سبيل المثال، يجب تقديم رمز الحساب أو رقم الحساب الأساسي، عند توفيره من خلال الشبكة، وفقاً للمواصفات الفنية أو المعايير الأخرى المتعلقة بالشبكة أو أحد مكوناتها.

3.19.2 استخدام الأعضاء لمعلومات النظام

لا يتحمل مشغل شبكة الدفع المحلية أي مسؤولية عن دقة أو اكتمال أو حسن توقيت أي معلومات

2.19.3 Member Use of Scheme Information

The National Scheme Operator is not responsible for and disclaims any responsibility for the accuracy, completeness, or timeliness of any information disclosed by the National Scheme Operator to a Member; and the National Scheme Operator makes no warranty, express or implied, including, but not limited to, any warranty of merchantability or fitness for any particular purpose with respect to any information disclosed by or on behalf of the National Scheme Operator to any Member or disclosed directly or indirectly to any participant in a Member's Activity. Each Member assumes all risk of use of any information disclosed directly or indirectly to a Member or to any participant in a Member's Activity by or on behalf of the National Scheme Operator.

2.19.4 Confidentiality of Scheme Information

(Category A)

A Member must not disclose confidential information of the National Scheme Operator or its parents, subsidiaries, and Payment Service Providers (herein collectively referred to as the National Scheme Operator) except:

1. On a need-to-know basis to the Member's staff, accountants, auditors, or legal counsel subject to standard confidentiality restrictions, or
2. As may be required by any court process or governmental agency having or claiming jurisdiction over the Member, in which event the Member must promptly provide written notice of such requirement to the designated officer of the National Scheme Operator, and to the extent possible, the Member must seek confidential treatment by the court or agency.

A Member has the right to use confidential or proprietary information and/or trade secrets of the National Scheme Operator solely for the purpose of carrying out the Member's Activities.

2.20 Data Security

(Category A)

In the Data Security Section, the following terms have the meanings set forth in the definition section presented in this document.

Applicable Data Protection Law, Data Subject, Organization, Personal Data, Processing of Personal Data and Transaction-related Personal Data

2.20.1 Processing of Transaction-Related Personal Data

A Member who collects, uses or discloses Transaction-related Personal Data in Libya must comply with the Applicable Data Protection Law. A Member is the Organization responsible for complying with the Applicable Data Protection Law in respect of the collection, use and disclosure of Personal Data, including the transfer of Personal Data outside Libya, for the purposes of authorizing, recording, clearing and settling transactions, and the National Scheme Operator acts as an entity that processes Personal Data on behalf of the Member for these purposes. The National Scheme Operator will only undertake Processing of Personal Data in accordance with the Member's instructions and the Standards and will comply with security obligations equivalent to those imposed on the Members under the Applicable Data Protection Law, and such other obligations as applicable to the National Scheme Operator under the Applicable Data Protection Law.

يتم الكشف عنها من قبله للعضو؛ ولا يقدم مشغل شبكة الدفع المحلية أي ضمان، صريحًا أو ضمنيًا، بما في ذلك، على سبيل المثال، أي ضمان للتسويق أو الملاءمة لأي غرض معين فيما يتعلق بأي معلومات يتم الكشف عنها من قبله أو نيابة عنه لأي عضو أو تم الكشف عنها بشكل مباشر أو غير مباشر لأي مشارك في نشاط العضو. يتحمل كل عضو جميع مخاطر استخدام أي معلومات يتم الكشف عنها بشكل مباشر أو غير مباشر لعضو أو لأي مشارك في نشاط عضو من قبل مشغل شبكة الدفع المحلية.

4.19.2 سرية معلومات النظام

(الفئة أ)

يلتزم العضو بعدم الكشف عن المعلومات السرية لمشغل شبكة الدفع المحلية أو نائبه أو الشركات التابعة له ومقدمي خدمات الدفع (يشار إليهم مجتمعة باسم مشغل شبكة الدفع المحلية) باستثناء:

1. المعلومات والبيانات التي يجب لموظفي العضو أو المحاسبين أو المراجعين أو المستشارين القانونيين الخاضعين لقيود السرية معرفتها.
2. إذا كانت مطلوبة من جهة تحقيق قضائي، وفي هذه الحالة يجب على العضو تقديم إشعار كتابي على الفور بذلك لمشغل شبكة الدفع المحلية.

يحق للعضو استخدام المعلومات السرية أو المسجلة، أما حق الملكية أو الأسرار التجارية فهو حق يتمتع به فقط مشغل شبكة الدفع المحلية لغرض تنفيذ أنشطة العضو.

20.2 أمن البيانات

(الفئة أ)

في قسم أمن البيانات، تحمل المصطلحات التالية المعاني الموضحة في قسم التعريف الوارد في هذا المستند.

قانون حماية البيانات المعمول به، وموضوع البيانات، والمنظمة، والبيانات الشخصية، ومعالجة البيانات الشخصية والبيانات الشخصية المتعلقة بالمعاملات.

1.20.2 معالجة البيانات الشخصية ذات الصلة بالمعاملات

يجب على العضو الذي يجمع البيانات الشخصية المتعلقة بالمعاملات في ليبيا، أو يستخدمها أو يكشف عنها الامتثال لقانون حماية البيانات المعمول به. العضو هو المؤسسة المسؤولة عن الامتثال لقانون حماية البيانات المعمول به فيما يتعلق بجمع البيانات الشخصية واستخدامها والإفصاح عنها، بما في ذلك نقل البيانات الشخصية خارج ليبيا، لأغراض التفويض والتسجيل والمسح وتسوية المعاملات، و يعمل مشغل شبكة الدفع المحلية كمؤسسة تقوم بمعالجة البيانات الشخصية نيابة عن العضو لهذه الأغراض. يتولى مشغل شبكة الدفع المحلية فقط معالجة البيانات الشخصية وفقًا لتعليمات العضو والمعايير، وسوف يمثل للالتزامات الأمنية المفروضة على الأعضاء بموجب قانون حماية البيانات المعمول به، ومثل هذه الالتزامات الأخرى التي تنطبق على مشغل شبكة الدفع المحلية بموجب

2.20.2 Data Subject Notice and Consent

A Member must ensure that Data Subjects are properly informed and, if necessary, have given proper consent in accordance with the Applicable Data Protection Law that Personal Data relating to them may be collected, used or disclosed by the applicable Member and the National Scheme Operator as set forth for the purposes provided for.

2.20.3 Data Subject Access to Personal Data

In accordance with the Applicable Data Protection Law, a member must develop and implement appropriate procedures for handling requests by Data Subjects for access to and/or correction of Personal Data maintained by the applicable Member or the National Scheme Operator. The National Scheme Operator will cooperate with a Member in responding to such requests and will provide access to Personal Data maintained by the National Scheme Operator where appropriate.

If an access request is made directly to the National Scheme Operator, a Member must cooperate with the National Scheme Operator in promptly responding to the request.

2.20.4 Integrity of Personal Data

Each Member must take reasonable steps to ensure that Personal Data which the Member provides to the National Scheme Operator is accurate, complete and current.

2.21 Quarterly Submitted Report

(Category C)

Each Member must complete and timely deliver to the National Scheme Operator the Quarterly Submitted Report in the manner and at such time as the National Scheme Operator requires.

Report Forms provided in Book1 Annex1.

2.21.1 Report Not Received

If the National Scheme Operator does not receive a member's properly completed Quarterly Submitted Report questionnaire when and how due, the National Scheme Operator has the right to:

1. Impose on the Member, after review of the Member's last correctly submitted Quarterly Submitted Report questionnaire and assessment paid, an assessment equal to, or greater than, the Member's assessment for such calendar quarter;
2. Impose on the Member a noncompliance assessment;
3. If the Member's actual payment based on the Quarterly Submitted Report questionnaire submitted by the Member, compared with the National Scheme Operator's estimate of payment due, results in an underpayment by the Member, collect the amount of the underpayment due and impose an interest penalty of the lower of two percent per month or the highest rate permitted by law, from the date the payment was first due through the date on which the additional amount due is paid;
4. If the Member's actual payment based on the Quarterly Submitted Report questionnaire submitted by the Member compared with the National Scheme Operator's estimate of payment due results in an overpayment by the Member, return the amount of the overpayment, without interest or penalty thereon, as soon as practicable after the overpayment amount is identified and calculated; and
5. Collect the assessment amount and any penalty and interest due thereon.

قانون حماية البيانات المعمول به.

2.20.2 إشعار وموافقة موضوع البيانات

يجب على العضو التحقق من أن موضوع البيانات قد تم إبلاغه بشكل صحيح ، وإذا لزم الأمر، قد أعطى الموافقة المناسبة وفقًا لقانون حماية البيانات المعمول به على أنه يمكن جمع البيانات الشخصية المتعلقة بهم أو استخدامها أو الكشف عنها من قبل العضو المعني ومشغل شبكة الدفع المحلية المنصوص عليها للغرض المخصص له.

3.20.2 وصول موضوع البيانات إلى البيانات الشخصية

وفقًا لقانون حماية البيانات المعمول به ، يجب على العضو تطوير وتنفيذ الإجراءات المناسبة للتعامل مع الطلبات المقدمة من أصحاب البيانات للوصول إلى أو تصحيح البيانات الشخصية التي يحتفظ بها العضو المعني أو مشغل شبكة الدفع المحلية. ويجب على مشغل شبكة الدفع المحلية أن يتعاون مع الأعضاء في الاستجابة لمثل هذه الطلبات وسيوفر الوصول إلى البيانات الشخصية التي يحتفظ بها مشغل شبكة الدفع المحلية عند الاقتضاء.

إذا تم تقديم طلب وصول مباشرة إلى مشغل شبكة الدفع المحلية، يجب على العضو التعاون مع مشغل شبكة الدفع المحلية في الاستجابة السريعة للطلب.

4.20.2 سلامة البيانات الشخصية

يلتزم كل عضو ببذل الجهود المعقولة للتحقق من أن البيانات الشخصية التي يقدمها العضو لمشغل شبكة الدفع المحلية دقيقة وكاملة وحديثة.

21.2 تقرير مقدم ربع سنوي

(الفئة ج)

يلتزم كل عضو باستكمال التقرير ربع السنوي المقدم لمشغل شبكة الدفع المحلية وفي الوقت المحدد، بالطريقة التي يطلبها مشغل شبكة الدفع المحلية. نماذج التقارير الواردة في الكتاب 1 الملحق 1.

1.21.2 تقارير التي لم يتم استلامها

إذا لم يستلم مشغل شبكة الدفع المحلية استبيانًا عن التقرير ربع السنوي المقدم من أحد الأعضاء بشكل صحيح عند الاستحقاق، يجوز لمشغل شبكة الدفع المحلية ما يلي:

1. فرض تقييم على العضو، بعد مراجعة آخر استبيان للتقرير ربع السنوي مقدم بشكل صحيح من العضو وتقديم التقييم المدفوع، وهو تقييم يساوي أو يزيد عن تقييم العضو لهذا الربع من التقويم.
2. فرض تقييم عدم الامتثال على العضو.
3. إذا كان الدفع الفعلي للعضو بناءً على استبيان التقرير ربع السنوي المقدم من العضو، مقارنة بتقدير مشغل شبكة الدفع المحلية للدفعات المستحقة، ينتج عنه دفع أقل من قبل العضو، وتحصيل مبلغ الدفعة الناقصة المستحقة وفرض غرامة فائدة أقل من اثنين في المائة شهريًا أو أعلى معدل يسمح به القانون، (القانون الليبي يبطل التعامل بالفوائد) من تاريخ استحقاق الدفعة لأول مرة حتى تاريخ دفع المبلغ الإضافي المستحق.
4. إذا نتج عن الدفع الفعلي للعضو بناءً على استبيان التقرير ربع السنوي المقدم من العضو مقارنة بتقدير مشغل شبكة الدفع المحلية للدفعات المستحقة دفع العضو دفعة زائدة، فرد مبلغ الدفعة الزائدة بدون فوائد أو غرامة عليها، على النحو التالي: في أقرب وقت ممكن عمليًا بعد تحديد مبلغ

2.21.2 Incomplete or Erroneous Reports

If a member submits an erroneous or incomplete Quarter Submitted Report, the National Scheme Operator has the right to:

1. Impose on the Member, after review of the Member's last correctly submitted Quarter Reports and assessments paid thereon, an assessment equal to, or greater than, the Member's last properly paid assessment for each calendar quarter for which it submitted an erroneous or incomplete Quarterly Submitted Report;
2. Impose on the Member a noncompliance assessment;
3. the National Scheme Operator's estimate of payment due results in an underpayment by the Member, collect the amount of the underpayment due and impose an interest penalty of the lower of two percent per month or the highest rate permitted by law, from the date the payment was first due and payable through the date on which the additional amount due is paid;
4. If the National Scheme Operator's estimate of payment due results in an overpayment by the Member, return the amount of the overpayment, without penalty or interest thereon, as soon as practicable after the overpayment amount is identified and calculated; and
5. Collect the assessment amount and any penalty and interest due thereon from the Member's settlement account.

2.21.3 Overpayment Claim/Refund of Fees

After the Member delivers a completed Member Report to the National Scheme Operator, the Member has the right to submit a claim asserting an overpayment thereon. The National Scheme Operator may review such claim if the claim is received by the National Scheme Operator no later than one calendar quarter after the date of the purported overpayment. If the National Scheme Operator substantiates the Member's overpayment claim, the National Scheme Operator will return the amount of the overpayment to the Member as soon as practicable, without interest or penalty thereon.

2.22 Transaction Requirements

(Category A)

In accordance with the Standards, each Member must comply with each of the following requirements.

1. Accept and present to the Issuer records of Transactions arising from the use of a Card issued by any other Member at any POI location that the Member has authorized to accept Cards;
2. Accept and pay for Transactions received from another Member arising from the use of any Card issued by it. If an Payment Service Provider ceases to be Sponsored by a Member , the Member remains obligated to other Members to accept and pay for Transactions arising from the use of Cards issued by that Payment Service Provider;
3. Maintain a functional 24-hour-per-day operating connection to the Network, either directly or by means of a Service Provider operating on its behalf, and not force any other Member wishing to operate multilaterally using the Network into bilateral agreements;
4. Provide valid, accurate, complete, unaltered, and consistent data in all authorization and clearing Transaction messages.

الدفعة الزائدة وحسابه.

5. تحصيل مبلغ الربط وأي غرامات وفوائد مستحقة عليه.

2.21.2 تقارير غير مكتملة أو خاطئة

إذا أرسل أحد الأعضاء تقرير ربع سنوي غير صحيح، أو غير مكتمل، يحق لمشغل شبكة الدفع المحلية:

1. فرض تقييم على العضو، بعد مراجعة آخر تقارير ربع سنوية تم إرسالها بشكل صحيح للعضو وتقييمات مدفوعة عليها، تقييمًا يساوي أو يزيد عن آخر تقييم مدفوع بشكل صحيح للعضو لكل ربع سنة تقويمي قدم فيه تقريرًا ربع سنويًا خاطئًا أو غير مكتمل.
2. فرض تقييم عدم الامتثال على العضو.
3. إذا نتج عن تقدير مشغل شبكة الدفع المحلية للدفعة المستحقة دفع العضو دفعة أقل من اللازم، فيجب تحصيل مبلغ الدفعة الناقصة المستحقة وفرض غرامة فائدة أقل من اثنين في المائة شهريًا أو أعلى معدل يسمح به القانون، اعتبارًا من التاريخ كان الدفعة مستحقة الدفع لأول مرة وواجبة السداد حتى التاريخ الذي تم فيه دفع المبلغ الإضافي المستحق. (التعامل بالفائدة لايحوز طبقا للقانون الليبي)
4. إذا نتج عن تقدير مشغل شبكة الدفع المحلية للدفعات المستحقة دفع العضو دفعة زائدة، فيتم رد مبلغ الدفعة الزائدة، دون غرامة أو فائدة عليها، في أقرب وقت ممكن عمليًا بعد تحديد مبلغ الدفعة الزائدة وحسابها.
5. تحصيل مبلغ الربط وأي غرامة وفائدة مستحقة عليه من حساب تسوية العضو.

3.21.2 مطالبة المدفوعات الزائدة/ استرداد الرسوم

بعد أن يسلم العضو التقرير الكامل إلى مشغل شبكة الدفع المحلية، يجوز للعضو تقديم مطالبة تؤكد دفع مبالغ زائدة في هذا الشأن. ويجوز لمشغل شبكة الدفع المحلية مراجعة هذه المطالبة إذا تم استلام المطالبة من قبل مشغل شبكة الدفع المحلية في موعد لا يتجاوز ربع سنوي بعد تاريخ الدفع الزائد المزعوم. إذا قام مشغل شبكة الدفع المحلية بإثبات مطالبة العضو بالدفع الزائد، فسيعيد مشغل شبكة الدفع المحلية مبلغ الدفعة الزائدة إلى العضو في أقرب وقت ممكن عمليًا، دون فائدة أو جزاء.

22.2 متطلبات المعاملة

(الفئة أ)

وفقًا للمعايير، يلتزم كل عضو بالامتثال لكل القواعد التالية.

1. قبول وتقديم سجلات المعاملات الناشئة عن استخدام بطاقة صادرة عن أي عضو آخر في أي موقع POI يأذن العضو بقبول البطاقات وتقديمها إلى جهة الإصدار.
2. قبول ودفع المعاملات المستلمة من عضو آخر الناشئة عن استخدام أي بطاقة صادرة عنه. وإذا توقف مقدم خدمة الدفع عن رعايته من قبل أحد الأعضاء، فإن العضو يظل ملزمًا قبل الأعضاء الآخرين بقبول ودفع المعاملات الناشئة عن استخدام البطاقات الصادرة عن مقدم خدمة الدفع هذا.
3. الحفاظ على اتصال تشغيل فعال على مدار 24 ساعة في اليوم بالشبكة، إما بشكل مباشر أو عن طريق مقدم خدمة يعمل نيابة عنها، وعدم إجبار أي عضو آخر يرغب في العمل بشكل متعدد الأطراف باستخدام الشبكة في اتفاقيات ثنائية .
4. توفير بيانات صحيحة ودقيقة وكاملة وغير معدلة ومتسقة في جميع رسائل التفويض والمقاصة الخاصة بالمعاملات.

2.23 Payment Authorization Service

(Category A)

Each Member must provide, at its own expense and in compliance with the Standards:

1. Authorization services with respect to Cards that the Sponsoring Member and each of its Sponsored Payment Service Providers has issued; and
2. Regulated and reasonable authorization services with respect to its Merchants and those of its Sponsored Payment Service Providers. Each such Merchant must be instructed as to the proper use of such authorization services so as to ensure that Card acceptance and Transaction processing is conducted in compliance with the Standards.

2.24 Integrity of Brand and Network

(Category A)

A Member must not directly or indirectly engage in or facilitate any action that is illegal or that, in the opinion of the National Scheme Operator and whether or not addressed elsewhere in the Standards, damages or may damage the goodwill or reputation of the National Scheme Operator or of the NUMO Mark. Upon request of the National Scheme Operator, a Member will promptly cease engaging in or facilitating any such action.

In addition, a Member must not place or cause to be placed on any Card or any Terminal or other acceptance device any image, information, application or product that would in any way, directly or indirectly, have or potentially have the effect of diminishing or devaluing the reputation or utility of the Mark, a Card, or any of the National Scheme Operator's products, programs, services, networks, or systems.

Rules and Regulations of The Libyan National Payment Scheme
Chapter 3 - Issuing

This Chapter contains the Rules relating to Issuer requirements, product types, and Card requirements.

3.1 Issuer Requirements

3.1.1 Card Issuance - General requirements

(Category A as referenced in Chapter 1)

An Issuer must operate each of its Programs in accordance with the Standards that are in effect from time to time.

Each Program must be:

- Structured so as to avoid undue risk to the National Scheme Operator and other Members; and
- Operated in a manner that does not reflect poorly on the National Scheme Operator or the Mark of NUMO.

An Issuer must ensure that a Card or Access Device:

1. Only provides access to a valid account type;
2. Displays the Mark pursuant to the License and the Standards;
3. Complies with the Standards on security; and
4. If it contains a chip or has contactless payment functionality, complies with the requirements for chip and/or contactless payment functionality.

23.2 خدمة تفويض الدفع

(الفئة أ)

يجب على كل عضو أن يقدم، على نفقته الخاصة ووفقًا للمعايير، ما يلي:

1. خدمات التفويض فيما يتعلق بالبطاقات التي أصدرها العضو الراعي وكل من مقدمي خدمة الدفع المكفول.
2. خدمات تفويض منظمة ومعقولة فيما يتعلق بالتجار وتجار مقدمي خدمة الدفع المكفولين. يجب توجيه تعليمات لكل تاجر فيما يتعلق بالاستخدام الصحيح لخدمات التفويض هذه لضمان قبول البطاقة ومعالجة المعاملات وفقًا للمعايير.

24.2 سلامة العلامة التجارية والشبكة

(الفئة أ)

يلتزم كل العضو بعدم تسهيل أو الانخراط بشكل مباشر أو غير مباشر في أي إجراء غير قانوني، في رأي مشغل شبكة الدفع المحلية وسواء تم تناوله في مكان آخر في المعايير أم لا، يؤدي إلى الإضرار أو قد يضر بحسن نية أو سمعة مشغل شبكة الدفع المحلية أو بعلامة (نمو). بناءً على طلب مشغل شبكة الدفع المحلية، سيتوقف العضو على الفور عن المشاركة في أي إجراء من هذا القبيل أو تسهيله.

بالإضافة إلى ذلك، يجب على العضو عدم وضع أو التسبب في وضعه على أي بطاقة أو أي جهاز طرفي أو أي جهاز قبول آخر، أي صورة أو معلومات أو تطبيق أو منتج قد يكون له بأي شكل من الأشكال، بشكل مباشر أو غير مباشر، أو يحتمل أن يكون له تأثير التضاؤل أو التقليل من قيمة سمعة أو منفعة العلامة أو البطاقة أو أي من منتجات مشغل شبكة الدفع المحلية أو برامجه أو خدماته أو شبكاته أو أنظمتها.

قواعد ولوائح شبكة الدفع المحلية الليبية

الفصل 3 – الإصدار

يحتوي هذا الفصل على القواعد المنظمة لجهة إصدار البطاقات وأنواع المنتجات التي تقدمها.

1.3 متطلبات جهة الإصدار

1.1.3 إصدار البطاقة - القواعد العامة

(الفئة أ كما هو مشار إليه في الفصل 1)

يجب على جهة الإصدار تشغيل كل برنامج من برامجها وفقًا للمعايير السارية وقت القيام بها.

يجب أن يكون كل برنامج:

- منظم بطريقة تجنب المخاطر التي قد يتعرض لها مشغل شبكة الدفع المحلية والأعضاء الآخرين.
- يعمل بطريقة لا تؤثر بشكل سلبي على مشغل شبكة الدفع المحلية أو علامة (نمو).

يجب على جهة الإصدار التحقق من أن البطاقة أو جهاز الوصول:

1. يوفر فقط الوصول إلى نوع حساب صالح لقيام بإجراء العمليات المستهدفة.
2. يعرض العلامة وفقًا للترخيص والمعايير المعمول بها.
3. يتوافق مع معايير الأمن القانوني والإلكتروني.
4. إذا كان يحتوي على شريحة أو لديه وظيفة الدفع عن بعد، فإنه يتوافق مع متطلبات وظيفة الشريحة /أو وظيفة الدفع عن بعد.

There is no limitation on the types of Accounts that are permitted to co-reside on the same Mobile Payment Device, provided that such Accounts are not linked, but rather exist independently and are each accessed by a separate and distinct Payment Application hosted on the same user interface.

3.1.2 Credit Card Issuance

(Category A as referenced in Chapter 1)

Subject to approval of the concerned authorities (Sharia Committee)

The following requirements apply to the issuance of Credit Cards:

1. If an approved Cardholder application for issuance of a payment card or payment device indicates the applicant's preference, by way of a checkmark or otherwise, to be issued a NUMO Credit Card, then the Issuer must issue a NUMO Credit Card and no other brand.
2. The Issuer must provide a personal identification number (PIN) or allow the Cardholder to have a self-Assigned PIN.
3. An Issuer must ensure that each contactless-enabled Card or Payment Device is personalized with the appropriate device type value.

3.1.3 Debit & Prepaid Card Issuance

(Category A as referenced in Chapter 1)

The following requirements apply to the issuance of Debit Cards:

1. The Issuer must maintain the funds in the Member Debit Account.
2. The Issuer must not place the NUMO brand on any card that has access to any of the following types of accounts:
 - a. Accounts that “pass-through” to an account at an institution not eligible to be a Member.
3. The Issuer must provide a PIN or allow the Cardholder to have a self-Assigned PIN.
4. An Issuer must verify its Cardholders by means of online PIN verification, except that PIN verification is not required for contactless Transactions.
5. If PIN bypass is applied, the Cardholder must be verified by signature.
6. An Issuer must ensure that each contactless-enabled Card or Payment Device is personalized with the appropriate device type value.

3.1.3.1 Eligible Accounts – Debit

(Category A as referenced in Chapter 1)

The Issuer must ensure that the account to which a Debit Card provides access, directly or indirectly, is one of the following:

Any current or sight deposit (including overdraft lines of credit linked to such accounts), a savings account or a pooled account (linked to an approved prepaid Card Program) maintained by or on behalf of a Cardholder with an Issuer.

لا توجد قيود على أنواع الحسابات التي يُسمح لها بالاشتراك في نفس جهاز الدفع عبر الهاتف المحمول، بشرط ألا تكون هذه الحسابات مرتبطة بحسابات أخرى، بل توجد بشكل مستقل ويتم الوصول إلى كل منها بواسطة تطبيق دفع منفصل و مختلف يتم تثبيته على سطح واجهة جهاز المستخدم.

2.1.3 إصدار بطاقة الائتمان

(الفئة أ كما هو مشار إليه في الفصل 1)

خاضع لموافقة السلطات المعنية (اللجنة الشرعية).

تنطبق القواعد التالية على إصدار بطاقات الائتمان:

1. إذا كان طلب حامل البطاقة الموافق عليه لإصدار بطاقة دفع أو جهاز دفع يشير إلى تفضيل مقدم الطلب، عن طريق علامة اختيار أو غير ذلك، لإصدار بطاقة ائتمان (نمو)، فيجب على جهة الإصدار أن تصدر بطاقة ائتمان (نمو) وليس علامة تجارية أخرى .
2. يجب على جهة الإصدار وضع رمز تعريف شخصي أو السماح لحامل البطاقة بالحصول على رمز تعريف شخصي مخصص ذاتيًا.
3. يجب على جهة الإصدار التأكد من تخصيص كل بطاقة أو جهاز دفع مزود بتقنية الدفع عن بعد مع قيمة نوع الجهاز المناسبة.

3.1.3 إصدار بطاقة الخصم والدفع المسبق

(الفئة أ كما هو مشار إليه في الفصل 1)

تنطبق القواعد التالية على إصدار بطاقات الخصم:

1. يجب على جهة الإصدار الاحتفاظ بالأموال في حساب العضو مسبق الدفع.
2. يجب على جهة الإصدار عدم وضع علامة (نمو) التجارية على أي بطاقة يمكنها الوصول إلى أي من أنواع الحسابات التالية:
 - أ. حساب بطاقة شحن أو بطاقة ائتمان كحساب أساسي؛ أو
 - ب. الحسابات التي “تعبّر” إلى حساب في مؤسسة غير مؤهلة لتكون عضوًا.
3. يجب على جهة الإصدار توفير رقم تعريف شخصي أو السماح لحامل البطاقة بالحصول على رقم تعريف شخصي مخصص ذاتيًا.
4. يجب على جهة الإصدار أن تتحقق من حاملي البطاقات، عن طريق التحقق من رمز التعريف الشخصي عبر الإنترنت، ولا يكون التحقق مطلوباً في المعاملات التي تتم عن بعد.
5. يجوز لجهة الإصدار عدم الاعتماد على رمز التحقق الشخصي، إذا اعتمدت على التوقيع الإلكتروني كوسيلة بديلة لهذا التحقق.
6. يجب على جهة الإصدار التحقق من أن كل بطاقة أو جهاز دفع مزود بتقنية الدفع عن بعد، تتوافق مع مواصفات نوع الجهاز المعد لهذه الخدمة.

1.3.1.3 الحسابات المؤهلة - الخصم

(الفئة أ كما هو مشار إليه في الفصل 1)

يجب أن تتحقق جهة الإصدار من أن الحساب الذي توفر بطاقة الخصم الوصول إليه، بشكل مباشر أو غير مباشر، هو أحد الحسابات التالية:

أن يكون أحد الحسابات المعتمدة، سواء كان من الحسابات جاري، أو حسابات الودائع تحت الطلب (بما في ذلك خطوط ائتمان السحب على المكشوف المرتبطة بهذه الحسابات)، أو حساب توفير أو حساب مجمع (مرتبط ببرنامج بطاقة الدفع المسبق) يحتفظ به حامل البطاقة، أو نائبه أو وكيله مع جهة الإصدار.

5.1.3.2 Ineligible Accounts

(Category A as referenced in Chapter 1)

Any account held or serviced by a member that is Licensed to conduct only acquiring Activity is not eligible to be an Account.

3.1.4 Appeals and Marketing - Linked Card Programs

(Category A as referenced in Chapter 1)

Without the express prior written consent of the National Scheme Operator, an Issuer must not use an Appeal or conduct any advertising, promotion, marketing, or the like in connection with a Card Program that is in any way linked to a different payment card.

3.1.5 Selective Authorization

(Category A as referenced in Chapter 1)

Without the express prior written approval of the National Scheme Operator, a Member must not launch or maintain a Card Program that has the effect of selectively authorizing Transactions arising from use of the Cards and Accounts at only a subset of Member acceptance locations.

A Member has the right to authorize or decline individual Transactions based on:

1. The amount of funds or credit available;
2. Fraud or credit risks presented by individual Cardholder usage patterns;
3. Cash access restrictions to manage a high-risk account;
4. Cardholder-designated restrictions on use.
5. Any other restriction on use which the National Scheme Operator permits.

An Issuer's authorization decision must be made on an individual Transaction basis and not on the basis of Transaction type, acceptance environment, or other similar factors except as permitted by the Standards (although any such factors or combination thereof may contribute to the decision).

Notwithstanding the foregoing, a Member is permitted to issue a Contactless Payment Device that provides access to a Member Account without also issuing an accompanying Card for the same Account. Any Contactless Payment Device issued without an accompanying Card must support Transactions of any amount, and the Issuer must provide clear instructions to the Cardholder as to the limitations of its use.

3.1.6 Information to Cardholders

(Category B as referenced in Chapter 1)

An Issuer must provide the following information to each of its Cardholders:

1. Before the Card is used, the Issuer must inform the Cardholder that the Card may be used wherever the NUMO Brand is displayed, and:
 - a. The issuing fees of the Card;
 - b. Specific charges, if any, to be paid to the Issuer for services provided through the Card or auxiliary charges applicable to the account, including but not limited to any Account access fees, cash advance fees, ATM usage fees, late payment fees in case of overdraft, and any other additional fees that could be applied;

2.3.1.3 الحسابات غير المؤهلة

(الفئة أ كما هو مشار إليه في الفصل 1)

أي حساب يحتفظ به أو يخدمه عضو مرخص له لإجراء نشاط قبول فقط غير مؤهل ليكون حسابًا.

4.1.3 التفعيل والتسويق - برامج البطاقات المرتبطة

(الفئة أ كما هو مشار إليه في الفصل 1)

لا يجوز لجهة الإصدار، بدون الحصول على الموافقة المكتوبة المسبقة، من مشغل شبكة الدفع المحلية لأنظمة الدفع، تفعيل أو إجراء أي إعلان أو دعاية أو تسويق، أو القيام بأي إجراء وبأي وسيلة كانت يتعلق ببرامج البطاقات المرتبطة أو بطاقات الدفع المسبق.

5.1.3 التفويض الانتقائي

(الفئة أ كما هو مشار إليه في الفصل 1)

لا يجوز لأي عضو، بدون الحصول على الموافقة المكتوبة المسبقة، من مشغل شبكة الدفع المحلية، القيام بأي إجراء يتعلق بإطلاق أو الاحتفاظ ببرامج البطاقات ويكون من شأنه التفويض بشكل انتقائي على المعاملات الناشئة عن استخدام البطاقات والحسابات في مجموعة فرعية فقط من قبل مواقع الأعضاء.

يحق للعضو التصريح بالمعاملات الفردية أو رفضها بناءً على:

1. مقدار الأموال أو الائتمان المتاح لديه.
2. الاحتيال أو مخاطر الائتمان التي تقدمها طبيعة استخدام حامل البطاقة الفردية.
3. قيود الوصول للقيم النقدية لإدارة حساب عالي المخاطر.
4. قيود الاستخدام التي يحددها حامل البطاقة.
5. أي قيود أخرى على الاستخدام يسمح بها مشغل شبكة الدفع المحلية.

يجب اتخاذ قرار التفويض الصادر عن جهة الإصدار على أساس معاملة فردية، وليس على أساس نوع المعاملة أو بيئة القبول أو عوامل أخرى مماثلة، باستثناء ما تسمح به المعايير (على الرغم من أن أي من هذه العوامل أو مجموعة منها قد تساهم في قرار الترخيص).

بالرغم مما سبق ذكره، يُسمح للعضو بإصدار جهاز دفع عن بعد يوفر الوصول إلى حساب عضو دون إصدار بطاقة مرفقة معه لنفس الحساب، ويجب أن يدعم أي جهاز دفع عن بعد صادر بدون بطاقة مرفقة معه جميع العمليات وبأي مبلغ، ويجب على جهة الإصدار تقديم تعليمات واضحة وصريحة إلى حامل البطاقة فيما يتعلق بقيود استخدامها.

6.1.3 معلومات لحاملي البطاقات

(الفئة ب كما هو مشار إليه في الفصل 1)

يجب على جهة الإصدار تقديم المعلومات التالية إلى كل حاملي بطاقات التي تصدرها:

قبل استخدام البطاقة، يجب على جهة الإصدار إبلاغ حامل البطاقة بأنه يمكن استخدام البطاقة أينما يتم عرض علامة (نمو) التجارية، و:

- أ. تحديد قيمة رسوم إصدار البطاقة.
- ب. تحديد قيمة الرسوم المحددة، إن وجدت، التي يتعين دفعها إلى جهة الإصدار مقابل الخدمات التي تقدمها البطاقة، أو الرسوم الإضافية المطبقة على الحساب، بما في ذلك على سبيل المثال لا الحصر رسوم الوصول إلى الحساب، ورسوم السلفة النقدية، ورسوم استخدام أجهزة الصراف الآلي، ورسوم السداد المتأخر في حالة السحب على المكشوف، أو وأي رسوم إضافية أخرى يمكن تطبيقها.

- c. The Cardholder's liability, including the cost, if the Card is lost or stolen. This information must be stated clearly in the body of the product literature. The Cardholder must also be told what to do if the Card is lost or stolen;
- d. The standard limit, if any, up to which the Cardholder can use the Card.
2. For the Transaction statement, as applicable, the following information must be provided to the Cardholder:
- Transaction Date and Time.
 - Transaction type (for example, ATM cash withdrawal, cash advance) and location (if technically feasible);
 - Transaction amount and currency;
 - Total commission and fees applied (if applicable);

3.1.7 Limitation of Liability of Cardholders for Unauthorized Use (Zero Liability)

(Category B as referenced in Chapter 1)

An Issuer must not hold a Cardholder liable for a Transaction that was not authorized by the Cardholder if the Cardholder exercised reasonable care in safeguarding the Card from risk of loss or theft and, upon becoming aware of such loss or theft, promptly reported the loss or theft to the Issuer.

This Rule shall not apply to a Transaction conducted with a Card that is:

- Issued to an entity other than a natural person or for a commercial purpose.
- Issued and/or sold to a person until such time as that person's identity is registered by or on behalf of the Issuer in connection with such issuance and/or sale, which registration may include identification requirements.

If applicable law imposes a greater liability or a conflicting obligation, such applicable law shall govern.

3.1.8 Lost or Stolen Card Reporting

(Category B as referenced in Chapter 1)

An Issuer must provide a means for Cardholders to notify it of the loss or theft of a Card, 24 hours/day, 7 days/week.

3.1.9 Emergency Card Replacement

When a Cardholder reports a card lost or stolen, it is recommended that the Issuer provide an emergency replacement Card, if the Issuer is not able to provide a new Card within [72] hours of being informed that the card has been lost or stolen.

The Cardholder may obtain replacement Cards from a location assigned by the Issuer.

3.1.10 Emergency Request – Fines and Penalties

Subject to early stated issuer fees.

- ت. المعلومات المتعلقة بمسؤولية حامل البطاقة، بما في ذلك التكلفة، في حالة ضياع البطاقة أو سرقتها. يجب ذكر هذه المعلومات بشكل واضح في متن دليل استخدام البطاقة (كتابات المنتج). يجب أيضًا إعلام حامل البطاقة بالإجراءات التي يجب اتخاذها في حالة ضياع البطاقة أو سرقتها.
- ث. الحد القياسي، إن وجد، الذي يمكن لحامل البطاقة استخدامه للبطاقة.
2. بالنسبة لبيان المعاملة، عند الاقتضاء، يجب تقديم المعلومات التالية إلى حامل البطاقة:
- أ. تاريخ ووقت إجراء المعاملة.
 - ب. بنوع المعاملة (على سبيل المثال، السحب النقدي من أجهزة الصراف الآلي، والسلف النقدية) ومكان إجراء المعاملة (إذا كان ذلك ممكنًا من الناحية الفنية).
 - ت. تمبلغ المعاملة ونوع العملة.
 - ث. إجمالي العمولات والرسوم المستحقة (إن وجدت).

7.1.3 تحديد مسؤولية حاملي البطاقات عن الاستخدام غير المصرح به (الإعفاء من المسؤولية)

(الفئة ب كما هو مشار إليه في الفصل 1)

لا يكون حامل البطاقة مسؤولاً عن معاملة لم يصرح له بها إذا بذل العناية المعقولة في حماية البطاقة من مخاطر الضياع أو السرقة، وعند العلم بواقعة الضياع أو السرقة، يجب إبلاغ جهة الإصدار عن هذه الواقعة فوراً.

لا تنطبق هذه القاعدة على المعاملة التي يتم إجراؤها باستخدام بطاقة:

- صادرة لشخص اعتباري، أو لغرض تجاري.
- تم إصدارها و/أو بيعها إلى شخص قبل تسجيل هوية ذلك الشخص، أو نائبه أو وكيله من قبل جهة الإصدار، فيما يتعلق بهذا الإصدار و/أو البيع، والذي قد يتضمن التسجيل متطلبات تحديد الهوية.

إذا كان القانون المعمول به يفرض مسؤولية أكبر أو التزامًا متضاربًا ، فأن هذا القانون هو الذي يحكم

8.1.3 الإبلاغ عن البطاقة الضائعة أو المسروقة

(الفئة ب كما هو مشار إليه في الفصل 1)

يجب على جهة الإصدار أن تحدد الإجراءات والوسائل التي يلتزم حاملي البطاقات باتباعها للإخطار بواقعة ضياع البطاقة أو سرقتها، خلال 24 ساعة يوميًا، وطيلة أيام الأسبوع.

9.1.3 الاستبدال الطارئ للبطاقة

عندما يعلن حامل البطاقة عن ضياع البطاقة أو سرقتها، يوصى بأن تقدم له جهة الإصدار بطاقة بديلة في حالات الطوارئ، وإذا لم تكن جهة الإصدار قادرة على تقديم بطاقة بديلة في غضون [72] ساعة من إبلاغه ضياع البطاقة أو سرقتها.

يجوز لحامل البطاقة الحصول على بطاقات جديدة من الموقع المحدد من قبل جهة الإصدار.

10.1.3 طلب الطوارئ - الغرامات والعقوبات

تخضع لرسوم جهة الإصدار المذكورة سابقاً.

3.1.11 Proprietary Scheme Cardholder Loyalty Programs

An Issuer may offer to its Cardholders loyalty points or other rewards for payments made with a Card. If the loyalty program involves recourse to a third party, the Issuer must register the third party as a Service Provider with the National Scheme Operator.

3.1.12 ATM Usage

An Issuer must support the use of its Cards to make ATM cash withdrawals, unless it has been permitted to suppress this functionality with regard to specific card programs, typically certain types of prepaid programs.

The Issuer sets the daily or weekly limits on cash withdrawals, within the limits set by Center Bank.

Contactless functionality may be supported for cash withdrawals.

3.1.13 ATM Issuer Requirements

(Category A as referenced in Chapter 1)

An Issuer must not discriminate against any ATM with regard to processing and authorizing Transactions, including ATMs owned by other Members. This Rule also applies with regard to balance inquiry and any other functionality provided at ATMs.

3.1.14 ATM Balance Inquiry Service

Support by the Issuer for balance inquiry service at the ATM is strongly recommended.

3.1.15 Tokenization of Accounts

(Category A as referenced in Chapter 1)

With respect to the Tokenization of Accounts, all of the following apply:

1. The National Scheme Operator has the sole right to designate a Token Account Range to an Issuer.
2. Each Token must be allocated by the National Scheme Operator, unless the National Scheme Operator has expressly approved otherwise.
3. The Tokenization of an Account primary account number (PAN) must be performed in compliance with all applicable Standards.
4. The National Scheme Operator must be provided the mapping between the PAN assigned to a Card, and each Token associated with the Account for use by the authorized user of the Card.
5. An Account PAN must be Tokenized whenever a Mobile Payment Device, or other non-Card method is used, in addition to a Card, to provide access to an Account.
6. The PAN of a Card must not be replaced by, mapped to, or Tokenized with any PAN issued from an Issuer Identification Number (IIN) range reserved by the ISO Registration Authority for a competing payment network. Refer to the current ISO Register Of Issuer Identification Numbers for more information.
7. The Token cryptogram must be validated during the authorization of all Transactions involving Tokenized Accounts.

11.1.3 نظام الملكية لبرامج ولاء حامل بطاقة

يجوز لجهة الإصدار أن تعرض على حاملي البطاقات نقاط ولاء أو مكافآت أخرى للمدفوعات التي تتم باستخدام البطاقة. وإذا كان برنامج الولاء ينطوي على اللجوء إلى طرف ثالث، فيجب على جهة الإصدار تسجيل الطرف الثالث كمقدم خدمة لدى مشغل شبكة الدفع المحلية.

12.1.3 استخدام أجهزة الصراف الآلي

يجب أن تزود جهة الإصدار بطاقتها بأنظمة لإجراء عمليات السحب النقدي من أجهزة الصراف الآلي، كما قد يتم تزويد خدمة الدفع عن بعد للسحب النقدي.

ما لم يُسمح لها بإلغاء هذه الميزة فيما يتعلق ببرامج بطاقات معينة، وعادةً ما تكون أنواعًا معينة من برامج الدفع المسبق.

تحدد جهة الإصدار السقف اليومي أو الأسبوعي لعمليات السحب النقدية، ضمن الحدود التي يضعها مصرف ليبيا المركزي.

13.1.3 قواعد جهة إصدار أجهزة الصراف الآلي

(الفئة أ كما هو مشار إليه في الفصل 1)

يجب ألا تميز جهة الإصدار بين أجهزة الصراف آلي فيما يتعلق بمعالجة المعاملات والترخيص بها، بما في ذلك أجهزة الصراف الآلي المملوكة لأعضاء آخرين. وتنطبق هذه القاعدة أيضًا فيما يتعلق بالاستعلام عن الرصيد، وأي وظائف أخرى متوفرة في أجهزة الصراف الآلي.

14.1.3 خدمة الاستعلام عن الرصيد عن طريق أجهزة الصراف الآلي

يوصى بشدة بدعم جهة الإصدار لخدمة الاستعلام عن الرصيد في أجهزة الصراف الآلي.

15.1.3 ترميز الحسابات

(الفئة أ كما هو مشار إليه في الفصل 1)

فيما يتعلق بترميز الحسابات، يتم تطبيق القواعد التالية:

1. لمشغل شبكة الدفع المحلية وحده الحق في تحديد طريقة ترميز الحساب إلى جهة إصدار.
2. يجب تخصيص كل رمز مميز بواسطة مشغل شبكة الدفع المحلية، ما لم يوافق مشغل شبكة الدفع المحلية صراحةً على خلاف ذلك.
3. يجب أن تتم عملية الترميز لرقم الحساب الأساسي بما يتوافق مع جميع المعايير المعمول بها في مصرف ليبيا المركزي.
4. يجب تزويد مشغل شبكة الدفع المحلية بالرباط بين رقم الحساب الأساسي المخصص للبطاقة، وكل ترميز آخر مرتبط بالحساب، يستخدمه المرخص له باستخدام البطاقة.
5. يجب أن يكون رقم الحساب الأساسي رمزياً عند استخدام جهاز الدفع عبر الهاتف المحمول، أو أي طريقة أخرى بخلاف البطاقة، بالإضافة إلى البطاقة، لتوفير الوصول إلى الحساب.
6. يجب عدم استبدال أو تعيين أو ترميز رقم الحساب الأساسي الخاص بالبطاقة بأي رقم حساب أساسي صادر من نطاق رقم تعريف جهة الإصدار المحجوز من قبل هيئة تسجيل ISO لشبكة دفع منافسة. راجع سجل ISO الحالي لأرقام تعريف جهة الإصدار للمزيد من المعلومات.
7. يجب التحقق من صحة الرمز المشفر أثناء تصريح جميع المعاملات التي تتضمن الحسابات الرمزية.

An Issuer wishing to support the Tokenization of its Accounts for use on a Mobile Payment Device must:

1. Comply with all technical specifications and other Standards applicable to Tokenization and Digitization set by the National Scheme.
2. Complete all testing and certifications as required by the National Scheme Operator from time to time in connection with Tokenization and Digitization;
3. Decline any request to Tokenize an Account if:
 - a. The identity of the Cardholder is unknown to the Issuer;
 - b. The Token Requestor is not a Digital Activity Member or other Member approved by the National Scheme Operator to conduct Digital Activity.
4. Establish Cardholder support policies and procedures.

3.1.16 Stand-in Processing

If stand-in processing is provided, the Issuer will be liable for Transactions authorized in stand-in by the National Scheme Operator, in the same manner as if the Transactions were authorized by the Issuer itself.

3.1.17 Chip Issuer Liability

An Issuer is responsible for the Transactions on its Cards, unless a chargeback right or other dispute right is available.

Refer to Chapter 11 for further information.

3.1.18 EMV Liability Shift

Refer to Book 3 Chapter 3 for information on this topic.

3.1.19 Address Verification Service (AVS)

The National Scheme Operator does not currently support AVS.

3.1.20 3-D Secure Participation Requirements

Enrollment by the Issuer of its Cardholders in 3-D Secure is strongly recommended, because it provides a means to authenticate the Cardholder for e-commerce Transactions.

The National Scheme Operator mandates participation in 3-D Secure for e-commerce transactions.

3.1.21 3-D Secure Participation Non-Compliance Penalties

The National Scheme Operator would fine Members that do not support it. The violation would fall under Category A as referenced in Chapter 1 of the noncompliance framework.

3.1.22 Cardholder Authentication

It is strongly recommended that the Issuer use 3-D Secure to authenticate its Cardholders for the completion of e-commerce Transactions. Authentication of the Cardholder provides confidence that the Transaction is not fraudulent and so supports improved approval rates on e-commerce Transactions.

يجب على جهة الإصدار التي ترغب في دعم عملية ترميز حساباتها لاستخدامها على جهاز الدفع عبر الهاتف المحمول:

1. الالتزام بجميع المعايير والمواصفات الفنية، المطبقة على الترميز والرقمنة التي وضعها مشغل شبكة الدفع المحلية .
2. إجراء جميع الاختبارات والشهادات التي يطلبها مشغل شبكة الدفع المحلية من وقت لآخر فيما يتعلق بالترميز والرقمنة.
3. رفض أي طلب لترميز حساب إذا:
 - أ. كانت هوية حامل البطاقة غير معروفة لجهة الإصدار؛
 - ب. كان طالب الترميز ليس عضوًا في النشاط الرقمي أو عضوًا آخر مرخص له من قبل مشغل شبكة الدفع المحلية لإجراء نشاط رقمي.
4. وضع سياسات وإجراءات دعم حامل البطاقة.

16.1.3 المعالجة الاحتياطية:

إذا تم توفير المعالجة الاحتياطية، فستكون جهة الإصدار مسؤولة عن المعاملات المرخص بها احتياطياً من قبل مشغل شبكة الدفع المحلية، وبنفس الطريقة كما لو تم الترخيص بالمعاملات من قبل جهة الإصدار نفسها.

17.1.3 مسؤولية جهة إصدار الشريحة

جهة الإصدار مسؤولة عن المعاملات التي تنفذ عن طريق بطاقتها، ما لم يتوفر حق رد المبالغ المدفوعة، أو كانت محلاً لمنازعة قضائية أو تحكيمية.

راجع الفصل 11 للمزيد من المعلومات.

18.1.3 انتقال مسؤولية EMV

راجع الكتاب 3 الفصل 3 للحصول على معلومات حول هذا الموضوع.

19.1.3 خدمة التحقق من العنوان (AVS)

لا يدعم مشغل شبكة الدفع المحلية خدمة التحقق من العنوان (AVS) حالياً.

20.1.3 متطلبات المشاركة الآمنة ثلاثية الأبعاد

يوصى بشدة بالتسجيل من قبل جهة إصدار لحاملي البطاقات في نظام الأمان ثلاثي الأبعاد، لأنه يوفر وسيلة لمصادقة حامل البطاقة على معاملات التجارة الإلكترونية. يفرض مشغل شبكة الدفع المحلية المشاركة في نظام الأمان ثلاثي الأبعاد لمعاملات التجارة الإلكترونية.

21.1.3 عقوبات عدم الامتثال للمشاركة الآمنة ثلاثية الأبعاد

يقوم مشغل شبكة الدفع المحلية بفرض غرامة على الأعضاء الذين لا يدعمونها. يندرج الانتهاك ضمن الفئة أ كما هو مشار إليه في الفصل 1 من إطار عمل عدم الامتثال.

22.1.3 مصادقة حامل البطاقة

يجب أن تستخدم جهة الإصدار الآمن ثلاثي الأبعاد للمصادقة على حاملي البطاقات لإتمام معاملات التجارة الإلكترونية. وتعد مصادقة حامل البطاقة قرينة على أن المعاملة ليست احتيالية، وبالتالي تدعم معدلات الائتمان في معاملات التجارة الإلكترونية.

3.1.23 Membership Management

Reserved for future use.

3.1.24 Client Portfolio Management Self-Service Tools Requirements

The National Scheme Operator may provide self-service tools that an Issuer is able to use to manage its Card Portfolio.

3.1.25 Data Retention and Transmission

(Category A as referenced in Chapter 1)

An Issuer must securely retain Transaction data for at least [12] months after the presentment of the Transaction and must be able to securely transmit Transaction data to the relevant Cardholder upon request.

The Issuer must also be able to securely transmit Transaction data to government authorities in response to a justified and documented request. The Issuer must inform the National Scheme Operator when any such request is received.

3.1.26 Card Shipping Requirements

(Category A as referenced in Chapter 1)

3.1.26.1 Personalized Cards

An Issuer that issues and/or personalizes Cards onsite at a bank branch, retail store, or other location outside of a Card production vendor facility is obliged to take all steps necessary to safeguard the issuance of Cards and to protect Cardholder data at such locations.

3.1.26.2 Cards Without Personalization

A Member must not send Cards that have not yet been personalized with a primary account number [PAN] or expiration date through the mail. Unpersonalized Cards must be shipped according to secure shipping methods as described in the Card Production Physical Security Requirements. In the rare event that rapid delivery is required, and secure shipping methods are infeasible, the Issuer is permitted to use an express courier service that provides shipment tracking, recipient authentication, and receipt confirmation for the shipment of no more than 500 unfinished Cards a day.

3.1.26.3 Card Count Discrepancies

Upon receiving a shipment of Cards, the Issuer must verify that the correct Card quantity was delivered and take immediate action to resolve any Card count discrepancy and recover any missing Cards. The Issuer has the right to use the Card count noted on each sealed carton in the Card count verification. Sealed cartons may also be opened at random, audited, and resealed. All open cartons and all sealed cartons with no Card count noted on the carton must have the contents counted.

23.1.3 إدارة العضوية

محجوزة للاستخدام في المستقبل.

24.1.3 متطلبات قواعد أدوات الخدمة الذاتية لإدارة محفظة العميل

قد يوفر مشغل شبكة الدفع المحلية أدوات الخدمة الذاتية التي يمكن لجهة الإصدار استخدامها لإدارة محفظة البطاقات الخاصة بها.

25.1.3 حفظ ونقل البيانات

(الفئة أ كما هو مشار إليه في الفصل 1)

يجب أن تقوم جهة الإصدار بحفظ بيانات المعاملة لديها، بشكل آمن لمدة [12] شهرًا على الأقل بعد القيام بالمعاملة، ويجب عليها أن تكون قادرة على نقل بيانات المعاملة بشكل آمن إلى حامل البطاقة عند طلبه لها.

يجب أن تكون جهة الإصدار أيضًا قادرة على نقل بيانات المعاملات بشكل آمن إلى السلطات الرسمية المختصة استجابة لطلب رسمي، مع مراعاة قواعد حماية الخصوصية التي يحميها القانون. ويجب على جهة الإصدار إعلام مشغل شبكة الدفع المحلية عند استلام هذا الطلب.

26.1.3 قواعد شحن البطاقة

(الفئة أ كما هو مشار إليه في الفصل 1)

1.26.1.3 البطاقات المخصصة

جهة الإصدار التي تصدر، أو تخصص البطاقات في المصارف أو فروعها، أو في محال التسويق، أو أي مكان آخر خارج محال جهة إصدار البطاقات ملزمة باتخاذ جميع الخطوات اللازمة لحماية إصدار البطاقات وحماية بيانات حامل البطاقة في هذه المواقع.

2.26.1.3 بطاقات بدون تخصيص

يجب ألا يرسل العضو البطاقات التي لم يتم تخصيصها برقم حساب أساسي، أو تاريخ انتهاء الصلاحية عبر البريد. ويجب شحن البطاقات التي لم يتم تخصيصها وفقًا لطرق الشحن الآمنة كما هو موضح في قواعد الأمان المادي لإنتاج البطاقة. في الحالات الاستعجال والتي تتطلب التسليم السريع، وكانت طرق الشحن غير آمنة، يُسمح لجهة الإصدار باستخدام خدمة البريد السريع التي توفر تتبع الشحن، وتوقعات المستلمين، وتأكيد الاستلام لشحن ما لا يزيد عن 500 بطاقة غير مكتملة في اليوم.

3.26.1.3 الاختلافات في عدد البطاقات

عند استلام شحنة من البطاقات، يجب على جهة الإصدار التحقق من تسليم العدد الصحيح للبطاقات، واتخاذ إجراءات فورية لحل مسألة الاختلاف في عدد البطاقات، واستعادة أي بطاقات ضائعة. ويحق لجهة الإصدار استخدام عدد البطاقات المدون على كل شحنة مختومة في التحقق من عدد البطاقات. يمكن لها أيضًا فتح الشحنة المختومة بطريقة اختيارية، وتدقيقها وإغلاقها للتحقق من عددها. ويجب احتساب العدد الموجود في جميع الشحنات المفتوحة وجميع الشحنات المختومة التي لم يُدرج فيها عدد البطاقات على الشحنة.

3.1.26.4 Reporting Card Loss or Theft

Within 24 hours of discovery, a Member must report to the National Scheme Operator the suspected or confirmed loss or theft of any Cards while in transit from a vendor or in the Member's possession. The report must contain the following information:

- Issuer name and Member ID
- Card type and quantity
- With respect to the loss or theft of Cards while in transit from a vendor:
 - The vendor name
 - The location from which the Cards were shipped
 - The date and method of shipment
 - The address to which the Cards were shipped
- Pertinent details about the loss and the investigation
- Name and phone number of contact for additional information
- Name and phone number of person reporting the loss or theft

3.1.26.5 Disposition of Unissued Cards and Account Information

A Member that ceases to issue Cards must promptly destroy all unissued Cards and all media containing Card Account information in a secure manner. It must provide a full report to the National Scheme Operator on the method and timing of disposition of unissued Cards and media containing Card Account information.

3.2 Product Types

3.2.1 Consumer

A consumer product is used for the payment of personal expenses of all types. Consumer products may be credit, debit or prepaid Cards. Consumer products may be standard Cards or premium Cards.

Please refer to the product guides for further details.

3.2.2 Commercial

A commercial product is intended to be used for the payment of business expenses, such as employee expenses while traveling on business, payment for commercial merchandise, and purchase of office supplies.

The following are examples of commercial products:

- Salary Cards
- Small business Cards
- Corporate Cards
- Purchasing Cards
- Fleet Cards

Please refer to the product guides for further details.

4.1.26.3 الإبلاغ عن ضياع البطاقة أو سرقتها

يجب على العضو إبلاغ مشغل شبكة الدفع المحلية بواقعة السرقة أو الضياع خلال 24 ساعة من اكتشاف بتلك الواقعة إثناء عملية النقل من البائع او اثناء حيازتها من العضو، ويجب أن يحتوي التقرير على المعلومات التالية:

- اسم جهة الإصدار، وهوية العضو.
- نوع البطاقات وعددها.
- فيما يتعلق بضياع البطاقات أو سرقتها أثناء نقلها من البائع:
 - اسم البائع.
 - المكان الذي شحنت منه البطاقات.
 - تاريخ وطريقة الشحن
 - العنوان الذي تم شحن البطاقات إليه.
- تفاصيل ذات صلة حول الاضرار المتوقعة، وإجراءات التحقيق.
- اسم ورقم هاتف جهة الاتصال للحصول على معلومات إضافية.
- اسم ورقم هاتف الشخص الذي أبلغ عن الضياع أو السرقة.

5.26.1.3 التخلص من البطاقات غير الصادرة وبيانات الحساب

يجب على العضو الذي يتوقف عن إصدار البطاقات إتلاف جميع البطاقات غير المُصدرة وجميع الوسائط التي تحتوي على معلومات وبيانات حساب البطاقة بطريقة آمنة. ويجب أن يقدم تقريرًا مفصلاً لمشغل شبكة الدفع المحلية عن طريقة وتوقيت التخلص من البطاقات غير الصادرة والوسائط التي تحتوي على معلومات وبيانات حساب البطاقة.

2.3 أنواع المنتجات

1.2.3 المستهلك

يتم استخدام منتج المستهلك لدفع المصاريف الشخصية بجميع أنواعها. وقد تكون المنتجات الاستهلاكية بطاقات ائتمان أو بطاقات الخصم أو بطاقات الدفع مسبق. قد تكون المنتجات الاستهلاكية بطاقات عادية أو بطاقات متميزة. يرجى الرجوع إلى أدلة المنتج للمزيد من التفاصيل.

2.2.3 تجاري

الغرض من المنتج التجاري هو استخدامه لدفع مصاريف العمل، مثل نفقات الموظفين أثناء السفر للعمل، ولإسداد مقابل البضائع التجارية، وشراء المستلزمات المكتبية.

فيما يلي أمثلة على المنتجات التجارية:

- بطاقات الرواتب
 - بطاقات الأعمال الصغيرة
 - بطاقات الشركات
 - بطاقات الشراء
 - بطاقات الأسطول
- يرجى الرجوع إلى أدلة المنتج للمزيد من التفاصيل.

3.2.3 Governmental

A Governmental product is intended to be used for the payments availed, enabled or funded through the Government, such as Governmental pensions, financial subsidy services funded by the Government.

3.3 Prepaid Cards

(Category A as referenced in Chapter 1)

A Prepaid Card accesses

1. value maintained by an Issuer or a third party designated by the Issuer on behalf of the owner of the funds in the Account, the value of which shall be fully available to the owner of the funds in the Account at all times.
2. Any other permitted form of Electronic Money.

The funds may be maintained in an omnibus, segregated trust, or pooled account.

A prepaid Card may be a consumer, commercial or Governmental Card.

The Issuer must ensure compliance with all regulations of the Central Bank of Libya applicable to prepaid Card usage specific for those relevant to AML/CFT.

3.3.1 Prior Consent of the National Scheme Operator

A Member must not conduct or modify an existing Prepaid Card Program without the express prior consent of the National Scheme Operator.

Each Member request to conduct or modify a Prepaid Card Program must be submitted to, and approved by, the National Scheme Operator.

3.3.2 Reservation of rights

The National Scheme Operator reserves the right:

1. To approve or reject any Prepaid Card Program application; and
2. To require that any previously approved Prepaid Card Program be modified and/or updated on a recurring basis; and
3. To withdraw its approval of any Prepaid Card Program and require the Prepaid Card Program to be terminated. A Member has the right to request that the National Scheme Operator review the rejection or withdrawal of the approval of a Prepaid Card Program. Such a request must be submitted in writing. The request must be postmarked no later than 30 days after the date of receipt of the notice of rejection or withdrawal of approval. Any decision by the National Scheme Operator with respect to such rejection or withdrawal of approval is final and not subject to further review or other action.

3.3.3 Responsibility for the Prepaid Card Program

An Issuer is responsible for its Prepaid Card Programs, the Prepaid Card Program funds associated with those Prepaid Card Programs, and for the actions (or inaction) of any agents it uses in connection with such Prepaid Card Programs. The National Scheme Operator determines if an Issuer is in compliance with the foregoing requirements.

3.2.3 حكومية

الغرض من المنتج الحكومي هو استخدامه للمدفوعات التي يتم توفيرها أو تمويلها من خلال الحكومة، مثل المعاشات الحكومية وخدمات الدعم المالي التي تمويلها الحكومة.

3.3 بطاقات الدفع المسبق

(الفئة أ كما هو مشار إليه في الفصل 1)

ما يمكن الوصول إليه عن طريق بطاقة الدفع المسبق:

1. القيمة التي تحتفظ بها جهة الإصدار، أو طرف ثالث تعينه جهة الإصدار نيابة عن مالك الأموال في الحساب، يجب أن تكون قيمتها متاحة بالكامل للتصرف من قبل مالك الأموال في الحساب في جميع الأوقات.

2. أي شكل آخر مسموح به من النقود الإلكترونية.

يمكن الاحتفاظ بالأموال في حساب ائتماني شامل أو ائتماني منفصل أو مجمع.

قد تكون بطاقة الدفع المسبق بطاقة استهلاكية أو تجارية أو حكومية.

يجب أن تضمن جهة الإصدار الامتثال لجميع لوائح مصرف ليبيا المركزي المطبقة على استخدام بطاقة الدفع المسبق والخاصة بمكافحة غسيل الأموال وتمويل الإرهاب.

1.3.3 الموافقة المسبقة لمشغل شبكة الدفع المحلية

يجب على العضو عدم إصدار أو تعديل برنامج بطاقات الدفع المسبق دون الحصول على الموافقة المكتوبة مسبقاً من مشغل شبكة الدفع المحلية.

يجب تقديم طلب كل عضو إصدار برنامج بطاقات الدفع المسبق أو تعديله إلى مشغل شبكة الدفع المحلية للموافقة عليه.

2.3.3 حفظ الحقوق

يحتفظ مشغل شبكة الدفع المحلية بالحقوق في:

1. الموافقة على أي طلب متعلق ببرنامج بطاقات الدفع المسبق.
 2. المطالبة بتعديل، أو تحديث أي برنامج لبطاقات الدفع المسبق تمت الموافقة عليه مسبقاً.
 3. سحب موافقته على أي برنامج لبطاقات الدفع المسبق، وطلب إنهاء برنامج بطاقات الدفع المسبق.
- ويحق للعضو أن يطلب من مشغل شبكة الدفع المحلية مراجعة قرار الرفض أو سحب الموافقة على برنامج بطاقات الدفع المسبق. ويجب أن يكون طلب المراجعة مكتوباً ومرسلاً بعلم الوصول، في مدة لا تتجاوز 30 يوماً من تاريخ إشعار الرفض أو سحب الموافقة. أي قرار صادر من مشغل شبكة الدفع المحلية والمتعلق بالفصل في طلب المراجعة، يعد قرار نهائي.

3.3.3 المسؤولية عن برنامج بطاقات الدفع المسبق

تعد جهة الإصدار هي الجهة المسؤولة عن برامج بطاقات الدفع المسبق، وأموال برامج بطاقات الدفع المسبق المرتبطة ببرامج بطاقات الدفع المسبق، وعن تصرفات وكلاءها الذين ي فيما يتعلق ببرامج بطاقات الدفع المسبق. ويحدد مشغل شبكة الدفع المحلية مدى امتثال جهة الإصدار للقواعد المحددة.

3.3.4 Categories of Prepaid Card Programs

The National Scheme Operator categorizes Prepaid Card Programs into three categories: consumer, commercial, and government. The National Scheme Operator has the right to adopt additional and/or review the current categories of Prepaid Card Programs from time to time in its sole discretion.

3.3.5 Return of Unspent Value

An Issuer must have in place appropriate procedures to permit the return of the remaining balance on a prepaid Card at the time of closure or expiry, including documentation of the closure of the Account and verification of the identity of the person receiving the remaining balance.

Consumer Prepaid Card Programs

An Issuer of Consumer Prepaid Card Programs must provide the consumer with a minimum of 12 months from the date of the last value load or 30 days after the expiration date, whichever comes later, to request the return of unspent funds, less any applicable fees imposed by the Issuer or any other lawful offsets. Prominent disclosure must be made to the consumer as to how and when to request the refund of unspent funds and as to any fees that apply to the Prepaid Card Program.

Once the consumer submits a refund request, the consumer must receive a refund of unspent funds within 30 days of the date on which the refund request was received by the Issuer.

Commercial Prepaid Card Programs

The Issuer of a Commercial Prepaid Card Program must provide the commercial entity or individual or other third party designated by the commercial entity or consumer with a minimum of 30 days, or as otherwise approved by the National Scheme Operator, to spend the funds in the prepaid Account, after which time the funds revert to the commercial entity or as otherwise agreed between the commercial entity and the Issuer or its agents.

Government Prepaid Card Programs

If the owner of the funds in the prepaid Account is a government entity, then the Issuer of the Government Prepaid Card Program must provide the government entity with a minimum of 15 days, or as otherwise approved by the National Scheme Operator, to spend the funds in the prepaid Account, after which time the funds revert to the government entity or as otherwise agreed between the government entity and the Issuer or its agents.

If the owner of the funds in the prepaid Account is a consumer, then the Issuer of the Government Prepaid Card Program must provide the consumer with a minimum of [12] months from the date of the last value load or 30 days after the expiration date, whichever comes later, to request the return of unspent funds, less any applicable fees imposed by the Issuer or any other lawful offsets. Prominent disclosure must be made to the consumer as to how and when to request the refund of unspent funds and as to any fees that apply to the Prepaid Card Program.

Once the consumer submits a refund request, the consumer must receive a refund of unspent funds within 30 days of the date on which the refund request was received by the Issuer.

4.3.3 فئات برامج بطاقات الدفع المسبق

يصنف مشغل شبكة الدفع المحلية برامج بطاقات الدفع المسبق إلى ثلاث فئات: بطاقات المستهلك، والبطاقات التجارية، والبطاقات الحكومية. يحق مشغل شبكة الدفع المحلية اعتماد فئات إضافية، ومراجعة الفئات الحالية لبرامج بطاقات الدفع المسبق من وقت لآخر وفقاً لسلطته التقديرية.

5.3.3 إرجاع قيمة الرصيد الباقي في الحساب

تلتزم جهة الإصدار بوضع الإجراءات الواجبة الاتباع لإعادة الرصيد المتبقي في حساب بطاقات الدفع المسبق عند إغلاق الحساب أو انتهاء الصلاحية، بما في ذلك القيام بعملية توثيق إغلاق الحساب، والتحقق من هوية الشخص الذي يتلقى الرصيد المتبقي.

برامج بطاقات الدفع المسبق الاستهلاكية

تلتزم جهة إصدار برامج بطاقات الدفع المسبق الاستهلاكية، بتزويد المستهلك بكشف ما لا يقل عن 12 شهراً من تاريخ آخر تحميل للقيمة، أو بعد 30 يومًا من تاريخ انتهاء الصلاحية، أيهما يأتي لاحقًا، لطلب إعادة الرصيد الباقي، مخصصًا من أي رسوم سارية مفرضة من قبل جهة الإصدار أو أي مستحقات قانونية أخرى. ويجب عليها أن تفصح بشكل مفهوم للعميل عن كيفية ووقت طلب استرداد الرصيد الباقي، وبشأن أي رسوم تنطبق على برنامج البطاقات الدفع المسبق.

و بمجرد أن يقدم المستهلك طلب استرداد الرصيد الباقي، يجب أن يسترد المستهلك هذا الرصيد خلال 30 يومًا من تاريخ استلام جهة الإصدار لهذا الطلب.

برامج بطاقات الدفع المسبق التجارية:

تلتزم جهة إصدار بمنح برنامج بطاقات الدفع المسبق التجارية التاجر أو نائبه أو وكيله أو المستهلك خلال مدة لا تقل عن 30 يومًا، أو على النحو الذي تمت الموافقة عليه من قبل مشغل شبكة الدفع المحلية، لإنفاق الأموال في حساب الدفع المسبق، وبعد ذلك الوقت تعود الأموال إلى التاجر أو على النحو المتفق عليه بين التاجر وجهة الإصدار أو وكلائها.

برامج بطاقات الدفع المسبق الحكومية

إذا كان مالك الأموال في حساب الدفع المسبق جهة حكومية، فإن جهة إصدار ملزمة بتزويد الجهة الحكومية خلال مدة لا تقل عن 15 يومًا، أو وفقًا لما يوافق عليه مشغل شبكة الدفع المحلية، بطريقة إنفاق الأموال في حساب الدفع المسبق، وبعد ذلك الوقت تعود الأموال إلى الجهة الحكومية أو على النحو المتفق عليه بين الجهة الحكومية وجهة الإصدار أو وكلائها.

إذا كان مالك الأموال في حساب الدفع المسبق مستهلكًا، فيجب على جهة إصدار برنامج بطاقات الدفع المسبق الحكومية أن تقوم بتزويد المستهلك بكشف بما لا يقل عن [12] شهراً من تاريخ آخر تحميل للقيمة أو بعد 30 يومًا من تاريخ انتهاء الصلاحية، أيهما يأتي لاحقًا، لطلب إعادة الرصيد الباقي، مخصصًا من أي رسوم سارية تفرضها جهة الإصدار أو أي مستحقات قانونية أخرى. يجب عليها أن تفصح بشكل مفهوم للعميل عن كيفية ووقت طلب استرداد الرصيد الباقي، وبشأن أي رسوم تنطبق على برنامج بطاقة الدفع المسبق.

بمجرد أن يقوم المستهلك بتقديم طلب الاسترداد، يجب أن يسترد المستهلك الرصيد الباقي خلال 30 يومًا من تاريخ استلام جهة الإصدار لهذا الطلب.

In the case of Government Prepaid Card Programs, the funds deposited in the prepaid Account are owned by the government entity or by the consumer or other third party designated by the government entity or such consumer. If the government entity permits a consumer to deposit funds in the prepaid Account owned by the government entity, the Government Prepaid Card Program becomes a Consumer Prepaid Card Program and all relevant Consumer Prepaid Card Program requirements apply.

3.3.6 Value loading

Subject to the restrictions set forth below, the maximum load value and load parameters associated with a prepaid Account are established by the Issuer of the Prepaid Card Program and are subject to review and approval by the Central Bank of Libya.

3.3.7 Automatic Value Loads from Payment Cards

A payment card must not be used to automatically fund a purchase Transaction effected with a prepaid Account, except pursuant to an automatic value load or “top-up” arrangement agreed in advance by the Cardholder pursuant to predefined fixed parameters. For example, an automatic top-up is permitted to occur:

- In a predefined amount on a periodic time-based schedule, such as daily, weekly, or monthly; or
- In a predefined amount whenever a certain Account balance is reached (for example, an LYD 200 top-up is initiated when the Account balance reaches LYD 50). Any such predefined amount must not be increased at the time of authorization.

If an automatic top-up has occurred and the Account balance remains insufficient to fund a purchase Transaction, then the Issuer must respond to the authorization request with either a partial approval or a decline.

Notwithstanding this Rule, a Prepaid Account may be funded at any time with value accessed from another account maintained by the same Issuer or its designated agent for or on behalf of the same Cardholder.

3.3.8 Communication and Marketing Materials

If an Issuer’s prepaid Cards are intended to be used by Cardholders for personal, family or household use, then the Issuer must provide Cardholders with the terms and conditions of the Prepaid Card Program before any purchase is made or activation fees are incurred.

If the Issuer’s prepaid Cards are intended to be used by Cardholder for business use, then the Issuer must provide the commercial entity or government entity with the terms and conditions of the Prepaid Card Program before any purchase is made or activation fees are incurred.

Thereafter, the Issuer must provide the respective Cardholder, commercial entity or government entity with any amendment or modifications thereto and, in particular, make clear and conspicuous disclosures with respect to all fees to be incurred by the prepaid Account holder to obtain, use, reload, maintain and/or cash out the balance in the prepaid Account or for any other use, as required by the Standards and applicable law.

Press releases must be submitted for review and consent to the National Scheme Operator prior to the launch or subsequent modification of any Prepaid Card Program and prior to any marketing of the Prepaid Card Program.

في حالة برامج بطاقات الدفع المسبق الحكومية، تكون الأموال المودعة في الحساب المدفوع مسبقًا مملوكة للجهة الحكومية أو المستهلك أو أي طرف ثالث معين من قبل الجهة الحكومية أو المستهلك. وإذا وافقت الجهة الحكومية على طلب المستهلك بإيداع الأموال في الحساب المدفوع مسبقًا المملوك للجهة الحكومية، فإن برنامج البطاقة الحكومية مسبق الدفع يصبح برنامج بطاقة دفع مسبق استهلاكية، وتطبق عليها في هذه الحالة القواعد المنظمة برنامج بطاقات الدفع المسبق الاستهلاكية.

6.3.3 تحميل القيمة

وفقًا للقيود الموضحة أدناه، يتم تحديد الحد الأقصى لقيمة التحميل ومعلومات التحميل المرتبطة بحساب الدفع المسبق من قبل جهة الإصدار، وتخضع للمراجعة والموافقة من قبل مصرف ليبيا المركزي.

7.3.3 تحميل القيمة تلقائيًا من بطاقات الدفع

يجب عدم استخدام بطاقة الدفع المسبق للقيام بعملية شراء تلقائية باستخدام حساب الدفع المسبق، إلا وفقًا لتحميل القيمة التلقائي أو ترتيب “إعادة تعبئة” المتفق عليه مسبقًا من قبل حامل البطاقة وفقًا لمعايير ثابتة محددة مسبقًا. على سبيل المثال، يُسمح بحدوث إعادة تعبئة تلقائية:

- بمبلغ محدد مسبقًا وفقًا لجدول زمني دوري، قد يكون يومي أو أسبوعي أو شهري.
- بمبلغ محدد مسبقًا كلما تم الوصول إلى رصيد حساب معين (على سبيل المثال، يتم بدء شحن البطاقة بـ 200 دينار ليبي عندما يصل رصيد الحساب إلى 50 دينارًا ليبيًا). ويجب عدم زيادة أي مبلغ محدد مسبقًا إلا بعد الحصول على الإذن بذلك.

في حالة حدوث زيادة تلقائية وكان الرصيد في الحساب غير كافٍ للقيام بعملية شراء، فإن جهة الإصدار لها الحق في الاستجابة لطلب الإذن إما بموافقة عليه جزئيًا أو رفضه.

وعلى الرغم من ذلك، فإنه يجوز تمويل حساب الدفع المسبق في أي وقت بقيمة يتم الوصول إليها من حساب آخر تحتفظ به جهة الإصدار ذاتها، أو وكيلها المعين لحامل البطاقة نفسه أو نائبه.

8.3.3 مواد الاتصال والتسويق

إذا كان المقصود من بطاقات الدفع المسبق الخاصة بجهة الإصدار أن يستخدمها حاملو البطاقات للاستخدام الشخصي أو العائلي أو المنزلي، فيجب على جهة الإصدار تزويد حاملي البطاقات بشروط وأحكام برنامج بطاقة الدفع المسبق قبل إجراء أي عملية شراء، و أن تحدد تكاليف رسوم تفعيل الخدمة.

إذا كان المقصود من بطاقات الدفع المسبق الخاصة بجهة الإصدار أن يستخدمها حامل البطاقة للاستخدام التجاري، فيجب على جهة الإصدار تزويد التاجر أو الجهة الحكومية بقواعد وشروط برنامج بطاقة الدفع المسبق قبل إجراء أي عملية شراء، و أن تحدد تكاليف رسوم تفعيل الخدمة.

تلتزم جهة الإصدار بتزويد حامل البطاقة أو التاجر أو الجهة الحكومية بأي تعديلات أو تغييرات عليها، وعلى وجه الخصوص، تقديم إفصاحات واضحة وظاهرة فيما يتعلق بجميع الرسوم التي يتحملها صاحب حساب الدفع مسبق للحصول على استخدام الرصيد أو إعادة تحميله، أو الاحتفاظ به، أو لأي استخدام آخر، وفقًا لما تتطلبه المعايير والقانون المعمول به.

يجب تقديم البيانات الصحفية لمراجعتها والموافقة عليها من قبل مشغل شبكة الدفع المحلية، وذلك قبل إطلاق أو القيام بالتعديل اللاحق لأي برنامج لبطاقة الدفع المسبق، وقبل أي تسويق لبرنامج بطاقات الدفع المسبق.

Upon request, an Issuer must submit all communications and marketing materials including, but not limited to, printed materials and copies or electronic versions of websites and mobile applications, card carriers, websites, welcome letters, consumer applications, and terms and conditions if any, for all Prepaid Card Programs to the National Scheme Operator for review and consent prior to the launch or subsequent modification of the Prepaid Card Program and prior to any marketing of the Prepaid Card Program.

The National Scheme Operator review is limited to compliance with the Standards for Issuer communications. Each Issuer is responsible for ensuring that its Prepaid Card Program communication and marketing materials comply with applicable law and the Standards. An Issuer of prepaid Cards intended to be used by Cardholders for personal, family or household use must inform Cardholders that, in the event that the available amount in the prepaid Account is less than the purchase amount, some Merchants might not allow the Cardholder to combine multiple payment types (such as cash, check or another payment card) to complete the Transaction. Issuers of prepaid Cards intended to be used by Cardholders for business use must inform the commercial entity or government entity of the foregoing.

An Issuer of prepaid Cards intended to be used by Cardholders for personal, family or household use must inform Cardholders if their prepaid Cards are linked to a selective authorization Program. Issuers of prepaid Cards intended to be used by Cardholders for business use must inform the commercial entity or government entity of the foregoing.

3.4 Non-Personalized Prepaid Card Programs

(Category A as referenced in Chapter 1)

Prepaid Card Programs for which the Issuer does not collect, store or otherwise validate the consumer's identity are subject to specific limitations. Refer to the product guides for further information.

An Issuer must use dedicated BINs for Prepaid Card Programs. In the event of dispute or uncertainty, the National Scheme Operator determines, in its sole discretion, BINs for an Issuer's Prepaid Card Programs.

3.4.1 Ownership and Control of the Co-brand Program

A Co-brand Card Program must get first a written permissions and/approvals from CBL or to whom delegated this authority. Hence the Issuer at all times, and the co-brand partner must not own or control any part of the Program or the Program receivables. However, the assignment of receivables or sale of a participation in receivables to the partner, or some other financing vehicle involving the partner, is permitted provided the Program is owned and Controlled by the Member.

عندما يطلب منها ذلك، تلتزم جهة الإصدار بتقديم جميع الاتصالات والمواد التسويقية، بما في ذلك، على سبيل المثال لا الحصر، المواد المطبوعة والمنسوخة أو الإصدارات الإلكترونية من مواقع الويب وتطبيقات الهاتف المحمول، وحاملو البطاقات، والمواقع الإلكترونية، رسائل الترحيب، وتطبيقات المستهلك، والشروط والأحكام إن وجدت، لجميع برامج بطاقات الدفع المسبق لمشغل شبكة الدفع المحلية للمراجعة والموافقة قبل إطلاق البرنامج أو إدخال تعديلات لاحقة عليه، وذلك قبل أي تسويق لبرنامج بطاقة الدفع المسبق.

وتقتصر مراجعة مشغل شبكة الدفع المحلية على مدى الامتثال لمعايير اتصالات جهة الإصدار. وتحمل كل جهة إصدار مسؤولية ضمان توافق مواد الاتصال والتسويق الخاصة ببرنامج بطاقات الدفع المسبق مع القانون والمعايير المعمول بها.

يجب على جهة إصدار بطاقات الدفع المسبق، والمخصصة لاستخدامها من قبل حاملي البطاقات للاستخدام الشخصي أو العائلي أو المنزلي، إعلام حاملي البطاقات بأنه في حالة أن المبلغ المتاح في حساب الدفع المسبق أقل من عملية الشراء، فقد لا يسمح بعض التجار لحامل البطاقة بدمج أنواع دفع متعددة (مثل نقدًا أو بشيك أو ببطاقة دفع أخرى) لإنجاز عملية الشراء.

كما يجب على جهة إصدار بطاقات الدفع المسبق، والمزمع استخدامها من قبل حاملي البطاقات للاستخدام التجاري إبلاغ التاجر أو الجهة الحكومية بما سبق.

يجب على جهة إصدار بطاقات الدفع المسبق والمزمع استخدامها من قبل حاملي البطاقات للاستخدام الشخصي أو العائلي أو المنزلي، إعلام حاملي البطاقات إذا كانت بطاقتهم المدفوعة مسبقًا مرتبطة ببرنامج ترخيص انتقائي. يجب على جهات إصدار بطاقات الدفع المسبق والمزمع استخدامها من قبل حاملي البطاقات للاستخدام التجاري إعلام التاجر أو الجهة الحكومي بما سبق.

4.3 برامج بطاقات الدفع المسبق غير المخصصة

(الفئة أ كما هو مشار إليه في الفصل 1)

تخضع برامج بطاقات الدفع المسبق التي لا تقوم فيها جهة الإصدار بجمع هوية المستهلك أو تخزينها أو التحقق من صحتها لقيود محددة. يرجى الرجوع إلى أدلة المنتج للمزيد من المعلومات.

يجب على جهة الإصدار استخدام أرقام التعريف المصرفية المخصصة لبرامج بطاقات الدفع المسبق. وفي حالة حدوث منازعة، أو عدم التحقق، يحدد مشغل شبكة الدفع المحلية، وفقًا لسلطته التقديرية، أرقام التعريف المصرفية لبرامج بطاقات الدفع المسبق الخاصة بجهة الإصدار.

1.4.3 الملكية والتحكم في برنامج العلامة التجارية المشتركة

Translation is too long to be saved

يجب أن يحصل برنامج البطاقة ذات العلامة التجارية المشتركة أولاً على أذونات و / موافقات مكتوبة من مصرف ليبيا المركزي أو ممن فوض له هذه السلطة. ومن ثم وفي جميع الاوقات، يجب ألا تمتلك الجهة المصدرة وشريك العلامة التجارية المشتركة أو يتحكم في أي جزء من البرنامج أو الذمم المدينة للبرنامج. ومع ذلك ، يُسمح بالتنازل عن المستحقات أو بيع المشاركة في المستحقات للشريك ، أو بعض وسائل التمويل الأخرى التي تنطوي على الشريك ، بشرط أن يكون البرنامج مملوكًا ويتحكم فيه العضو.

3.4.2 Use of the Acceptance Brand Logos

An acceptance brand logo displayed at the POI must appear apart from any co-brand partner identification and must at least have parity in size and prominence with any Program logo, Program name, or the like, and with any competing mark also displayed. The National Scheme Operator has the right to require the modification or removal of any POI display of a Program name or logo that the National Scheme Operator determines does not comply with this Rule or reflects negatively on NUMO brand.

3.5 Proprietary Accounts

(Category A as referenced in Chapter 1)

Subject to the approval of the National Scheme Operator, a NUMO Card is permitted to also provide access to a third-party proprietary account, proprietary application, or both.

Access may be provided to:

1. a proprietary account through a Co-brand Card Program at the partner's own Merchant locations or at other Merchants that participate in the partner's services;
2. proprietary stored value residing on the Card's magnetic stripe or chip.
3. a non-payment application residing on the Card, such as a loyalty application, an electronic coupon, medical information, or paperless ticketing. The technology employed by the non-payment application must not facilitate or otherwise enable the use of a competitive payment product for the non-payment benefit or service.

3.5.1 Proprietary Account Access

A proprietary account number may have one or more of the following characteristics:

1. The proprietary account number is different from the primary account number (PAN) associated with the Member Account. The proprietary account number may appear on the Card face, be encoded on the Card, or be cross-referenced in the Member's or Partner's systems.
2. The proprietary account number is used in a system or network for authorization and settlement that is distinct from the Interchange System, and is not used in the Interchange System.
3. Any Cardholder billing related to use of the proprietary account number is distinct from any billing for the Member Account, whether as part of a common statement or in a separate statement.

3.5.2 Proprietary Account Types

A proprietary account is permitted to be present on a Card for the following functionalities:

1. Campus cards
2. Door payment devices
3. Loyalty applications
4. Cardholder reference numbers
5. Electronic coupons
6. Medical information
7. Paperless ticketing
8. Any functionality otherwise expressly approved in writing by the National Scheme Operator.

The National Scheme Operator exclusively determines if a proprietary account number is permitted to be used on a Card.

2.4.3 استخدام شعارات العلامة التجارية المقبولة

يجب أن يظهر شعار العلامة التجارية للقبول المعروض في نقطة التفاعل وبدون التقييد بتحديد هوية الشريك في العلامة التجارية المشتركة، ويجب أن يكون له على الأقل الحق في التكافؤ في الحقوق الممنوحة لأي شعار برنامج أو اسم برنامج أو ما شابه، ومع عرض أي علامة تجارية منافسة. يجوز لمشغل شبكة الدفع المحلية أن يطلب تعديل أو إزالة أي عرض نقطة التفاعل لاسم البرنامج أو الشعار الذي يقرر مشغل شبكة الدفع المحلية أنه لا يتوافق مع هذه القاعدة، أو ينعكس سلباً على علامة (نمو) التجارية.

5.3 حسابات الملكية

(الفئة أ كما هو مشار إليه في الفصل 1)

هذه الحسابات خاضعة لموافقة مشغل شبكة الدفع المحلية، ويُسمح أيضًا لبطاقة (نمو) بالوصول إلى حساب مملوك لشخص ثالث أو تطبيق خاص أو كليهما.

يمكن توفير الوصول إلى:

1. لحساب ملكية من خلال برنامج بطاقة ذات علامة تجارية مشتركة في مواقع التجار الخاصة بالشريك، أو لدى التجار الآخرين الذين يساهمون في خدمات الشريك.
2. القيمة المقيدة في حساب الملكية والموجودة على الشريط المغناطيسي للبطاقة أو الشريحة.
3. تطبيق عدم الدفع الموجود على البطاقة، مثل تطبيق الولاء، أو القسيمة الإلكترونية، أو المعلومات الطبية، أو التذاكر غير الورقية. ويجب ألا تساعد التكنولوجيا التي يستخدمها تطبيق عدم الدفع في استخدام منتج دفع تنافسي لمزايا و خدمة عدم الدفع.

1.5.3 الوصول إلى حساب الملكية

قد يحتوي رقم حساب الملكية على واحدة أو أكثر من الخصائص التالية:

1. يختلف رقم حساب الملكية عن رقم الحساب الأساسي المرتبط بحساب العضو. وقد يظهر رقم حساب الملكية على وجه البطاقة، أو يتم ترميزه على البطاقة، أو يتم الرجوع إليه في أنظمة العضو أو الشريك.
2. يتم استخدام رقم حساب الملكية في نظام أو شبكة للتصريح والتسوية التي تختلف عن نظام التبادل، ولا يتم استخدامها في نظام التبادل.
3. فواتير حامل البطاقة التي تتعلق باستخدام رقم حساب الملكية تختلف عن فواتير حساب العضو، سواء كانت جزء من بيان مشترك أو كانت بيان منفصل.

2.5.3 أنواع حسابات الملكية

يُسمح بوجود حساب ملكية على البطاقة للقيام بالوظائف التالية:

1. بطاقات الحرم الجامعي.
2. أجهزة الدفع بالباب.
3. طلبات الولاء
4. الأرقام المرجعية لحامل البطاقة.
5. القسائم الإلكترونية.
6. المعلومات الطبية.
7. التذاكر غير الورقية.
8. أي وظيفة تمت الموافقة عليها بشكل مكتوب من قبل مشغل شبكة الدفع المحلية. يختص مشغل شبكة الدفع المحلية وحده بتحديد ما إذا كان رقم حساب الملكية مخصصاً باستخدامه على البطاقة أم غير مخصص باستخدامه.

3.5.3 Fees and Reporting Requirements

From time to time, the National Scheme Operator has the right to establish, implement, and collect fees, assessments, or both arising from or related to proprietary accounts.

The Member must separately report to the National Scheme Operator the number of Cards outstanding, the proprietary account sales volume on such Cards, and any other requested information in the form and at such times as the National Scheme Operator requires.

3.6 Virtual Accounts

(Category A as referenced in Chapter 1)

Subject to the requirements set forth below, a Member is not required to issue a physical Card in connection with or which links to a Virtual Account.

For the avoidance of doubt, an Account PAN Tokenized for use on a Mobile Payment Device is not considered a Virtual Account.

An Issuer of a Virtual Account must comply with all of the following requirements:

1. A Virtual Account must be assigned a primary account number (PAN), a Card Verification Value (CVV) value and an expiration date.
2. A reference device is permitted to be used to communicate this information, but must not be designed in a manner that could cause consumer or acceptance confusion with a Card (such as the inclusion of artwork that would resemble a magnetic stripe or EMV chip).
3. Before activating a Virtual Account, the Issuer must communicate to the Cardholder the PAN and the expiration date of the Account, the identity of the Issuer, and instructions as to the manner in which the Virtual Account is permitted to be used.

The National Scheme Operator recommends that the Issuer prominently disclose upon issuance that the Virtual Account should not be used to purchase an item over the Internet that subsequently would require presentment of a physical reference device in order to obtain that item.

Examples include certain theater ticket purchases, hotel stays, car rentals, and online purchases picked up in person.

3.7 Youth Card Programs

(Category A as referenced in Chapter 1)

Solely for the purposes of this Section, the following terms have the meanings set forth below:

1. “Minor” or “Youth” means a person under the age of majority as determined by the laws of Libya, Example is the currently issued Student card.
2. “Primary Cardholder” means the Cardholder authorized to use the Card and to be financially responsible for the Card.
3. “Youth Card” means a Card issued to a Minor as a Primary Cardholder. For clarity, a Card issued to a Minor at the request of the Primary Cardholder and bearing the same Primary Account Number as the Card issued to the Primary Cardholder is not a Youth Card if the Primary Cardholder is responsible for use of the Card.

An Issuer of a Youth Card has the right to restrict use of the Card by the Merchant category code (MCC), including cash access restrictions.

3.5.3 الرسوم ومتطلبات الإبلاغ

يجوز لمشغل شبكة الدفع المحلية من وقت لآخر إنشاء وتنفيذ وجمع الرسوم وإجراء عمليات التقييم أو كليهما الناشئة عن حسابات الملكية.

يلتزم كل عضو بإعلام مشغل شبكة الدفع المحلية بشكل مفصل عن عدد البطاقات المعلقة، وحجم مبيعات حسابات الملكية لهذه البطاقات، وأي معلومات أخرى مطلوبة في النموذج المعد لذلك، وفي الأوقات التي يحددها مشغل شبكة الدفع المحلية.

6.3 الحسابات الافتراضية

(الفئة أ كما هو مشار إليه في الفصل 1)

لا يُطلب من العضو إصدار بطاقة فعلية فيما يتعلق بحساب افتراضي أو يرتبط به.

لا يُعتبر ترميز رقم حساب أساسي للاستخدام على جهاز الدفع عبر الهاتف المحمول حسابًا افتراضيًا.

يجب أن تلتزم جهة إصدار الحساب الافتراضي بجميع القواعد التالية:

1. يجب تحديد رقم حساب أساسي للحساب الافتراضي، وتحديد قيمة التحقق من البطاقة وتاريخ انتهاء صلاحيتها.
2. يُسمح باستخدام جهاز مرجعي لإيصال هذه المعلومات، ولكن يجب ألا يتم تصميمه بطريقة لا يستوعبها المستهلك أو القبول بالبطاقة (مثل تضمين عمل فني يشبه الشريط المغناطيسي أو شريحة EMV).
3. قبل تفعيل الحساب الافتراضي، تلتزم جهة الإصدار بإعلام حامل البطاقة برقم الحساب الأساسي، وتاريخ انتهاء صلاحية الحساب، وهوية جهة الإصدار، والتعليمات المتعلقة بالطريقة التي يُسمح بها استخدام الحساب الافتراضي.

يوصي مشغل شبكة الدفع المحلية جهة الإصدار بأن تكشف بوضوح عند الإصدار؛ على أنه لا ينبغي استخدام الحساب الافتراضي للشراء عبر الإنترنت؛ والذي سيتطلب لاحقًا تقديم جهاز مرجعي مادي من أجل الحصول على هذا الشراء.

تشمل الأمثلة مشتريات معينة من تذاكر المسرح، والإقامات في الفنادق، وتأجير السيارات، والمشتريات عبر الإنترنت التي يتم انتقاؤها شخصيًا.

7.3 برامج بطاقات الشباب

(الفئة أ كما هو مشار إليه في الفصل 1)

لأغراض تطبيق هذا البرنامج، يقصد بالمصطلحات التالية المعاني الموضحة أمامها:

1. “القاصر” هو ذلك الشخص الذي لم يبلغ سن الرشد (18 سنة) على النحو الذي تحدده قوانين الدولة الليبية، ومن الأمثلة على ذلك بطاقة منحة الطالب الصادرة حديثًا.
2. “حامل البطاقة الأساسية” يعني حامل البطاقة المرخص له باستخدامها، ويكون مسؤولاً عن استخدام البطاقة، في حدود التشريعات النافذة.
3. “بطاقة الشباب” هي تلك البطاقة الصادرة للقاصر للطالب كحامل بطاقة أساسية. ولتوضيح ذلك، فإن البطاقة الصادرة للقاصر للشباب بناءً على طلب حامل البطاقة الأساسية، وتحمل نفس رقم الحساب الأساسي مثل البطاقة الصادرة لحامل البطاقة الأساسية ليست بطاقة شبابية إذا كان حامل البطاقة الأساسية مسؤولاً عن استخدام البطاقة.

ويجوز لجهة إصدار بطاقات الشباب تقييد استخدامها بواسطة رمز فئة التاجر، بما في ذلك قيود الوصول إلى العمليات النقدية.

3.7.1 Appeal and Disclosure Requirements

Prior to use, an Issuer must submit all Youth Card Program communications and marketing materials for any Prepaid Card Program including, but not limited to, printed materials and copies or electronic versions of websites and mobile applications, advertisements, card carriers, press releases, websites, welcome letters, marketing plans such as product announcements and program advertisements, consumer applications, and terms and conditions, if any, to the National Scheme Operator for review and must not use any such materials without the express approval of the National Scheme Operator.

3.8 Card Requirements

3.8.1 Principles of Standardization

(Category A as referenced in Chapter 1)

All Cards must be usable in all standard magnetic stripe Card-reading devices and in all hybrid terminals and devices, so that the electronic interchange of Transaction data is possible.

All embossed Cards must be usable in all standard imprinters—the embossed information must produce a clear imprint and comply with all positioning and type font Standards.

All Cards containing a chip must be EMV-compliant. Such Cards are called Chip Cards. All Chip Cards must have a single primary application defined by the National Scheme Operator that resides on the chip and on the magnetic stripe; the Account information appearing on the Card front must be for the primary application resident on the magnetic stripe. No payment application resident on the chip is permitted to have a higher application priority than the Card's primary application.

All Payment Applications on a Chip Card must have a valid date (if applicable) and expiration date within or the same as the dates present on the Card front. The valid dates appearing on the Card front must be those of the primary application on the Card.

All Issuers must comply with the Card Design Standards, including but not limited to requirements relating to the following:

- Physical Card materials, dimensions, and measurements for the Card's embossing, magnetic stripe, chip, Marks, and other Card features
- Card design
- Use of Card activation and selective authorization disclosure stickers.

1.7.3 متطلبات الاستئناف والإفصاح

تلتزم جهة الإصدار قبل الاستخدام، بتقديم جميع اتصالات برنامج بطاقات الشباب والمواد التسويقية لأي برنامج لبطاقات الدفع المسبق بما في ذلك، على سبيل المثال لا الحصر، المواد المطبوعة والمنسوخة و الإصدارات الإلكترونية من مواقع الويب وتطبيقات الهواتف المحمولة والإعلانات وشركات البطاقات والبيانات الصحفية والمواقع الإلكترونية رسائل الترحيب وخطط التسويق مثل إعلانات المنتجات وإعلانات البرامج وتطبيقات المستهلك والشروط والأحكام، إن وجدت، مشغل شبكة الدفع المحلية للمراجعة.

وفي جميع الاحوال يجب عدم استخدام أي من هذه المواد دون الحصول على الموافقة المكتوبة المسبقة من مشغل شبكة الدفع المحلية.

8.3 متطلبات البطاقة

1.8.3 مبادئ التوحيد القياسي

(الفئة أ كما هو مشار إليه في الفصل 1)

يجب أن تكون جميع البطاقات قابلة للاستخدام في جميع أجهزة قراءة البطاقات ذات الشريط المغناطيسي القياسي، وفي جميع الأجهزة الطرفية والأجهزة المختلطة، بحيث يكون التبادل الإلكتروني لبيانات المعاملات ممكنًا.

يجب أن تكون جميع البطاقات المنقوشة قابلة للاستخدام في جميع أدوات الطباعة القياسية، يجب أن تنتج المعلومات المنقوشة بصمة واضحة، وتتوافق مع جميع معايير تحديد الموضع والخط.

يجب أن تكون جميع البطاقات التي تحتوي على شريحة متوافقة مع معيار EMV- وتسمى هذه البطاقات ببطاقات الشريحة. يجب أن تحتوي جميع بطاقات الشريحة الإلكترونية على تطبيق أساسي واحد، يحدده مشغل شبكة الدفع المحلية، يكون مثبت على الشريحة وعلى الشريط المغناطيسي. معلومات التطبيق الظاهرة على الوجه الامامي للبطاقة يجب أن تكون للتطبيق الأساسي والمقيم على الشريط المغناطيسي. ولا يُسمح لأي تطبيق دفع مقيم على الشريحة بالحصول على أولوية تطبيق أعلى من التطبيق الأساسي للبطاقة.

يجب أن يكون لجميع طلبات الدفع على البطاقات ذات الشريحة الإلكترونية تاريخ صالح (إن وجد) وتاريخ انتهاء صلاحية موجودة على الوجه الامامي للبطاقة. يجب أن تكون تواريخ الصلاحية التي تظهر على الوجه الامامي للبطاقة هي تلك الخاصة بالتطبيق الأساسي على البطاقة.

يجب على جميع جهات الإصدار الالتزام بمعايير تصميم البطاقة، بما في ذلك على سبيل المثال لا الحصر القواعد المتعلقة بما يلي:

- مواد البطاقة المادية، والأبعاد والقياسات لنقش البطاقة والشريط المغناطيسي والشريحة والعلامات وميزات البطاقة الأخرى.
- تصميم البطاقة.
- استخدام تنشيط البطاقة وملصقات الكشف عن التصريح الانتقائي.

3.8.2 Account Range and BIN Use

(Category A as referenced in Chapter 1)

The National Scheme Operator has the right to assign a Member that engages in or is approved by the National Scheme Operator to engage in Activity one or more bank identification numbers (BINs).

The National Scheme Operator has the right to assign BINs at its discretion from the following range:

NUMO: [xxx] [to be completed by National Scheme Operator]

Use of a BIN must not be sublicensed or re-assigned or otherwise transferred without the prior express written consent of the National Scheme Operator.

The National Scheme Operator has the right to:

- Review a Member's BIN usage for compliance with the Standards; and
- Retract the assignment of any BIN that has been assigned to a Member.

3.8.3 Primary Account Number

(Category A as referenced in Chapter 1)

The primary account number (PAN) must be 16 digits or 19 digits in length.

A PAN begins with a BIN in the range of xxx to xxx.

3.8.4 Signature Panel

(Category B as referenced in Chapter 1)

The signature panel is not a required Card element. If the optional signature panel is included on a Card, please consult Chapter 6 for the applicable Card specifications.

If the Card has a signature panel, the Issuer must include written notice to the Cardholder preferentially sign the Card when received and before initial use.

Only the authorized Cardholder (the person whose name appears on the Card) has the right to sign the signature panel on the Card back. The Issuer must state this as a condition of Card use, if the Card has a signature panel.

A Fleet Card assigned to a particular vehicle does not have to be signed.

3.8.5 Magnetic Stripe Encoding

(Category A as referenced in Chapter 1)

The specifications for the physical and magnetic characteristics of the magnetic stripe on Cards must comply with ISO/IEC 7813 (Information technology—Identification cards—Financial transaction cards). Production of Card plastics with low coercivity magnetic tape is prohibited.

The Issuer of a Card must ensure that the encoded magnetic stripe contains Track 1 and Track 2 data, and also includes the information specified in this Chapter.

For a Debit Card, only the encoding of Track 2 data is required; the encoding of Track 1 data is optional.

If Track 3 is encoded, the encoding must comply with ISO/IEC 4909 (Identification cards—Financial transaction cards—Magnetic stripe data content for Track 3).

2.8.3 نطاق الحساب واستخدام رقم التعريف المصرفي

(الفئة أ كما هو مشار إليه في الفصل 1)

يجوز لمشغل شبكة الدفع المحلية تعيين أي عضو يشارك في تفعيل رقم تعريف مصرفي واحد أو أكثر.

يجوز لمشغل شبكة الدفع المحلية تعيين أرقام التعريف المصرفية وفقًا لسلطته التقديرية على النحو التالي:

نمو: [xxx] [يُكتمل بواسطة مشغل شبكة الدفع المحلية]

يجب ألا يتم ترخيص استخدام رقم التعريف المصرفي من الباطن أو إعادة تخصيصه أو نقله بطريقة أخرى دون الحصول على الموافقة الكتابية المسبقة من مشغل شبكة الدفع المحلية.

مشغل شبكة الدفع المحلية السلطة التقديرية في:

- مراجعة استخدام العضو لرقم التعريف المصرفي للامتثال للمعايير المحددة من قبل مشغل شبكة الدفع المحلية.
- التراجع عن تخصيص أي رقم تعريف مصرفي تم تعيينه لعضو.

3.8.3 رقم الحساب الأساسي

(الفئة أ كما هو مشار إليه في الفصل 1)

يجب أن يتكون رقم الحساب الأساسي من أعداد لا تقل 16 رقمًا ولا تزيد عن 19 رقمًا.

من ستة عشر خانة، ولا تزيد عن تسع عشرة خانة.

يبدأ رقم الحساب الأساسي برقم التعريف المصرفي في نطاق من xxx إلى xxx.

4.8.3 لوحة التوقيع

(الفئة ب كما هو مشار إليه في الفصل 1)

لوحة التوقيع ليست من العناصر المطلوبة في البطاقة. وإذا كانت لوحة التوقيع الاختيارية مضمنة في بطاقة، فيرجى الرجوع إلى الفصل 6 للتعرف على مواصفات البطاقة المعمول بها.

تلتزم جهة الإصدار إذا كانت البطاقة تحتوي على لوحة توقيع، بأن تقوم بتضمين إشعار كتابي لحامل البطاقة بشكل تفضيلي عند استلام البطاقة وقبل الاستخدام الأولي.

يجوز لحامل البطاقة فقط، والمرخص له بذلك (الشخص الذي يظهر اسمه على البطاقة) التوقيع على لوحة التوقيع الموجودة على ظهر البطاقة، ويجب على جهة الإصدار أن تقوم بذكر ذلك كشرط لاستخدام البطاقة، إذا كانت تحتوي على لوحة توقيع.

ولا يلزم التوقيع على بطاقة الأسطول المخصصة لمركبة معينة.

5.8.3 ترميز الشريط المغناطيسي

(الفئة أ كما هو مشار إليه في الفصل 1)

يجب أن تتوافق مواصفات الخصائص المادية والمغناطيسية للشريط المغناطيسي الموجود على البطاقات مع ISO / IEC 7813 (تكنولوجيا المعلومات - بطاقات التعريف - بطاقات المعاملات المالية)، ويحظر إنتاج بطاقات بلاستيكية ذات شريط مغناطيسي منخفض الإكراه.

تلتزم جهة إصدار البطاقات بالتحقق من أن الشريط المغناطيسي المشفر يحتوي على بيانات المسار 1 والمسار 2، ويتضمن أيضًا المعلومات المحددة في هذا الفصل.

وأما بالنسبة لبطاقات الخصم، يلزم فقط تشفير بيانات المسار 2؛ بينما ترميز بيانات المسار 1 ه إجراء اختياري.

وإذا تم ترميز المسار 3، فيجب أن يتوافق الترميز مع ISO / IEC 4909 (بطاقات التعريف - بطاقات المعاملات المالية - محتوى بيانات الشريط المغناطيسي للمسار 3).

3.8.5.1 Card Verification Value 1 (CVV 1)

Track 1 and Track 2 of the magnetic stripe must be encoded with a CVV 1 value.
Refer to section [3.16] for further information.

3.8.5.2 Service Code

Track 1 and Track 2 of the magnetic stripe must contain an encoded three-digit service code value.
Refer to section [5.17] for further information.

3.8.5.3 Cardholder Name

The Cardholder's name must be present on the Card front or back or both and encoded on the magnetic stripe.
The encoded Cardholder Name field in Track 1 is a variable length, alphanumeric field, with a maximum length of 26 characters within (up to) three subfields.

Due to the variable length of the field, the starting position of each remaining field depends on the ending position of the Cardholder name.
Characters “%”, “^”, and “?” cannot be used in the Cardholder Name field, because they are used only for specified encoding purposes.

Use the following specifications to encode the Cardholder name on the magnetic stripe of all Cards:

- If the Card is a Corporate Card product, the Cardholder name encoded on Track 1 and the name present on the Card should be the same, although the formats are different.

For example: MOHAMED/AHMED S

- Issuers engaged in the instant issuance and/or instant personalization of Cards or the issuance of non-personalized prepaid Cards must ensure that when a Program name appears on the Card front in place of the Cardholder name, the same Program name is also encoded in the Cardholder Name field in Track 1.
- The magnetic stripe may encode a Cardholder's title, such as Dr., Sir, or Mrs. A separator period (.) must precede the title.

For example: MOHAMED/AHMED S.DR

- If two Cardholder names are present on the same Card, encode in any of the following four formats:

MOHAMED/AHMED S or MOHAMED/ALY S or MOHAMED/AHMED ALY or

MOHAMED/AHMED S.MR MRS

- If a Card has a company name present on the Card, in addition to a Cardholder name, encode the Cardholder name.

For example:

Present on the Card: AHMED S. MOHAMED ALPHA COMPANY

Encoded on the magnetic stripe: MOHAMED/AHMED S

The subfields surname, initials or first name, and title may contain spaces. For example:

Present on the Card: RT REV AHMED J SAEED

Encoded on the magnetic stripe: SAEED/AHMED J.RT REV

1.5.8.3 قيمة التحقق من البطاقات 1 (CVV1)

يجب ترميز المسار 1 والمسار 2 للشريط المغناطيسي بقيمة التحقق من البطاقات.
راجع القسم [16.3] للمزيد من المعلومات.

2.5.8.3 رمز الخدمة

يجب أن يحتوي المسار 1 والمسار 2 للشريط المغناطيسي على قيمة رمز خدمة مشفرة مكونة من ثلاثة أرقام.
راجع القسم [17.5] للمزيد من المعلومات.

3.5.8.3 اسم حامل البطاقة

يجب أن يكون اسم حامل البطاقة موجودًا على وجه البطاقة أو ظهرها أو كليهما، ومشفرًا على الشريط المغناطيسي.
حقل اسم حامل البطاقة المشفر في المسار 1 هو حقل متغير الطول، أبجدي ورقمي، بحيث يكون في حده الأقصى 26 حرفًا وضمن ثلاثة حقول فرعية.
ونظرًا للطول المتغير للحقل، يعتمد موضع البداية لكل حقل متبقي على موضع النهاية للاسم حامل البطاقة.
الرموز والعلامات التالية “%” و “^” و “?” لا يمكن استخدامها في حقل اسم حامل البطاقة، ولكنها تستخدم فقط لأغراض التشفير المحددة.

- استخدم المواصفات التالية لتشفير اسم حامل البطاقة على الشريط المغناطيسي لجميع البطاقات:
- إذا كانت البطاقة عبارة عن منتج بطاقة شركة، فيجب أن يكون اسم حامل البطاقة المشفر في المسار 1 والاسم الموجود على البطاقة متطابقين، على الرغم من اختلاف التنسيقات.
على سبيل المثال: محمد / أحمد س
 - يجب أن تضمن جهات الإصدار المشاركة في الإصدار الفوري أو التخصيص الفوري للبطاقات أو إصدار بطاقات الدفع المسبق الغير مخصصة، أنه عند ظهور اسم البرنامج على البطاقة في مقدمة اسم حامل البطاقة، أن يتم ترميزه في حقل اسم حامل البطاقة في المسار 1.
 - قد يقوم الشريط المغناطيسي بترميز عنوان حامل البطاقة، مثل د. أو السيد أو السيدة. فيجب أن تسبقه الفاصلة (.) العنوان.
على سبيل المثال: محمد / أحمد سيد. د.
 - في حالة وجود اسمين لحامل البطاقة على نفس البطاقة، فيتم الترميز بأي من التنسيقات الأربعة التالية:
محمد / أحمد س أو محمد / علي س أو محمد / أحمد علي أو
محمد / أحمد س. سيد.
 - إذا كانت البطاقة تحمل اسم شركة موجودًا على البطاقة، بالإضافة إلى اسم حامل البطاقة، فيتم ترميز اسم حامل البطاقة.
على سبيل المثال:

موجود على البطاقة: أحمد س. محمد شركة ألفا

المشفر على الشريط المغناطيسي: محمد / أحمد س

قد يحتوي اسم الحقول الفرعية أو الأحرف أو الاسم الأول والعنوان، على مسافات فيما بينهم. على

سبيل المثال: موجود على البطاقة: RT REV AHMED J SAEED

مشفر على الشريط المغناطيسي: سعيد / أحمد جيه آر تي ريف

3.8.5.4 Expiration Date

The following requirements apply for the encoded expiration date:

- The magnetic stripe must include the encoded Account's expiration date.

Acceptable expiration date values are the following:

Year 00-99

Month 01-12

- The format for the encoded expiration date is YYMM to comply with ISO/IEC specifications.
- The encoded expiration date on Track 1 must be the same as the expiration date encoded on Track 2 and present on the Card.
- Do not encode the start date for dual dating, except as part of the Discretionary Data field on Track 1 and Track 2 of the magnetic stripe.

The maximum validity period of a Card is 5 years.

The expiration date of a Chip Card must not exceed the expiration date of any of the certificates contained within the chip.

3.9 Chip Cards

(Category A as referenced in Chapter 1)

Chip Cards, also known as integrated circuit Cards (ICC) or smart Cards, are Cards containing computer chips with memory and interactive capabilities and can be used to identify and store additional data about the Cardholder, Cardholder account, or both.

It's recommended that NUMO Cards to be Contact Chip Cards; support for EMV Mode contactless functionality is recommended.

Issuers of Chip Cards must comply with all applicable Standards, and with the EMV specifications.

The Issuer of a Chip Card must implement (CBL approved and selected Kernel) as the EMV payment application on the Card, in accordance with a current Card kernel application specification. A contact Chip Card may be an online-only Contact Chip Card. An online-only contact chip Card is configured to always require a POS Terminal to obtain online authorization from the Issuer for a Contact Chip Transaction.

The Issuer of a contact Chip Card must perform an online Card authentication method (online CAM) for each online-authorized Contact Chip Transaction by validating the Authorization Request Cryptogram (ARQC) contained in the Authorization Request or Financial Transaction Request message and populating an Authorization Response Cryptogram (ARPC), in the Authorization Request Response or Financial Transaction Request Response message.

The Issuer must define the priority of PIN verification methods within the chip.

3.9.1 Chip Card Applications

All Payment Applications must be type-approved by the National Scheme Operator, prior to Chip Card production. Furthermore, the composition of the chip, operating system (if present), and the EMV application must have successfully passed a security evaluation. Issuers must define within the chip the preferred verification method for Point-of-Interaction (POI) Transactions. A non-Member that personalizes Payment Applications acts on behalf of the Card Issuer and must conform to National Scheme Operator security Standards.

4.5.8.3 تاريخ انتهاء الصلاحية

تنطبق القواعد التالية على تاريخ انتهاء الصلاحية المشفر:

يجب أن يتضمن الشريط المغناطيسي تاريخ انتهاء صلاحية الحساب المشفر.

قيم تاريخ انتهاء الصلاحية المقبولة هي كما يلي:

السنة 00-99

الشهر 01-12

- تنسيق تاريخ انتهاء الصلاحية المشفر هو YYMM ليتوافق مع مواصفات ISO / IEC.
- يجب أن يكون تاريخ انتهاء الصلاحية المشفر على المسار 1 هو نفس تاريخ انتهاء الصلاحية المشفر في المسار 2 والموجود على البطاقة.
- لا تقم بتشفير تاريخ البدء للتاريخ المزدوج، إلا كجزء من حقل البيانات التقديرية على المسار 1 والمسار 2 للشريط المغناطيسي.

مدة صلاحية البطاقة في جميع الاحوال لا تتجاوز 5 سنوات.

يجب ألا يتجاوز تاريخ انتهاء صلاحية البطاقات ذات الشريحة الإلكترونية تاريخ انتهاء صلاحية أي من الشهادات المدرجة في الشريحة.

9.3 البطاقات ذات الشريحة

(الفئة أ كما هو مشار إليه في الفصل 1)

بطاقات الشريحة، وتعرف أيضًا باسم بطاقات الدوائر المتكاملة أو البطاقات الذكية، هي بطاقات تحتوي على شرائح كمبيوترية ذات ذاكرة وإمكانات تفاعلية، ويمكن استخدامها لتحديد وتخزين بيانات إضافية حول حامل البطاقة أو حسابه، أو كليهما.

يوصى بأن تكون بطاقات (نمو) عبارة عن بطاقات شرائح اتصال؛ ويوصى بدعم وظائف الخدمة عن بعد في وضع EMV.

تلتزم جهة إصدار بطاقات الشريحة بجميع المعايير المعمول بها ومواصفات EMV.

يجب أن تقوم جهة إصدار البطاقات ذات الشريحة الإلكترونية، بتطبيق (المرخص به من قبل مصرف ليبيا المركزي و Kernelالمختار) كتطبيق دفع EMV على هذه البطاقات، وفقًا لمواصفات تطبيق بطاقة ker- nelالحالية. وقد تكون بطاقة الشريحة الخاصة بجهة الاتصال هي بطاقة جهة اتصال فقط عبر الإنترنت. ويتم تكوين بطاقة شريحة جهة اتصال عبر الإنترنت فقط، لتطلب دائمًا جهاز نقطة بيع للحصول على ترخيص عبر الإنترنت من جهة الإصدار لمعاملة شريحة جهة اتصال.

يجب على جهة إصدار بطاقات شريحة جهة الاتصال أن تقوم بتنفيذ طريقة مصادقة البطاقة عبر الإنترنت لكل معاملة شريحة جهة اتصال مرخص بها عبر الإنترنت من خلال التحقق من تشفير طلب الترخيص الوارد في طلب الترخيص أو رسالة طلب المعاملة المالية وملء استجابة الترخيص المشفر، في رسالة استجابة طلب الترخيص أو استجابة طلب المعاملة المالية.

يجب على جهة الإصدار أن تقوم بتحديد وترتيب أولوية طرق التحقق من رقم التعريف الشخصي داخل الشريحة.

1.9.3 تطبيقات بطاقة الشريحة

قبل إنتاج الشريحة، يجب أن تتم الموافقة على جميع طلبات الدفع من قبل مشغل شبكة الدفع المحلية. إضافة إلى ذلك، يجب أن يكون تكوين الشريحة ونظام التشغيل (إن وجد) وتطبيق EMV قد اجتاز بنجاح الاختبار التقييم الأمني. كما يجب أن تحدد جهات الإصدار داخل الشريحة طريقة التحقق المفضلة لمعاملات نقطة التفاعل. يجب أن يكون تصنيف الشخص غير العضو والذي يقوم بتخصيص تطبيقات الدفع نيابة عن جهة الإصدار متوافقاً مع معايير الأمان المحددة من قبل مشغل شبكة الدفع المحلية.

Prior to Chip Card production, purchase, and distribution, Issuers must confirm with their vendor(s) that the Chip Card will be on the list of approved chip products over the intended period of issuance and adjust their procurement quantities accordingly.

3.9.2 Integrated Circuit Chip Providers

An Issuer must obtain all EMV chips for embedding on a Card from an EMV chip manufacturer that has been approved in advance by National Scheme Operator. The National Scheme Operator publishes a list of approved EMV chip manufacturers periodically.

3.9.3 Multiple Application Chip Cards

Any Card Program is permitted to reside on a chip, and any combination of Card Programs are permitted to reside together on a single Chip Card. All payment applications residing on a single Chip Card must be offered by, and are the responsibility of the Card Issuer. Additionally, all other applications stored on a Chip Card by any Issuer, or any other party at an Issuer's request, must conform to all relevant technical specifications of the National Scheme Operator or its agent.

3.10 Contactless Cards and Payment Devices

(Category A as referenced in Chapter 1)

A Contactless Chip Card or Payment Device issuance program must be implemented using an [Approved Kernel as per CBL] product.

3.11 Contactless Cards and Mobile Payment Devices

(Category A as referenced in Chapter 1)

It is recommended that Cards be enabled with EMV Mode contactless functionality in addition to contact chip functionality.

Cardholder Name

The National Scheme Operator prohibits the encoding of the Cardholder name in the contactless Chip of a Contactless Card or Contactless Payment Device that allows such information to be transmitted through the radio frequency (RF) contactless interface.

Online CAM

The Issuer of a Contactless Card or Contactless Payment Device must perform an online CAM for each online-authorized EMV Mode Contactless Transaction by validating the Authorization Request Cryptogram (ARQC) contained in the Authorization Request or Financial Transaction Request message.

Mobile Payment Devices

There is no limitation on the type of account that has the right to co-reside on the same Mobile Payment Device user interface, so long as such accounts are not linked, but rather exist independently and are accessed by a separate and distinct Payment Application hosted on the same or different user interfaces.

يجب أن تؤكد جهة الإصدار مع مورديهم (البائعين) وقبل إنتاج بطاقة الشريحة وشراؤها وتوزيعها، أن بطاقات الشريحة ستكون مدرجة في قائمة منتجات الشرائح المعتمدة خلال الفترة المحددة للإصدار وعليهم تعديل كميات مشترياتهم وفقاً لذلك.

2.9.3 مقدمي شرائح الدوائر المتكاملة

على جهة الإصدار أن تحصل على جميع شرائح EMV لتثبيتها في البطاقة من قبل صانع الشرائح EMV التي تمت الموافقة عليها مسبقاً من قبل مشغل شبكة الدفع المحلية. وعلى مشغل شبكة الدفع المحلية أن ينشر قائمة بمصنعي شرائح EMV المعتمدين من قبله بشكل دوري.

3.9.3 بطاقات الشرائح متعددة التطبيقات

أي برنامج بطاقة يمكنه البقاء على الشريحة، ويجوز لمجموعة من برامج البطاقات بالتثبيت معاً على بطاقة شريحة واحدة. يقع على مسؤولية جهة الإصدار تقديم جميع طلبات الدفع المقيمة على بطاقة شريحة واحدة.

بالإضافة إلى ذلك، يجب أن تتوافق جميع التطبيقات المثبتة على بطاقة الشريحة من قبل جهات الإصدار، أو أي طرف آخر بناءً على طلب جهة الإصدار، مع جميع المواصفات الفنية المحددة من قبل مشغل شبكة الدفع المحلية أو وكيله.

10.3 بطاقات وأجهزة الدفع عن بعد

(الفئة أ كما هو مشار إليه في الفصل 1)

يجب تنفيذ برنامج إصدار بطاقات الشريحة (عن بعد) أو أجهزة الدفع، باستخدام منتج Kemel معتمد وفقاً لمصرف ليبيا المركزي.

11.3 بطاقات الخدمة عن بعد وأجهزة الدفع عبر الهاتف المحمول

(الفئة أ كما هو مشار إليه في الفصل 1)

يوصى بتفعيل البطاقات بوظيفة الخدمة عن بعد في وضع EMV ، بالإضافة إلى وظيفة شريحة الاتصال.

اسم حامل البطاقة

يحظر مشغل شبكة الدفع المحلية ترميز اسم حامل البطاقة في شريحة الخدمة عن بعد لبطاقات الخدمة عن بعد أو جهاز الدفع عن بعد الذي يسمح بنقل هذه المعلومات من خلال واجهة التردد اللاسلكي عن بعد.

المصادقة على البطاقة عبر الإنترنت

يجب على جهة إصدار البطاقات عن بعد أو أجهزة الدفع عن بعد إجراء مصادقة على البطاقات عبر الإنترنت لكل معاملة تتم عن بعد لوضع EMV المرخص به عبر الإنترنت من خلال التحقق من تشفير طلب الترخيص الوارد في طلب الترخيص أو رسالة طلب المعاملة المالية.

أجهزة الدفع عبر الهاتف المحمول

لا توجد قيود على نوع الحسابات المرخص لها في الوجود المشترك على نفس واجهة مستخدم جهاز الدفع عبر الهاتف المحمول، طالما أنها كانت حسابات مستقلة وليست مرتبطة، ويمكن الوصول إليها بواسطة تطبيق دفع منفصل ومميز ومثبت على نفس واجهات المستخدم أو واجهات مختلفة.

Mobile Payment Devices are permitted to support National Scheme Operator contactless payment and/or Digital Secure Remote Payment (DSRP) functionality. If an Issuer chooses to add this functionality to a Secure Element (SE)-based Mobile Payment Device, the application software, personalization data, and all other aspects of the functionality must comply with the requirements set forth in the Standards, including but not limited to other applicable technical specifications published by National Scheme Operator from time to time. The SE must meet all applicable security requirements.

3.12 Cardholder Verification Method

(Category A as referenced in Chapter 1)

All Cards must follow specific CVM requirements according to the interface being used. For contact and contactless EMV mode Transactions the CVM used for a Transaction is determined by the Terminal, based on the Terminal capabilities and the Issuer preferences expressed in the CVM List or elsewhere on the Card.

For Contactless Transactions less than or equal to the appropriate CVM Limit, no cardholder verification is required regardless of the setting of the service code for magstripe mode or the CVM List for EMV mode transactions. For certain Transaction types (for example, ATM, purchase with cash back) this limit is set to zero. Some mobile payment device implementations require CDCVM for Transactions less than or equal to the appropriate CVM Limit.

For Contactless Transactions above the CVM Limit:

- For magstripe mode Transactions, the cardholder verification method is determined by the Terminal. The Terminal is not required to refer to the service code. For a Mobile Payment Device, support for and performance of CDCVM is communicated to the Terminal as part of the Transaction data
- For EMV mode Transactions, the CVM is determined by the reader application in the Terminal based on the Terminal capabilities and CVM List or other data in the Contactless Card or Payment Device.

For DSRP transactions, CDCVM is the only cardholder verification method that is permitted. For Transactions with biometric Cards, the CVM List might not be present, therefore the CVM requirements do not apply to biometric Cards that do not support Cardholder verification.

Chip Cards must support online PIN at the CVM. 'No CVM' must be supported on the contactless interface for Contactless Transactions below the CVM Limit. Contactless Cards and non-mobile payment devices must support online PIN. Mobile Payment Devices must support online PIN.

Support for online PIN is recommended for all debit-enabled Mobile Payment Devices to permit ATM withdrawals.

Online PIN must be the only CVM supported for Contactless Transactions effected with a Card at a contactless-enabled ATM.

Offline PIN is not supported for Contactless Transactions. Issuers must not include offline plaintext PIN or offline enciphered PIN in the CVM List that is read through the contactless interface.

يجوز لأجهزة الدفع عبر الهاتف المحمول بدعم وظيفة الدفع عن بعد لمشغل شبكة الدفع المحلية، و وظيفة الدفع الرقمي الآمن عن بُعد. وإذا اختارت جهات الإصدار إضافة هذه الوظائف إلى أجهزة الدفع بواسطة الهاتف المحمول المحمي بواسطة عنصر آمن، فيجب أن يتوافق برنامج التطبيق وبيانات التخصيص وجميع الجوانب الأخرى لهذه الوظيفة مع القواعد المنصوص عليها في المعايير والمواصفات الفنية المنشورة من قبل مشغل شبكة الدفع المحلية بشكل دوري. ويجب أن يحقق عنصر الآمن جميع قواعد الأمان المعمول بها.

12.3 طريقة التحقق من حامل البطاقة

(الفئة أ كما هو مشار إليه في الفصل 1)

يجب على حامل البطاقة الالتزام بجميع القواعد CVM المحددة وفقًا للواجهة المستخدمة. بالنسبة للمعاملات في وضع EMV للتواصل والاتصال عن بعد، فإن تحديد طريقة التحقق من البطاقة (CVM) المستخدمة في المعاملة تتم بواسطة أجهزة التحقق، بناءً على إمكانيات هذه الأجهزة وتفضيلات جهة الإصدار المعبر عنها في قائمة CVM أو في أي مكان آخر على البطاقة.

بالنسبة إلى المعاملات التي تتم عن بعد، والتي تقل عن الحد CVM المناسب، أو تتساوى معه، فإنه لا يلزم التحقق من حامل البطاقة بغض النظر عن إعداد رمز الخدمة لوضع الشريط المغناطيسي أو قائمة CVM لمعاملات وضع EMV. بالنسبة لأنواع معينة من المعاملات (على سبيل المثال، أجهزة الصراف الآلي، الشراء باسترداد نقدي) يتم تعيين هذا الحد على صفر. وتتطلب بعض تطبيقات أجهزة الدفع عبر الهاتف المحمول تنفيذ CDCVM للمعاملات التي تقل عن أو تساوي حد CVM المناسب.

للمعاملات عن بعد فوق حد CVM :

- بالنسبة للمعاملات في وضع الشريط المغناطيسي ، يتم تحديد طريقة التحقق من حامل البطاقة بواسطة الجهاز المناسب. الجهاز غير مطلوب للإشارة إلى رمز الخدمة. وبالنسبة لجهاز الدفع عبر الهاتف المحمول، يتم إرسال دعم CDCVM وأدائه إلى الجهاز كجزء من بيانات المعاملة
- بالنسبة لمعاملات في وضع EMV ، يتم تحديد CVM بواسطة تطبيق القارئ في الجهاز بناءً على إمكانيات الجهاز الطرفي وقائمة CVM أو بيانات أخرى في البطاقة عن بعد أو جهاز الدفع.

بالنسبة لمعاملات الدفع الرقمي الآمن عن بعد DSRP، فإن CDCVM هي الطريقة الوحيدة المسموح بها للتحقق من حامل البطاقة. أما فيما يتعلق بالمعاملات التي تتم باستخدام بطاقات المقاييس الحيوية، فإذا لم تكن قائمة CVM موجودة عليها، فإن قواعد CVM لا تنطبق عليها والتي لا تدعم التحقق من حامل البطاقة.

يجب أن تدعم بطاقات الشريحة رقم التعريف الشخصي عبر الإنترنت في CVM. يجب دعم "No CVM" على الواجهة البطاقات عن بعد للمعاملات عن بعد أسفل حد CVM .

يجب أن تدعم البطاقات عن بعد وأجهزة الدفع غير المحمولة، وأجهزة الدفع عبر الهاتف المحمول رقم التعريف الشخصي عبر الإنترنت.1

يوصى بدعم رقم التعريف الشخصي عبر الإنترنت لجميع أجهزة الدفع عبر الهاتف المحمول والتي تدعم عملية الخصم للسماح بعمليات السحب من أجهزة الصراف الآلي.

يعد رقم التعريف الشخصي للبطاقة عبر الإنترنت هو رمز التحقق الوحيد المدعوم للمعاملات البطاقات عن بعد، والتي يتم إجراؤها باستخدام بطاقة في جهاز الصراف الآلي عن بعد.

يعد رقم التعريف الشخصي في وضع عدم الاتصال غير مدعوم للمعاملات عن بعد. تلتزم جهات الإصدار بعدم تضمين، رقم التعريف الشخصي في وضع عدم الاتصال أو رقم التعريف الشخصي المشفر في وضع عدم الاتصال، في قائمة التحقق من البطاقة (CVM) التي تتم قراءتها من خلال الواجهة التبادلية.

3.12.1 CVM Fallback (PIN Bypass)

CVM fallback is possible when the preferred CVM cannot be used and a different CVM, usually Signature, is used instead.

CVM fallback normally occurs either when the PIN Try Counter of the card is exceeded, or when the Cardholder or Merchant uses the PIN bypass function that is available on some Terminals.

CVM fallback to signature is only allowed at attended POS Terminals and not ATM.

If the CVM is online PIN, CVM fallback to signature is possible only as a result of PIN entry bypass.

Support for PIN entry bypass is not available at all Terminals, so holders of Cards for which the primary CVM at POS is online PIN should be made aware that if they are unable to input their PIN at POS, the Transaction might fail.

The issuer controls how and when CVM fallback proceeds through the personalization of data in the Card. This impacts the CVM list and Issuer Action Codes (IACs).

3.13 Consumer Device Cardholder Verification Method (CDCVM)

(Category A as referenced in Chapter 1)

Consumer authentication technologies used on consumer devices, such as personal computers, tablets, mobile phones, and watches, are designed to verify a person as an authorized device user based on one or more of the following:

- “Something I know”—Information selected by and intended to be known only to that person, such as a passcode or pattern
- “Something I am”—A physical feature that can be translated into biometric information for the purpose of uniquely identifying a person, such as a face, fingerprint, or heartbeat
- “Something I have”—Information intended to uniquely identify a particular consumer device.

Any such consumer authentication technology must be approved by National Scheme Operator as a “National Scheme Operator-qualified CVM” before it may be used as a Consumer Device Cardholder Verification Method (CDCVM) to process a Transaction.

3.14 Card Verification Value

(Category A as referenced in Chapter 1)

The CVV is a security feature which makes it more difficult for counterfeiters to alter Cards and reuse them for fraudulent purposes.

CVV 1 and CVV 2 are mandatory security features for all Cards.

1.12.3 نموذج التحقق من البطاقة الاحتياطية (تجاوز رقم التعريف الشخصي)

يمكن استخدام النظام الاحتياطي لـ CVM للتحقق من البطاقات عندما لا يمكن استخدام النظام المفضل لـ CVM. ويتم استخدام نظام التوقيع CVM كوسيلة بديلة.

عادةً ما يعمل رمز التحقق الاحتياطي CVM في حالة تجاوز عداد تجربة رقم التعريف الشخصي للبطاقات، أو في حالة استخدام حامل البطاقة أو التاجر وظيفة تجاوز رقم التعريف الشخصي المتوفرة في بعض الأجهزة.

لا يجوز اعتبار التوقيع CVM وسيلة بديلة للتحقق من البطاقات إلا في نقاط البيع الخاضعة للإشراف، وليس في أجهزة الصراف الآلي.

إذا كان رمز التحقق من البطاقات CVM هو رقم تعريف شخصي عبر الإنترنت، فلا يعتد بالرجوع إلى نموذج التوقيع إلا في حالة تعذر إدخال رقم التعريف الشخصي.

يجب إعلام حاملي البطاقات في نقاط البيع، والتي يكون رمز التحقق منها هو رقم التعريف الشخصي عبر الإنترنت أنهم إذا لم يتمكنوا من إدخال رقم التعريف الشخصي الخاص بهم في نقطة البيع، فقد تفشل المعاملة، بسبب عدم توفر دعم تجاوز إدخال رقم التعريف الشخصي في جميع الأجهزة.

جهة الإصدار هي الجهة التي تتحكم في كيفية ووقت اتخاذ الإجراءات الاحتياطية للتحقق من البطاقات من خلال تخصيص البيانات فيها. وهذا يؤثر على قائمة نظام التحقق من البطاقة CVM ورموز إجراءات جهة الإصدار (IACs).

13.3 إجراءات التحقق من حامل بطاقة جهاز المستهلك (CDCVM)

(الفئة أ كما هو مشار إليه في الفصل 1)

تم تصميم تقنيات التحقق من المستهلك المستخدمة على أجهزة المستهلك، مثل أجهزة الكمبيوتر الشخصية والأجهزة اللوحية والهواتف المحمولة والساعات، للتحقق من جهاز المستهلك، كمستخدم لجهاز مرخص له بناءً على طريقة أو أكثر من الطرق التالية:

- “شيء ما أعرفه” - معلومات يختارها ويقصد أن تكون معروفة لجهاز المستهلك فقط، مثل رمز المرور أو رسم نمط معين.
- “شيء ما أنا عليه” - ميزة مادية يمكن ترجمتها إلى معلومات بيومترية بغرض التعرف بشكل مميز على جهاز المستهلك، مثل الوجه أو بصمة الإصبع أو ضربات القلب.
- “شيء لدي” - معلومات تهدف إلى التعرف بشكل مميز على جهاز المستهلك.

يجب على جهات الإصدار الحصول على الموافقة المكتوبة المسبقة من قبل مشغل شبكة الدفع المحلية على إجراءات وتقنيات التحقق من أجهزة المستهلكين، قبل أن يتم استخدامها كطريقة للتحقق من حامل بطاقة جهاز المستهلك (CDCVM) لمعالجة المعاملة.

14.3 قيمة التحقق من البطاقة

(الفئة أ كما هو مشار إليه في الفصل 1)

تعد قيمة التحقق من البطاقات ميزة أمنية، تجعل من الصعب على المزورين تغيير البطاقات وإعادة استخدامها لأغراض احتيالية.

تعد قيمة التحقق من البطاقة 1 وقيمة التحقق من البطاقة 2 من ميزات الأمان الإلزامية لجميع البطاقات.

CVV 1 must be encoded on Track 1 and Track 2 in three contiguous positions in the Discretionary Data field of the magnetic stripe.

Chip CVV must be encoded in the Track 2 Equivalent Data field in three contiguous positions within the Discretionary Data field of the chip on all Chip Cards and must be different than the CVV 1 value encoded on the magnetic stripe.

NOTE: Due to the pseudo-random method by which the three-digit values for CVV 1, CVV 2, and Chip CVV are generated, there is approximately a one in 1,000 chance that the CVV 1 and Chip CVV values for a new or reissued Card will be identical. If the CVV 1 and Chip CVV are identical values based solely on chance, then the use of these identical values for a new or reissued Card is acceptable.

The following applies to contactless-enabled Cards (“Contactless Cards”) and Contactless Payment Devices:

All magnetic stripe profile Contactless Cards and Contactless Payment Devices must generate a dynamic CVV 3.

3.14.1 Issuer Requirements for CVV 1

(Category A as referenced in Chapter 1)

Issuers must:

- Encode the CVV 1 on Tracks 1 and 2
- Verify the encoded CVV 1 when processing a magnetic stripe-read authorization request

The Issuer verifies the CVV 1 value from the magnetic stripe-read data as transmitted in the authorization request during the online authorization process. The Issuer’s host can perform the verification.

Certification is required for Issuers to validate the CVV 1 value during the authorization process and to signal CVV 1 validation errors.

3.14.2 Issuer Requirements for CVV 2

(Category A as referenced in Chapter 1)

An Issuer must verify the CVV 2 value when provided by the Merchant and transmitted by the Acquirer in the Authorization Request message.

The Issuer must verify the CVV 2 value by providing a valid response code in the appropriate field of the Authorization Request Response or Financial Transaction Request Response.

يجب ترميز قيمة التحقق من البطاقة 1 في المسار 1 والمسار 2 في ثلاثة مواضع متجاورة في حقل البيانات التقديرية للشريط المغناطيسي.

يجب ترميز شريحة قيمة التحقق من البطاقة في حقل البيانات المكافئة للمسار 2 في ثلاثة مواضع متجاورة داخل حقل البيانات التقديرية للشريحة وعلى جميع بطاقات الشريحة، ويجب أن تكون مختلفة عن قيمة التحقق من البطاقة 1 المشفرة على الشريط المغناطيسي.

ملاحظة: نظرًا للطريقة العشوائية التي يتم من خلالها إنشاء القيم المكونة من ثلاثة أرقام لقيمة التحقق من البطاقة 1 و قيمة التحقق من البطاقة 2 و شريحة قيمة التحقق من البطاقة، هناك احتمال ونسبة 1:1000 تقريبًا أن تكون قيمة التحقق من البطاقة 1 و شريحة قيمة التحقق من البطاقة الجديدة أو المعاد إصدارها سيكون هناك تطابق بين البطاقات.. فإذا كان ذلك من قبيل الصدفة، فإن استخدام هذه القيم المتطابقة للبطاقة الجديدة أو المعاد إصدارها يكون مقبولاً.

ينطبق ما يلي على البطاقات التي تعمل بتقنية الخدمة عن بعد (“البطاقات عن بعد”) وأجهزة الدفع عن بعد:

يجب أن تنتج جميع البطاقات عن بعد وأجهزة الدفع عن بعد ذات الشريط المغناطيسي رمز قيمة التحقق من البطاقة 3 بشكل حركي ذاتي.

1.14.3 قواعد جهات الإصدار لقيمة التحقق من البطاقة 1

(الفئة أ كما هو مشار إليه في الفصل 1)

يجب على جهات الإصدار:

- أن تقوم بتشفير قيمة التحقق من البطاقة 1 في المسارين 1 و 2
- أن تتحقق من رمز قيمة التحقق من البطاقة 1 المشفر عند معالجة طلب إذن قراءة شريط مغناطيسي

على جهات الإصدار أن تتحقق من قيمة التحقق من البطاقة 1 من خلال بيانات قراءة الشريط المغناطيسي كما تم إرسالها في طلب الترخيص أثناء عملية الترخيص عبر الإنترنت. ويمكن لمضيف جهة الإصدار إجراء التحقق.

على جهات الإصدار أن تحصل على شهادة للتحقق من مدى صحة قيمة التحقق من البطاقة 1 أثناء عملية الترخيص، والإشارة إلى أخطاء التحقق من صحة قيمة التحقق من البطاقة 1.

2.14.3 قواعد جهات الإصدار لقيمة التحقق من البطاقة 2

(الفئة أ كما هو مشار إليه في الفصل 1)

على جهات الإصدار أن تقوم بالتحقق من قيمة التحقق من البطاقة 2 عندما يقدمها التاجر ويرسلها الحامل في رسالة طلب الترخيص.

على جهات الإصدار أن تقوم بالتحقق من قيمة التحقق من البطاقة 2 من خلال توفير رمز استجابة صالح في الحقل المناسب لاستجابة طلب الترخيص أو استجابة طلب المعاملة المالية.

3.14.3 CVV Calculation Methods

The Issuer may calculate the CVV 1, CVV 2, and Chip CVV by one of two methods:

- Issuer proprietary calculation—which gives the Issuer the option to derive the CVV algorithmically.
- Data Encryption Standard (DES) software—where the Issuer can perform the calculation through a DES software application within a host system or through use of a tamper-resistant security module.

Issuers that choose the DES software method must use the DES algorithm procedure to generate the CVV 1, CVV 2, and Chip CVV.

The DES algorithm procedure is described below and is also published in the following documents:

- ANSI X3.92-1981 American National Standard, Data Encryption Algorithm
- ISO/IEC 18033-3:2010, Information technology—Security techniques—Encryption algorithms—Part 3: Block ciphers (see Annex A)

The DES method algorithm generates the three-digit CVV 1 for the Discretionary Data field of Track 1 and Track 2. The Issuer also uses this method to develop the three-digit CVV 2 and Chip CVV. This algorithm procedure applies only to Issuers that implement the CVV generation process in their host systems.

CVV (but not the CVV 3) provided that separate service codes are used. The same keys should not be shared among multiple Issuers, such as when Issuers use a common Service Provider for CVV 1, CVV 2, and Chip CVV processing.

Issuers are discouraged from using a CVV 2 value of “000.”

The DES algorithm procedure is performed by following the steps below:

1. If the primary account number (PAN) is longer than 16 digits, extract the last 16 digits of the PAN.
2. Construct a string of bits by concatenating (left to right) the sequence of 4-bit values (or nibbles), each of which is the binary representation of a numeric digit in the CVV Data Elements, in the order indicated in the table below.

NOTE: The Issuer must perform independent calculations to produce each CVV value. (See appendix number 7)

3.14.3 طرق حساب قيمة التحقق من البطاقة

يجوز لجهات الإصدار حساب قيمة التحقق من البطاقة 1 و قيمة التحقق من البطاقة 2 و شريحة قيمة التحقق من البطاقة بإحدى طريقتين:

- من حساب الملكية الخاص بجهة الإصدار - والذي يمنح لجهة الإصدار خيار اشتقاق قيمة التحقق من البطاقة بطريقة حسابية.
- من برنامج معيار تشفير البيانات - حيث يمكن لجهات الإصدار إجراء الحساب من خلال برنامج تطبيق لمعيار تشفير البيانات ضمن نظام مثبت، أو من خلال استخدام وحدة أمان مقاومة للهجمات الالكترونية.

على جهات الإصدار التي تختار طريقة برنامج معيار تشفير البيانات أن تستخدم خوارزمية معيار تشفير البيانات لإنشاء قيمة التحقق من البطاقة 1 و قيمة التحقق من البطاقة و شريحة قيمة التحقق من البطاقة.

تم شرح و نشر إجراء خوارزمية معيار تشفير البيانات في المستندات التالية:

- ANSI X3.92-1981 المعيار الوطني الأمريكي، خوارزمية تشفير البيانات
- ISO / IEC 18033-3: 2010 ، تكنولوجيا المعلومات - تقنيات الأمن - خوارزميات التشفير - الجزء 3: كتلة الاصفار (انظر الملحق أ)

تقوم خوارزمية طريقة معيار تشفير البيانات بإنتاج قيمة التحقق من البطاقة 1 المكونة من ثلاثة أرقام لحقل البيانات التقديرية للمسار 1 والمسار 2. على جهات الإصدار استخدام هذه الطريقة لتطويع الشريحة وقيمة التحقق من البطاقة 2 المكونة من ثلاثة أرقام. وينطبق إجراء هذه الخوارزمية فقط، على جهات الإصدار التي تنفذ عملية إنشاء رمز التحقق من البطاقة وقيمة التحقق من البطاقة في أنظمتهم المضيفة.

قيمة التحقق من البطاقة (وليس قيمة التحقق من البطاقة 3) بشرط استخدام رموز خدمة منفصلة. على جهات الإصدار عدم استخدام نفس المفاتيح فيما بينها عندما تستخدم هذه الجهات مقدما لخدمة مشتركًا لمعالجة قيمة التحقق من البطاقة 1 و قيمة التحقق من البطاقة 2 وشريحة قيمة التحقق من البطاقة.

لا يُنصح جهات الإصدار باستخدام قيمة “000” لقيمة التحقق من البطاقة 2.

يتم تنفيذ إجراء خوارزمية معيار تشفير البيانات باتباع الخطوات التالية:

1. إذا كان رقم الحساب الأساسي أطول من 16 رقمًا، فاستخرج آخر 16 رقمًا من رقم الحساب الشخصي.
2. أنشئ سلسلة من البتات عن طريق ربط (من اليسار إلى اليمين) تسلسل القيم المكونة من 4 بتات، كل منها يمثل تمثيلًا ثنائيًا لرقم في عناصر بيانات قيمة التحقق من البطاقة، بالترتيب الموضح في الجدول أدناه.

ملاحظة: على جهات الإصدار إنشاء حسابات مستقلة لإنتاج كل قيمة التحقق من البطاقات. (انظر الملحق رقم 7)

1. Apply ISO/IEC 9797-1 (Information technology—Security techniques—Message Authentication Codes [MACs]—Part 1: Mechanisms using a block cipher) “MAC Algorithm 3”, “Padding Method 1” to the string created in Step 2, using two independent DES keys, to produce an 8-byte result.
2. From the result of Step 3, going from left to right, a nibble at a time, extract all nibbles that correspond to numeric digits (0-9); left-justify these digits in a 16-position field.
3. From the result of Step 3, going from left to right, a nibble at a time, extract all nibbles that correspond to hexadecimal characters (A-F). To compensate for hexadecimal, subtract 10 from each extracted hexadecimal digit.
4. Concatenate the resulting digits from Step 5 to the right of the digits extracted in Step 4.
5. Set the CVV to the first three left-most digits of the decimal string created in Step 6.
6. Run the program three times, once for each CVV, using the CVV data elements indicated in the table above.

3.15 Service Codes

(Category A as referenced in Chapter 1)

The service code, a three-digit number that complies with ISO/IEC 7813, is encoded on Track 1 and Track 2 of the magnetic stripe of a Card and indicates the Transaction acceptance parameters of the Card to a magnetic stripe-reading Terminal. Each digit of the service code represents a distinct element of the Issuer’s Transaction acceptance policy. However, not all combinations of valid digits form a valid service code. Issuers have the right to encode only one service code on Cards, and the same value must be encoded on both Track 1 and Track 2 in their respective, designated positions.

Service codes provide Issuers with flexibility in defining Card acceptance parameters, and provide Acquirers with the ability to interpret Issuers’ Card acceptance preferences for all POI conditions.

Service codes apply to magnetic stripe-read Transactions only. In the case of Chip Cards used in Hybrid POS Terminals, the Hybrid POS Terminal uses the data encoded in the chip to complete the Transaction. A value of 2 or 6 in position 1 of the service code indicates that a chip is present on a Card which contains the payment application that is present on the magnetic stripe.

An Issuer has the right to use service codes to support the issuance of ICC applications and PIN requirements.

For purposes of fraud prevention, Issuers are strongly recommended to set authorization parameters that decline any Transaction containing the invalid service code values of 000 or 999.

1. تطبيق ISO / IEC 9797-1 (تكنولوجيا المعلومات - تقنيات الأمان - رموز مصادقة الرسائل - الجزء 1: الآليات التي تستخدم تشفير الكتلة) “خوارزمية رموز مصادقة الرسائل 3”، “طريقة الإدخال 1” على السلسلة التي تم إنشاؤها في الخطوة 2، باستخدام مفتاحي معيار تشفير البيانات مستقلين، للحصول على نتيجة 8 بايت.
2. من نتيجة الخطوة 3، الانتقال من اليسار إلى اليمين، عاب في كل مرة، قم باستخراج جميع العباب الذي يتوافق مع الأرقام الرقمية (0-9)؛ اليسار - ضبط هذه الأرقام في حقل ذي 16 خانة.
3. من نتيجة الخطوة 3، الانتقال من اليسار إلى اليمين ، عاب في كل مرة ، قم باستخراج جميع العباب الذي يتوافق مع الأحرف السداسية العشرية (A – F). للتعويض عن النظام السداسي عشري، اطرح 10 من كل رقم سداسي عشري مستخرج.
4. اربط الأرقام الناتجة من الخطوة 5 إلى يمين بالأرقام المستخرجة في الخطوة 4.
5. عَيِّن قيمة التحقق من البطاقة على أول ثلاثة أرقام في أقصى اليسار من السلسلة العشرية التي تم إنشاؤها في الخطوة 6.
6. قم بتشغيل البرنامج ثلاث مرات، مرة واحدة لكل قيمة التحقق من البطاقة، باستخدام عناصر بيانات قيمة التحقق من البطاقة الموضحة في الجدول أعلاه.

15.3 رموز الخدمة

(الفئة أ كما هو مشار إليه في الفصل 1)

رمز الخدمة هو رقم مكون من ثلاثة أرقام يتوافق مع ISO/IEC 7813 ، ويتم ترميزه على المسار 1 والمسار 2 للشريط المغناطيسي للبطاقة ويشير إلى إشارات قبول المعاملة الخاصة بالبطاقة في محل قراءة شريط مغناطيسي. يمثل كل رمز من رموز الخدمة عنصرًا مميزًا في سياسة قبول المعاملات الخاصة بجهات الإصدار، ومع ذلك، لا تشكل جميع مجموعات الأرقام الصالحة رموز خدمة صالحة. يجوز لجهات الإصدار ترميز رمز خدمة واحد فقط على البطاقات، ويجب عليها تشفير نفس القيمة على كل من المسار 1 والمسار 2 في المواضع المخصصة لكل منهما.

توفر رموز الخدمة لجهات الإصدار مرونة في تحديد إشارات قبول البطاقة، وتزود الحاملين بالقدرة على تفسير ميزات قبول البطاقة الخاصة بجهات الإصدار لجميع شروط نقطة التفعيل.

تنطبق رموز الخدمة على المعاملات المقررة من الشريط المغناطيسي فقط. وفي حالة بطاقات الشريحة المستخدمة في محطات نقاط البيع المجهزة، تستخدم محطة نقاط البيع المجهزة البيانات المشفرة في الشريحة لإكمال المعاملة.

تشير القيمة 2 أو 6 في الموضع 1 من رمز الخدمة إلى وجود شريحة مثبتة على بطاقة تحتوي على تطبيق الدفع الموجود على الشريط المغناطيسي.

يجوز لجهات الإصدار استخدام رموز الخدمة لدعم إصدار تطبيقات بطاقات الدوائر المتكاملة ICC وإجراءات رقم التعريف الشخصي.

لمنع الاحتيال، يُنصح جهات الإصدار أن تقوم بتعيين إشارات التصريح التي ترفض أي معاملة تحتوي على قيم رمز الخدمة غير الصالحة البالغة 000 أو 999.

3.15.1 Valid Service Codes

The table below defines service code values and each position of the three-digit service code.

NOTE: To identify valid service code values, combine the valid numbers for each of the three positions in this table. The value 000 is not a valid service code and must not be encoded on the magnetic stripe of a Card.

The service code for NUMO Chip Cards is [620].

(See appendix number 8)

3.15.2 Additional Service Code Information

The following information explains the service code values in the above table.

Normal authorization is an authorized Transaction according to the established rules governing Transactions at the POI.

Positive Online Authorization Required service codes (value of 2 in position 2) indicate that an electronic authorization must be requested for all Transactions.

Normal Cardholder verification indicates that the CVM must be performed in accordance with established rules governing Cardholder verification at the POI.

ICC-related service codes (value of 2 or 6 in position 1) are permitted only on Chip Cards containing an Application type-approved by the National Scheme Operator or its agent.

ICC-related service codes (value of 2 or 6 in position 1) must not be used for stand-alone stored value (purse) applications that reside on Cards. In these instances, a value of 1 must be placed in the first position.

National Use Only service codes (value of 5 or 6 in position 1) are to be used on National Use Only Cards approved by the National Scheme Operator. This includes PIN-related service codes on National Use Only Cards (for example, 506) governed by local PIN processing rules.

Private label or proprietary service codes (value of 7 in position 1) on Cards that contain a valid National Scheme Operator BIN are permitted only on private label or proprietary Cards approved by the National Scheme Operator.

Issuers must not use PIN-related service codes for Card Programs unless the National Scheme Operator has approved the indicated use of a PIN.

3.16 Card Authentication Method

(Category A as referenced in Chapter 1)

Card authentication is the process by which either the terminal or the issuer checks that the card is genuine and the integrity of data on the card/terminal interface. CDA is the required Card authentication method.

1.15.3 رموز الخدمة الصالحة

يحدد الجدول أدناه قيم رموز الخدمة وكل موضع من رموز الخدمة المكون من ثلاثة أرقام.

ملاحظة: لتحديد قيم رموز الخدمة الصالحة، اجمع الأرقام الصالحة لكل من المواضع الثلاثة في هذا الجدول. والقيمة الصفرية 000 ليست رموز خدمة صالحة، ويجب ألا يتم ترميزها على الشريط المغناطيسي للبطاقات.

رموز الخدمة الخاص ببطاقة شريحة نمو هو [620].

(انظر الملحق رقم 8)

2.15.3 معلومات رموز الخدمة الإضافية

توضح المعلومات التالية قيم رموز الخدمة في الجدول أعلاه.

الترخيص العادي هو الترخيص بإجراء معاملة وفقًا للقواعد المعمول بها في نقطة التفعيل.

تشير رموز الخدمة المطلوبة لإجراء المصادقة الإيجابية عبر الإنترنت (القيمة 2 في الموضع 2) إلى وجوب طلب الترخيص الإلكتروني لجميع المعاملات.

يشير التحقق العادي من حامل البطاقة إلى أنه: يجب إجراء التحقق من حامل البطاقة وفقًا للقواعد المعمول بها في نقطة التفعيل.

رموز الخدمة المتعلقة ببطاقات الدوائر المتكاملة ICC (القيمة 2 أو 6 في الموضع 1) مخصص بها فقط على بطاقات الشريحة التي تحتوي على نوع التطبيق المعتمد من قبل مشغل شبكة الدفع المحلية أو وكيله.

يجب عدم استخدام رموز الخدمة المتعلقة ببطاقات الدوائر المتكاملة ICC (القيمة 2 أو 6 في الموضع 1) لتطبيقات القيمة المخزنة (المحفوظة) المستقلة والموجودة على البطاقات. وفي هذه الحالات، يجب وضع قيمة 1 في الموضع الأول.

يجب استخدام رموز (القيمة 5 أو 6 في الموضع 1) لخدمة الاستخدام الوطني فقط على بطاقات المعتمدة من قبل مشغل شبكة الدفع المحلية. ويتضمن ذلك رموز الخدمة المتعلقة برقم التعريف الشخصي على بطاقات الاستخدام الوطني فقط (على سبيل المثال ، 506) التي تحكمها قواعد معالجة رقم التعريف الشخصي المحلية.

يُسمح فقط بوضع علامة خاصة، أو رموز خدمة الملكية (القيمة 7 في الموضع 1) على البطاقات التي تحتوي على رقم تعريف مصرفي صالح من قبل مشغل شبكة الدفع المحلية فقط على العلامة الخاصة أو بطاقات الملكية المعتمدة من قبل مشغل شبكة الدفع المحلية.

يجب ألا تستخدم جهات الإصدار رموز الخدمة المتعلقة برقم التعريف الشخصي لبرامج البطاقات ما لم يوافق مشغل شبكة الدفع المحلية على الاستخدام المشار إليه كرقم للتعريف الشخصي.

16.3 طريقة مصادقة البطاقة

(الفئة أ كما هو مشار إليه في الفصل 1)

مصادقة البطاقة هي العملية التي يتحقق من خلالها الجهاز أو جهة الإصدار من أن البطاقة هي بطاقة أصلية وأن البيانات الموجودة صحيحة.

3.16.1 Additional Information

Online CAM is the process that enables issuers to authenticate their card during an online chip transaction. All cards must support online CAM by generating a dynamic cryptogram that is delivered to the issuer in the authorization.

Issuers must always validate these cryptograms before approving transactions.

In Cloud-Based Payments implementations, there are two card cryptograms to validate: a User & Mobile Device (UMD) authentication cryptogram and a Mobile Device (MD) authentication cryptogram. Issuers must ensure that they always verify MD and also that they verify UMD where appropriate.

The results of the two cryptogram validations and the Online PIN, if present, are forwarded to the issuer's authorization system (and Online PIN Management System).

3.17 Chip Card Post-Issuance Updates

(Category C as referenced in Chapter 1)

An Issuer is able to change the state of the Card or update the data on the Card by means of script commands, which may only be sent in the authorization response to Contact Chip Transactions.

The National Scheme Operator recommends that Issuers support at least the 'APPLICATION BLOCK' script. An Issuer must not send more than one template 71 script or one template 72 script with each Authorization Request Response or Financial Transaction Request Response message, although each script template may contain multiple script commands. The value field length of all scripts sent, excluding the tag and length identifiers, must not be more than [127] bytes.

The Issuer is advised to use the Issuer Application Data in the following transaction to determine whether a script has been successfully delivered to the card.

Regulatory Rules of The Libyan National Payment Scheme

Chapter 4 - Payments Acceptance

The Purpose of this chapter is to cover the standards and acquirer obligations in favor of NUMO products acceptance across different Points of Interaction in addition to all types of cash Transactions.

4.1 Requirements of the Acquirer

4.1.1 Acquirer Jurisdiction

(Category A as per references set in Chapter 1)

The jurisdiction within which NUMO Transactions are performed is Libya.

The National Scheme Operator is the sole point of contact for Acquiring and switching services between all Banks working within the Libyan borders and complying with CBL roles.

1.16.3 معلومات إضافية

طريقة مصادقة البطاقة عبر الإنترنت هي العملية التي تمكن جهات الإصدار من مصادقة بطاقتها أثناء معاملة شريحة عبر الإنترنت. ويجب أن تدعم جميع البطاقات طريقة المصادقة عبر الإنترنت من خلال إنشاء برنامج تشفير ديناميكي يتم تسليمه إلى جهات الإصدار عند إجراء الترخيص.

على جهات الإصدار أن تتحقق بشكل دوري من صحة التشفير قبل الموافقة على إجراء المعاملات. في تطبيقات المدفوعات المستندة إلى الإنترنت، هناك نوعان من برامج تشفير البطاقة للتحقق من صحتها: برنامج تشفير مصادقة المستخدم (UMD)، برنامج تشفير مصادقة الجهاز المحمول (MD) ويجب على جهات الإصدار أن تتأكد من أنها تتحقق دائماً من الجهاز المحمول (MD) وكذلك التحقق من المستخدم (UMD) إذا اقتضى ذلك.

يتم إعادة توجيه نتائج عمليتي التحقق من صحة التشفير ورقم التعريف الشخصي عبر الإنترنت، إن وجدت، إلى نظام ترخيص جهات الإصدار (ونظام إدارة رقم التعريف الشخصي عبر الإنترنت).

17.3 تحديثات ما بعد الإصدار لبطاقة الشريحة

(الفئة ج كما هو مشار إليه في الفصل 1)

يجوز لجهات الإصدار تغيير حالة البطاقة، أو تحديث البيانات الموجودة عليها عن طريق أوامر البرنامج النصي، والتي قد يتم إرسالها فقط في حالة الاستجابة للتخصيص لمعاملات شريحة الاتصال. يوصي مشغل شبكة الدفع المحلية بأن تدعم جهات الإصدار على الأقل النص البرمجي "APPLICA-TION BLOCK".

يجب ألا ترسل جهات الإصدار أكثر من نص في نموذج واحد 71 أو نص في نموذج واحد 72 مع كل استجابة لطلب الترخيص أو رسالة استجابة لطلب المعاملة المالية. على الرغم من أن كل نموذج برمجي قد يحتوي على أوامر نصية متعددة.

يجب ألا يزيد طول حقل القيمة لجميع البرامج النصية المرسل، باستثناء معرفات العلامات والطول، عن [127] بايت.

يُنصح جهات الإصدار باستخدام بيانات تطبيق جهات الإصدار في المعاملة التالية لتحديد ما إذا كان قد تم تسليم البرنامج النصي بنجاح إلى البطاقة.

القواعد التنظيمية لشبكة الدفع المحلية الليبية

الفصل 4 – قبول المدفوعات

يتضمن هذا الفصل تحديد المعايير والالتزامات التي يجب على جهة القبول الوفاء بها عند قبول بطاقات نمو عبر نقاط الخدمة المختلفة، بالإضافة إلى جميع أنواع المعاملات النقدية.

1.4 متطلبات جهة القبول

1.1.4 اختصاص جهة القبول

(الفئة أ حسب المراجع المحددة في الفصل 1)

يختص القضاء الليبي بالفصل في المنازعات المتعلقة بمعاملات بطاقة نمو.

مشغل شبكة الدفع المحلية، هو الجهة المختصة بمنح التراخيص وتبديلها بين جميع المصارف العاملة في ليبيا، والتحقق من تطبيق قواعد الأمتثال المحددة من قبل مصرف ليبيا المركزي.

4.1.2 Acquirer Onboarding

(Category A as per references set in chapter 1)

4.1.2.1 Verifying Prospective Merchants

An Acquirer is responsible for verifying that a prospective Merchant, is conducting a major business operation by performing the verifying procedures set forth in this section.

The performance of these verifying procedures does not relieve an Acquirer from the responsibility of following good commercial banking practices. The review of a credit report, an annual report, or an audited statement, for example, might suggest the need for further inquiry, such as additional financial and background checks regarding the business, its principal owners, and officers.

Required Verifying Procedures

The Acquirer of a prospective Merchant, and/ or any Payment Service Provider of the Acquirer must ensure that the following verifying procedures are performed:

- In accordance with the Acquirer's policies and procedures, collect information about the entity and each of its principal owners as necessary or appropriate for identification and due diligence purposes; verify that the information collected is true and accurate.
- Establishing a fraud loss control measures appropriate for the business to be conducted, including but not limited to Transaction authorization and deposit activity monitoring parameters, as described in Chapter 6.
- Confirm that the entity is located and conducting legal business in Libya
- Assign a Merchant Category Code as per references set in chapter 1 Merchant category code (MCC) that most accurately describes the nature of the business.

4.1.6.1 Retention of Investigative Records

The Acquirer must retain all records concerning the inspection of a Merchant, for a minimum of one year after the date that the Merchant Agreement and Agent Agreement as applicable, is terminated or expires. Such records shall include any of the following, when applicable:

- Signed Merchant Agreement
- With respect to the verifying of a Merchant or Agent, a statement from the Merchant about previous Merchant Agreements, including the names of the entities where the Merchant has or had the agreements and the reasons for terminating the agreements, if applicable
- Corporate or personal banking statements
- Report from a credit bureau, or QSA (Qualified Security Assessor), if the credit bureau report is incomplete or unavailable, the written results of additional financial and background checks of the business.
- Liability on the Acquirer to conduct the Merchant Site inspection, to include photographs of premises, inventory verification, and the name and the details of the inspection, and preferred to be conducted on annual regular basis.
- Merchant certificate of incorporation, licenses, Commercial Registrations or permits
- Verification of references, including personal, business, or financial
- Verification of the authenticity of the supplier relationship for the goods or services (invoice records) that a Merchant is offering the Cardholder for sale
- All Acquirer correspondence with the Merchant.

2.1.4 إعداد جهة القبول

(الفئة أ حسب المراجع المحددة في الفصل 1)

1.2.1.4 التحقق من التجار الاحتماليين

الجهة القابلة هي المسؤولة عن التحقق من أن التاجر المحتمل يقوم بإجراء الأعمال التجارية من خلال تنفيذ إجراءات التحقق المحددة في هذا القسم.

إن قيام جهة القبول بتنفيذ إجراءات التحقق المطلوبة منها، لا يعفيها من مسؤولية اتباع الممارسات المصرفية التجارية الحرفية. فقد تشير مراجعة تقرير الائتمان أو التقرير السنوي أو البيان المدقق، على سبيل المثال، إلى القيام بمزيداً من الاستفسار، مثل الفحوصات المالية الإضافية، والخلفية المتعلقة بالعمل التجاري ومالكها الرئيسيين والمسؤولين.

إجراءات التحقق المطلوبة

يجب على جهة القبول التحقق من التاجر المحتمل و/أو مقدم خدمة الدفع، وفق الإجراءات التالية:

- تلتزم الجهة القابلة، بالقيام بجمع معلومات حول الجهة، ومالكها الرئيسيين حسب الضرورة لأغراض التحديد والعناية الواجبة؛ والتحقق من أن المعلومات التي تم جمعها صحيحة ودقيقة.
- وضع إجراءات مراقبة عمليات الاحتيال المتوقعة للأعمال التي سيتم إجراؤها، بما في ذلك على سبيل المثال لا الحصر، اعتماد المعاملات، ومعايير مراقبة نشاط الإيداع، كما هو موضح في الفصل 6.
- التأكد من أن للجهة موطن في ليبيا وتمارس أعمالها فيها.
- تعيين رمز فئة التاجر وفقاً للمراجع المحددة في الفصل 1 من رمز فئة التاجر (MCC) الذي يصف طبيعة العمل بدقة أكبر.

1.6.1.4 الاحتفاظ بسجلات التحقيق

يجب على جهة القبول أن تحتفظ بجميع السجلات المتعلقة بالتحقق من التاجر، لمدة لا تقل عن عام واحد بعد تاريخ إنتهاء عقد التاجر أو وكيله، أو انتهاء صلاحيتها حسب الاقتضاء. ويجب أن تتضمن هذه السجلات البيانات التالية:

- توقيع التاجر.
- فيما يتعلق بالتحقق من التاجر أو الوكيل، بيان من التاجر بشأن اتفاقيات التاجر السابقة، بما في ذلك أسماء الجهات التي يمتلك التاجر فيها حصة، أو لديه عقود معها، وكذلك أسباب إنهاء التعاقد، إن وجدت.
- البيانات المصرفية أو الشخصية للتاجر.
- تقرير من مكتب الائتمان، أو مقيم الأمان المفوض (QSA)، وإذا كان تقرير مكتب الائتمان غير مكتمل أو غير متوفر، فالنتائج المكتوبة للفحوصات المالية والخلفية الإضافية للشركة.
- مسؤولية الجهة القابلة عن إجراء فحص موقع التاجر، بما في ذلك صور المباني، والتحقق من المخزون، واسم وتفاصيل التفتيش، وبفضل إجراؤه على أساس سنوي منتظم.
- شهادة التاجر بالتأسيس أو التراخيص أو التسجيلات التجارية أو التصاريح.
- التحقق من المراجع، بما في ذلك الشخصية أو التجارية أو المالية.
- التحقق من صحة علاقة المورد بالسلع أو الخدمات (سجلات الفواتير) التي يعرضها التاجر على حامل البطاقة للبيع.
- جميع مراسلات جهة القبول مع التاجر.

- All correspondence relating to Issuer, Cardholder, or law enforcement inquiries concerning the Merchant, , or any associated Payment Service Provider
- Signed Payment Service Provider contract, including the name of agents involved in the verification process
- Acquirer verification records concerning the Payment Service Provider and its agents

It is recommended that the Acquirer retain all records, in the event that the National Scheme Operator conducts an audit to verify compliance with the verifying procedures described in this section.

4.1.6.2 Assessments for Non-Compliance with Verifying Procedures

The National Scheme Operator as per delegation granted from CBL for setting up the scheme operational rules has the right to audit an Acquirer for compliance with the verifying procedures set forth in this section, and each Acquirer must comply with and assist any such audit. The National Scheme Operator in his delegated authority will review the applicable records retained by the Acquirer to determine whether an Acquirer has complied with these verifying procedures.

If the National Scheme Operator determines that an Acquirer has not complied with these verifying procedures, and if the Acquirer does not correct all deficiencies that gave rise to the violation to its satisfaction within 30 days of knowledge or notice of such deficiencies, the National Scheme Operator may assess the Acquirer up to LYD XXX for each 30-day period following the aforementioned period, with a maximum aggregate assessment of LYD XXXX during any consecutive 12-month period. Any such assessment(s) will be in addition to any other financial responsibility that the Acquirer may carry-out, as set forth in the Standards. Violators will also be subject to chargebacks of fraudulent Transactions.

4.1.6.3 Ongoing Monitoring

An Acquirer must monitor and confirm regularly that the Transaction activity of each of its Merchants (sales, credits, and chargebacks) is conducted in a legal and ethical manner and in full compliance with the Standards, and ensure that a Payment Service Provider conducts such monitoring with respect to each of its Agents, in an effort to deter fraud. Monitoring must focus on changes in activity over time, activity inconsistent with the Merchant's or Agent's business, or exceptional activity relating to the number of Transactions and Transaction amounts outside the normal fluctuation related to seasonal sales.

With respect to an e-commerce Merchant, the Acquirer must regularly, as reasonably appropriate in light of all circumstances, review and monitor the Merchant's website(s) and business activities to confirm and to reconfirm regularly that any activity related to or using the Logo is conducted in a legal and ethical manner and in full compliance with the Standards. The Acquirer must ensure that a Payment Service Provider conducts such monitoring with respect to each of its Agent's website(s).

As a best practice, it is recommended that Acquirers use a Merchant monitoring solution to review their e-commerce Merchants' and Agents' activity to avoid processing illegal or brand-damaging Transactions.

- جميع المراسلات المتعلقة باستفسارات جهة الإصدار، أو حامل البطاقة أو جهات إنفاذ القانون المتعلقة بالتاجر أو أي مقدم خدمة الدفع المرتبط به.
- عقد مقدم خدمة الدفع الموقع، بما في ذلك اسم الوكلاء المشاركين في عملية التحقق.
- سجلات التحقق من الجهة القابلة المتعلقة بمقدم خدمة الدفع ووكلائه.

يوصى بأن تحتفظ جهة القبول بجميع السجلات، لغرض قيام مشغل شبكة الدفع المحلية بإجراء تدقيق للتحقق من الامتثال لإجراءات التحقق الموضحة في هذا القسم.

2.6.1.4 تقييمات عدم الامتثال لإجراءات التحقق

يجوز لمشغل شبكة الدفع المحلية وفقاً للتفويض الممنوح من مصرف ليبيا المركزي لإعداد القواعد التشغيلية للنظام، التحقق من أن الجهة القابلة تمثل لإجراءات التحقق المحددة في هذا القسم، ويجب على كل قابل الامتثال والمساعدة في القيام بعملية التحقق. ويقوم مشغل شبكة الدفع المحلية من خلال سلطة التفويض بمراجعة سجلات الجهة القابلة لمطابقتها، وتحديد مدى امتثال القابل لإجراءات التحقق.

إذا قرر مشغل شبكة الدفع المحلية أن القابل لم يمثل لإجراءات التحقق، وأنه لم يصح جميع أوجه القصور التي أدت إلى هذه المخالفات خلال 30 يومًا من العلم أو الإشعار بهذه العيوب، فإنه يجوز لمشغل شبكة الدفع المحلية تقييم القابل ما يصل إلى XXX دينار ليبي لكل فترة 30 يومًا بعد الفترة المذكورة أعلاه، مع أقصى تقييم إجمالي لـ XXXX دينار ليبي خلال أي فترة 12 شهرًا متتالية. أي تقييم (تقييمات) من هذا القبيل سيكون بالإضافة إلى أي مسؤولية مالية أخرى قد يقوم بها القابل، على النحو المنصوص عليه في المعايير. سيخضع المخالفون أيضًا لرد المبالغ المدفوعة من المعاملات الاحتيالية.

3.6.1.4 المراقبة المستمرة

تلتزم جهة القبول بأن تقوم بمراقبة نشاط المعاملات لكل من التجار التابعين لها (المبيعات والائتمانات وعمليات رد المبالغ المدفوعة) وتؤكد أنها تتم بطريقة قانونية وأخلاقية وفي إطار الامتثال الكامل للمعايير، والتأكد من قيام مقدم خدمة الدفع بإجراء هذه المراقبة فيما يتعلق بكل من ووكلائه، في محاولة لردع الاحتيال. ويجب أن تركز المراقبة على التغييرات في النشاط بشكل دوري، أو النشاط غير المتوافق مع أعمال التاجر أو الوكيل، أو النشاط الاستثنائي المتعلق بعدد المعاملات ومبالغ المعاملات خارج التقلبات العادية المتعلقة بالمبيعات الموسمية.

فيما يتعلق بالتجارة الإلكترونية، يجب على القابل أن يقوم بانتظام، وفي حدود جهده المعقول، بمراجعة ومراقبة موقع (مواقع) التاجر وأنشطته التجارية للتحقق وإعادة التحقق بانتظام على أن النشاط يتعلق أو يستخدم الشعار يتم بطريقة قانونية وأخلاقية وبالامتثال الكامل للمعايير. ويجب على القابل التحقق من أن مقدم خدمة الدفع يجري مثل هذه المراقبة فيما يتعلق بكل موقع (مواقع) وكيله.

ومن الناحية العملية، يوصى بأن يستخدم القابلون، طريقة مراقبة التاجر لمراجعة نشاط التجار والوكلاء في التجارة الإلكترونية لتجنب معالجة المعاملات غير القانونية أو الضارة بالعلامة التجارية.

4.1.6.4 Merchant Education

Once an acquiring relationship is established, an Acquirer must institute a fraud prevention program, including an education process consisting of periodic visits to Merchants, distribution of related educational literature, and participation in Merchant seminars.

Instructions to Merchants must include Card acceptance procedures, authorization procedures, proper completion of Transaction receipts (including primary account number [PAN] truncation), timely presentment of the Transaction to the Acquirer, and proper handling of Card capture requests. Acquirers must thoroughly review with Merchants the Standards prohibiting the presentment of fraudulent Transactions.

In addition, Acquirers must review the data security procedures to ensure that only appropriate Card data is stored, magnetic stripe data is never stored, and any storage of data is done in accordance with the Standards for encryption, Transaction processing, and other prescribed practices.

An Acquirer must also ensure that a Payment Service Provider conducts appropriate education activities for each of its Agents.

4.1.6.5 High-Risk Merchants and Agents

Refer to Chapter 6 for requirements relating to high-risk Merchants.

4.1.3 The Merchant Agreements; Aggregated Transactions

(Category A as per references set in Chapter 1)

Each Acquirer must directly enter into a written Merchant Agreement with each retailer or other person, firm, or corporation selling goods or services (herein, a “seller”) and must directly enter into a written Agreement with each Merchant from which it acquires Transactions, whether such Transactions are submitted to the Acquirer directly by the seller or through a Service Provider acting for or on behalf of such Acquirer.

A Merchant Agreement is not required in connection with Transactions acquired by an Acquirer from its registered Payment Service Provider, when submitted pursuant to an Agent Agreement between the Payment Service Provider and a seller.

The Acquirer must acquire all valid Transactions submitted to it from a Merchant in accordance with the Merchant Agreement. An Acquirer must not submit for processing any Transaction resulting from the acceptance of a Card by an entity or person except pursuant to a Merchant Agreement then in effect between the Acquirer and the entity or person.

Each Merchant Agreement must reflect the Acquirer’s primary responsibility for the Merchant relationship and the establishment of all management and operating policies relating to its acquiring Programs, and must otherwise comply with the Standards. A Merchant Agreement must not include any provision that limits, or attempts to limit, the Acquirer’s responsibility for such Programs.

An Acquirer in violation of this Rule may be assessed up to LYD XXXX per day with respect to each entity or person on whose behalf the Acquirer submits transactions into interchange with no Merchant Agreement being in effect between the Acquirer and the entity or person, retroactive to the first day of such noncompliant practice, which is called Merchant aggregation.

4.6.1.4 تعليم التاجر

بمجرد إنشاء علاقة قبول، يجب على القابل إنشاء برنامج لمنع الاحتيال، بما في ذلك عملية تعليمية تتكون من زيارات دورية للتجار وتوزيع المؤلفات التعليمية ذات الصلة والمشاركة في ندوات التاجر.

ويجب أن تتضمن التعليمات إلى التجار إجراءات قبول البطاقة، وإجراءات التفويض، والإكمال الصحيح لإيصالات المعاملات (بما في ذلك اقتطاع رقم الحساب الأساسي [PAN])، وتقديم المعاملة في الوقت المناسب إلى القابل، والتعامل الصحيح مع طلبات الحصول على البطاقة. ويجب على القابلين إجراء مراجعة شاملة مع التجار للمعايير التي تحظر تقديم المعاملات الاحتيالية.

بالإضافة إلى ذلك، يجب على القابلين مراجعة إجراءات حماية البيانات لضمان تخزين بيانات البطاقة المناسبة فقط، وعدم تخزين بيانات الشريط المغناطيسي مطلقًا، وأي تخزين للبيانات يتم وفقًا لمعايير التشفير، ومعالجة المعاملات والممارسات الأخرى المحددة.

ويجب على القابل أيضًا التحقق من أن مقدم خدمة الدفع يقوم بإجراء أنشطة تعليمية مناسبة لكل من وكلائه.

5.6.1.4 التجار والوكلاء ذوو المخاطر العالية

راجع الفصل 6 للتعرف على المتطلبات المتعلقة بالتجار ذوو المخاطر العالية.

3.1.4 اتفاقيات التاجر؛ المعاملات المجمعة

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب أن يكون التعاقد بين جهة القبول والتاجر مباشرًا، ومكتوبًا مع كل بائع تجزئة أو أي شخص آخر أو شركة أو مؤسسة تبيع سلعًا أو خدمات (هنا، “البائع”)، ومع كل تاجر تحصل منه على المعاملات، سواء تم إرسال هذه المعاملات إلى القابل مباشرة من قبل البائع أو من خلال مقدم خدمة يعمل لصالح أو نيابة عن هذا القابل.

التعاقد مع التاجر لا يكون مطلوبًا في الحالة التي تحصل فيها جهة القبول على المعاملات من مقدم خدمة الدفع المسجل، عند تقديمها وفقًا لعقد الوكالة بين مزود خدمة الدفع والبائع.

يجب على جهة القبول أن تحصل على جميع المعاملات الصالحة المقدمة إليه من التاجر وفقًا للتعاقد معه. ويجب ألا تقدم لمعالجة أي معاملة ناتجة عن قبول جهة أو شخص للبطاقة إلا بموجب العقد الساري المفعول بينها وبين الجهة أو الشخص.

يجب أن يحدد كل عقد المسؤولية الأساسية لجهة القبول عن علاقة التاجر ووضع جميع سياسات الإدارة والتشغيل المتعلقة ببرامج القبول الخاصة بها، ويجب أن تمتثل بخلاف ذلك للمعايير. ويجب ألا يتضمن العقد اتفاقات الحد من مسؤولية القابل على هذه البرامج أو يحاول تقييدها.

يجوز إجراء عملية تقييم للقابل الذي يخل بتطبيق هذه القاعدة بما يصل إلى XXXX دينار لليوم الواحد، عندما يقوم القابل بتقديم المعاملات نيابة عن الجهة أو الشخص دون وجود اتفاق بينهما على تقديم هذه المعاملات، ويكون ذلك بأثر رجعي من اليوم الأول من هذه الممارسة غير الممثلة.

4.1.6.6 Required Merchant Agreement Terms

(Category A as per references set in Chapter 1)

Each Merchant Agreement must contain the substance of each of the Standards set forth in the “Merchant Requirements” section of this chapter, and any other Standards applicable to the nature and manner of the Merchant’s business. The failure to include the substance of any one or more of such Standards in the Merchant Agreement or the grant of a variance by the National Scheme Operator with respect to any one or more such Standards does not relieve an Acquirer from responsibility for chargebacks or compliance.

Each Merchant Agreement shall contain only such terms agreed to by the Acquirer and the Merchant, provided that no such term conflicts with any Standard. The Merchant Agreement must also provide that the Merchant’s use or display of any Mark will terminate effective with the termination of the Merchant Agreement or upon notification by the National Scheme Operator to discontinue such use or display.

4.1.6.7 Maintaining Information

(Category C as per references set in chapter 1)

The Acquirer must maintain, on an ongoing basis:

1. For each Merchant, the Merchant’s name and address and a signed, unexpired Merchant Agreement; and
2. For each ATM Acquirer, a signed, unexpired ATM Acquirer Agreement and all of the following information:
 - a. The complete name and address of the ATM Operator (or principals of the business if the ATM Operator is a legal entity).
 - b. The complete address of the ATM location, if different from that of the ATM Acquirer.
 - c. The legal name, and if applicable the “Doing Business As” (DBA) name, of the ATM location.
 - d. The complete name and address of any Payment Service Provider performing services for, or otherwise associated with, the ATM Acquirer.
 - e. The complete name and address of any entity, other than the ATM Acquirer, that receives revenue as a result of the use, lease, placement, and/or maintenance of the ATM.
3. The supplier, manufacturer, and model of each of its ATMs and Bank Branch Terminals.

4.1.4 Merchant Compliance with the Standards

(Category A as per references set in chapter 1)

The Acquirer is responsible for ensuring that each of its Merchants and Agents complies with the Standards, and the Acquirer is itself responsible to the Payment Service Provider and to other Customers for any Merchant’s failure to do so.

To the extent a Merchant utilizes the service of a person or entity for a purpose arising from or related to Activity, the Acquirer is responsible for ensuring that each such person or entity complies with the Standards, and the Acquirer itself is responsible to the Payment Service Operator and to other Customers for any such person’s or entity’s failure to do so. The Acquirer must not support any Merchant action having a purpose or effect of evading detection by the National Scheme Operator’s fraud monitoring and other compliance thresholds set forth in the Standards, including but not limited to “load balancing” (that is, the distribution of Transactions between or among Merchant ID numbers in order to avoid minimum thresholds).

6.6.1.4 الشروط الواجب توافرها في العقد مع التاجر

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب أن يحتوي كل عقد مع التاجر على تطبيق جميع المعايير المنصوص عليها في قسم “متطلبات التاجر” من هذا الفصل، إضافة إلى أي معايير أخرى تنطبق على طبيعة وطريقة عمل التاجر. وعدم تضمين العقد لأي من هذه المعايير، أو منح تباين من قبل مشغل شبكة الدفع المحلية في درجة تطبيق هذه المعايير لا يعفي الجهة القابلة من مسؤولية رد المبالغ المدفوعة، أو الالتزام بقواعد الامتثال.

يجب ألا تخل الشروط التعاقدية بين الجهة القابلة والتاجر بتطبيق المعايير المنصوص عليها. يجب أن ينص العقد على أن استخدام التاجر أو عرضه لأي علامة سينتهي سريانه مع إنتهاء مدة العقد، أو بناءً على إشعار من مشغل شبكة الدفع المحلية لإيقاف هذا الاستخدام أو العرض.

7.6.1.4 الاحتفاظ بالمعلومات

(الفئة ج حسب المراجع المحددة في الفصل 1)

يجب على جهة القبول أن تقوم، وبشكل مستمر، بالاحتفاظ بالبيانات التالية:

1. لكل تاجر، اسم التاجر، عنوانه وعقد موقع ساري المفعول.
2. لكل قابل على أجهزة الصراف الآلي، عقد موقع ساري المفعول مع قابل أجهزة الصراف الآلي يحتوي على المعلومات التالية:
 - أ. الاسم و العنوان الكاملين لمشغل أجهزة الصراف الآلي وعنوانه (أو مديري النشاط التجاري إذا كان مشغل الصراف الآلي جهة قانونية).
 - ب. بالعنوان الكامل لموقع جهاز الصراف الآلي، إذا كان مختلفًا عن عنوان جهة القبول على أجهزة الصراف الآلي.
 - ت. تالاسم القانوني، واسم “ممارسة الأعمال باسم” ، إن أمكن، لموقع أجهزة الصراف الآلي.
 - ث. تالاسم والعنوان الكاملين لأي مقدم خدمات دفع، إذا كان يؤدي هذه الخدمات لحساب جهة القبول على أجهزة الصراف الآلي أو المرتبطة بها بأي شكل آخر.
 - ج. الاسم والعنوان الكاملين لأي جهة، بخلاف الجهة القابلة على أجهزة الصراف الآلي، التي تتلقى إيرادات نتيجة استخدام جهاز الصراف الآلي أو إيجاره أو وضعه و/أو صيانته.
3. المورد والشركة المصنعة ونموذج كل من أجهزة الصراف الآلي ومحطات الفروع المصرفية.

4.1.4 امتثال التاجر للمعايير

(الفئة أ حسب المراجع المحددة في الفصل 1)

جهة القبول هي المسؤولة عن ضمان امتثال كل من التجار والوكلاء للمعايير، وهي نفسها المسؤولة أمام مقدمي خدمة الدفع والعملاء الآخرين عن تعثر التاجر في القيام بذلك. تكون جهة القبول مسؤولة عن ضمان تطبيق، الغير الذي قد يستخدمه التاجر عند ممارسة نشاطه، لمعايير الامتثال المحددة، إضافة إلى مسؤولية جهة القبول عن مقدمي خدمة الدفع والعملاء الآخرين بسبب فشل أي شخص أو جهة في القيام بذلك. يجب على جهة القبول أن لا تقوم بإتخاذ أي إجراء يكون من شأنه مساعدة التاجر في التهرب من إجراء عمليات المراقبة للكشف عن عمليات الاحتيال، وتطبيق معايير الامتثال من قبل مشغل شبكة الدفع المحلية، على سبيل المثال: القيام بعملية “موازنة العبء” (أي توزيع المعاملات بين أوفيميا بين أرقام معرف التاجر من أجل تجنب الحد الأدنى من الحدود).

The Acquirer must take such actions, including ongoing monitoring, necessary or appropriate to ensure a Merchant's ongoing compliance with the Standards. Failure by a Merchant, or Acquirer to comply with any Standard shall result in chargebacks, an assessment to the Acquirer, and/or other disciplinary action.

4.1.6.8 Non-Compliance Assessments

If the National Scheme Operator becomes aware of a Merchant's noncompliance with any Standard, it shall notify the Acquirer and has the right to assess and/or otherwise discipline the Acquirer for such noncompliance, and the Acquirer must promptly cause the Merchant to discontinue the noncompliant practice. A notification by the National Scheme Operator with respect to any one location of a Merchant requires the Acquirer to ensure that the Merchant is in compliance with the Standards at all locations of the Merchant that are subject to the Merchant Agreements.

An Acquirer is permitted to request that the designated officer of the National Scheme Operator review an assessment for a Merchant's noncompliance with a Standard.

4.1.5 Display of NUMO Logo

(Category B as per references set in chapter 1)

As referenced in book 2 chapter 2 of the brand usage the following needs to be considered by acquirers and their representatives during the deployment of POS terminals.

An Acquirer must ensure that its Merchants and Terminals prominently display the Mark at the Point-of-Interaction (POI), wherever payment options are presented.

A Mark is permitted to be displayed in advertising or other materials or images at the physical or electronic POI to indicate brand acceptance with accordance to what is set in book 2 chapter 2

No other marks shall be used for these purposes.

4.1.6.9 Location of Display

The Mark must be clearly visible to the public at the POI.

(See appendix number 9)

4.1.6.10 Display with Other Marks

Other acceptance marks, symbols, logos, or combinations thereof are permitted to appear in the same material or image with the Mark, provided visual parity is maintained and no other acceptance mark, symbol, or logo displayed is more prominent or likely to cause confusion concerning the acceptance of Cards.

The Mark must be displayed as a free-standing mark, meaning that the Mark must not be displayed so as to suggest that it is either a secondary means of payment or exclusively linked to another acceptance brand.

4.1.6 Transaction Message Data

(Category A as per references set in chapter 1)

An Acquirer must ensure that each of its Merchants and Terminals complies with the following Transaction message data requirements.

4.1.6.11 Card Acceptor Business Code (MCC) Information

The Acquirer must ensure that each Merchant is identified in Transaction messages with the Card acceptor business code (MCC) that reflects the primary business of the Merchant.

يجب على جهة القبول اتخاذ مثل هذه الإجراءات، بما في ذلك المراقبة المستمرة، الضرورية أو المناسبة لضمان استمرار امتثال التاجر للمعايير. ويترتب على فشل التاجر أو جهة القبول في الامتثال لأي معيار إلى رد المبالغ المدفوعة وتقييماً للقابل و/أو إجراء تأديبي آخر.

8.6.1.4 تقييمات عدم الامتثال

بمجرد علم مشغل شبكة الدفع المحلية بعدم امتثال التاجر لأي معيار، يجب عليه إخطار القابل وله الحق في تقييم و/أو معاقبة القابل على إخلاله بعدم بتطبيق معايير الامتثال، ويجب عليه إيقاف التاجر عن ممارسة نشاطه فوراً. ويتطلب الإخطار المقدم من مشغل شبكة الدفع المحلية بالنسبة لأحد مواقع التاجر، أن يضمن القابل أن التاجر يمثل للمعايير في جميع مواقع الأخرى الخاضعة للعقد التجاري.

يجوز للجهة القابلة أن تطلب من المسؤول المعين لمشغل شبكة الدفع المحلية مراجعة تقييم التاجر لتطبيق معايير الامتثال.

5.4.1 عرض شعار علامة نمو

(الفئة ب حسب المراجع المحددة في الفصل 1)

كما هو مشار إليه في الكتاب 2، الفصل 2 من استخدام العلامة التجارية، يجب أن يأخذ القابلون وممثلوهم في الاعتبار ما يلي أثناء نشر محطات نقاط البيع.

يجب أن تتأكد جهة القبول من أن التاجر، ومحطاتهم يعرضون العلامة بشكل بارز عند نقطة التفاعل، (تقديم الخدمة) أينما يتم تقديم خيارات الدفع.

يجوز عرض العلامة في الإعلانات أو المواد أو الصور الأخرى في نقطة التفاعل المادية أو الإلكترونية للإشارة إلى قبول العلامة التجارية طبقاً لما هو محدد في الكتاب 2 الفصل 2 لا يجوز استخدام أي علامات أخرى لهذه الأغراض.

9.6.1.4 موقع العرض

يجب أن تكون العلامة مرئية بشكل واضح للجمهور في نقطة التفاعل، أو تقديم الخدمة.

(انظر الملحق رقم 9)

10.6.1.4 العرض مع علامات أخرى

يُسمح بظهور علامات قبول أو رموز أو شعارات أو مجموعات منها على نفس المادة أو الصورة مع العلامة، بشرط الحفاظ على التكافؤ البصري، وعدم ظهور علامة قبول أو رمز أو شعار آخر أو من المحتمل أن يسبب التباساً على المتعامل فيما يتعلق قبول البطاقات.

يجب عرض العلامة، كعلامة قائمة بذاتها، مما يعني أنه يجب عدم عرض العلامة للإشارة إلى أنها إما وسيلة دفع ثانوية، أو مرتبطة حصرياً بعلامة تجارية أخرى.

6.1.4 بيانات رسالة المعاملة

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب على جهة القبول التحقق من امتثال كل من التاجر، والمحطات التابعة له، لمتطلبات بيانات رسالة المعاملة، على النحو التالي:

11.6.1.4 معلومات رمز العمل الخاص بمتقبل البطاقة (MCC)

يجب أن تتحقق جهة القبول من تحديد كل تاجر في رسائل المعاملات لرمز عمل متقبل البطاقة (MCC) الذي يعكس الأعمال الأساسية للتاجر.

Any Transaction that includes, in whole or in part, the sale of products or services properly identified with one of the following MCCs must be identified with such MCC:

- Money Transfer (MCC 4829)

The National Scheme Operator shall have the ultimate authority to specify the appropriate MCC if any dispute shall arise.

4.1.6.12 Agent Name Information

The Acquirer must ensure that a Transaction conducted by an Agent includes the name of the Payment Service Provider followed by the name of the Agent.

4.1.6.13 ATM Information

The Acquirer of an ATM Transaction must transmit in Transaction messages the ATM Acquirer name and ATM location address, substantially the same as it appears on any Transaction receipt provided, and the unique ATM Terminal identification number. An Acquirer and any Service Provider performing ATM Transaction processing services must also identify itself using a unique number, assigned by the National Scheme Operator.

4.1.6.14 Transactions at Terminals with No Fixed Location

A Transaction arising from a Terminal with no fixed location (for example, aboard a train or ship) is deemed to take place at the address where the Merchant operating a POS Terminal or the Acquirer of an ATM or Bank Branch Terminal is headquartered or where the Transaction is processed.

4.1.7 Presentment of Transaction Records

(Category A as per references set in chapter 1)

Upon receiving a clearing record, the Acquirer must present the Transaction within the applicable presentment timeframe in order to avoid a late presentment chargeback.

For Card-present and Card-not-present key-entered Transactions, the presentment timeframe is 7 calendar days following the authorization date.

In case of a preauthorization, the presentment timeframe is 7 calendar days following the authorization date.

For all other Transaction types and authorizations, the presentment timeframe is 7 calendar days following the authorization date.

4.1.8 Retention of Transaction Records

(Category A as per references set in chapter 1)

The Acquirer must retain a record of each Transaction it receives or sends for a minimum of 6 months. During this period, the Acquirer must provide a copy of the Transaction receipt to the Issuer upon request.

أي معاملة تتضمن، كليًا أو جزئيًا، بيع المنتجات أو الخدمات المحددة بشكل صحيح مع أحد MCCs التالية يجب تحديدها مع MCCs هذا:

- تحويل الأموال (MCC 4829)

تكون لمشغل شبكة الدفع المحلية السلطة النهائية في تحديد MCC المناسب في حالة نشوء المنازعات.

12.6.1.4 معلومات اسم الوكيل

يجب على جهة القبول التحقق من أن المعاملة التي يجريها الوكيل تتضمن اسم مقدم خدمة الدفع، متبوعًا باسم الوكيل.

13.6.1.4 معلومات أجهزة الصراف الآلي

يجب على جهة القبول التحقق من أن جهاز الصراف الآلي يقوم بنقل رسائل المعاملات باسم القابل على جهاز الصراف الآلي، وعنوان موقع جهاز الصراف الآلي، إلى حد كبير كما يظهر في أي إيصال معاملة المقدم، ورقم تعريف جهاز الصراف الآلي المميز. ويجب على جهة القبول وأي مقدم خدمة؛ يقوم بخدمات معالجة معاملات جهاز الصراف الآلي أن يعرّف بنفسه أيضًا باستخدام رقم مميز يتم تعيينه بواسطة مشغل شبكة الدفع المحلية.

14.6.1.4 المعاملات في المحطات التي ليس لها موقع ثابت

تعتبر المعاملة التي تنشأ من محطة بدون موقع ثابت (على سبيل المثال، على متن قطار أو سفينة) قد تمت في العنوان الذي يقوم فيه التاجر بتشغيل محطة نقاط البيع، أو القابل على جهاز الصراف الآلي، أو محطة فرع المصرف أو حيث يقع المقر الرئيسي تتم معالجة المعاملة.

7.1.4. تقديم سجلات المعاملات

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب على جهة القبول عند استلام سجل المقاصة، أن تقوم بتقديم المعاملة ضمن الإطار الزمني للتقديم المعمول به من أجل تجنب رد رسوم التقديم المتأخر.

بالنسبة للمعاملات التي يتم إدخالها بواسطة مفتاح باستخدام البطاقة، و كانت البطاقة غير الموجودة، يكون الإطار الزمني للتقديم هو 7 أيام تقويمية بعد تاريخ التفويض.

وفي حالة التفويض المسبق، يكون الإطار الزمني للتقديم هو 7 أيام تقويمية بعد تاريخ التفويض. أما بالنسبة لجميع أنواع المعاملات والتفويضات الأخرى، يكون الإطار الزمني للتقديم هو 7 أيام تقويمية بعد تاريخ التفويض.

8.1.4. الاحتفاظ بسجلات المعاملات

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب أن تحتفظ جهة القبول بسجل خاص بكل معاملة يتلقاها أو يرسلها لمدة لا تقل عن 6 أشهر. خلال هذه الفترة، يجب عليها تقديم نسخة من إيصال المعاملة إلى جهة الإصدار عند الطلب.

4.1.9 PCI DSS Certification for Acquirers, PSPs and Merchants

(Category A as per references set in chapter 1)

The Payment Systems Operator requires that all Acquirers that store, process, or transmit Card, Cardholder, or Transaction data and all Acquirer agents, including PSPs, that store, process, or transmit Card, Cardholder, or Transaction data on the Acquirer's behalf, adhere to the most current Payment Card Industry PIN Transaction Security Program (PCI PTS) and Payment Card Industry Data Security Standard (PCI DSS). The PCI Security Standards are available on the PCI SSC website at <http://www.pcisecuritystandards.org>.

An Acquirer must certify to the National Scheme Operator that a Merchant is compliant with PCI DSS if it retains or holds any customer financial data that may include payment methods.

4.1.10 NUMO Tokens

(Category A as per references set in Chapter 1)

Neither an Acquirer nor any of the Acquirer's Merchants or Service Providers, including but not limited to any such entity that the National Scheme Operator has registered as a Token Requestor, is permitted to use Account or Transaction data to create or maintain a repository of NUMO Token primary account numbers (PANs) and corresponding Account PANs or perform mapping of NUMO Token PANs to Account PANs for any purpose.

The PAN of a NUMO Card or Access Device or Access Device for which NUMO is the primary Payment Application must not be replaced by, mapped to, or Tokenized with any PAN issued from an Issuer Identification Number (IIN) reserved by the ISO Registration Authority for a competing payment network. Refer to the current ISO Register of Issuer Identification Numbers for more information.

4.1.11 Acquirer Obligations with Respect to Merchants

An Acquirer must fulfill the obligations set forth in this section with respect to each of its Merchants.

4.1.11.1 Payment for Transactions

(Category A as per references set in chapter 1)

The Acquirer must pay the Merchant the amount (either gross or net of Merchant discount or setoff) of all Transactions that the Acquirer acquires from the Merchant in accordance with the Merchant Agreement and the Standards. This obligation is not discharged with regard to a Transaction until the Merchant receives payment from the Acquirer that acquired the Transaction, notwithstanding any Acquirer payment arrangement, including any such arrangement between an Affiliate and its Sponsor. A Merchant Agreement is permitted to provide for an Acquirer to withhold amounts for chargeback reserves or similar purposes in accordance with the Standards.

4.1.11.2 Supplying Materials

(Category B as per references set in chapter 1)

The Acquirer must regularly ensure the Merchant is provided with all materials necessary to conduct POS Transactions in accordance with the Standards and to signify Card acceptance. These materials include POS Terminals, PIN pads, Card acceptance decals, signage, and the like.

9.1.4 شهادة PCI DSS للقابلين و مقدمي خدمات الدفع والتجار

(الفئة أ حسب المراجع المحددة في الفصل 1)

يشترط مشغل شبكة الدفع المحلية، أن تلتزم جميع جهات القبول التي تقوم بتخزين أو معالجة أو نقل بيانات البطاقة أو حامل البطاقة أو المعاملة وجميع وكلاء جهات القبول، بما في ذلك مقدمي خدمات الدفع، الذين يقومون بتخزين أو معالجة أو نقل بيانات البطاقة أو حامل البطاقة أو المعاملة نيابة عن جهات القبول وفق أحدث برنامج لحماية وأمان معاملات رقم التعريف الشخصي لبطاقات الدفع (PCI PTS) ومعييار أمان بيانات صناعة بطاقات الدفع (PCI DSS). تتوفر معايير أمان PCI على موقع ويب PCI SSC على <http://www.pcisecuritystandards.org>.

يجب على جهة القبول أن تتعهد وتشهد لمشغل شبكة الدفع المحلية أن التاجر متوافق مع PCI DSS إذا كان يحتفظ أو يحمل أي بيانات مالية للعميل قد تتضمن طرق الدفع.

10.1.4 رموز نمو

(الفئة أ حسب المراجع المحددة في الفصل 1)

لا يُسمح لجهات القبول، أو التجار القابلين أو مقدمي الخدمة، بالإضافة إلى أي جهة قام مشغل شبكة الدفع المحلية بتسجيلها كطالب رمز، باستخدام بيانات الحساب أو المعاملة لإنشاء أو الاحتفاظ بمستودع أرقام الحسابات الأساسية لرمز نمو، وأرقام الحسابات الأساسية المقابلة أو إجراء تعيين أرقام الحسابات الأساسية لرمز نمو إلى أرقام حسابات أساسية لأي غرض.

ولا يجب استبدال رقم الحساب الأساسي لبطاقة نمو أو جهاز وصول أو جهاز الوصول الذي تعد بطاقة نمو تطبيق الدفع الأساسي له، أو تعيينه أو ترميزه بأي رقم حساب أساسي صادر من رقم تعريف جهة الإصدار المحجوز من قبل هيئة تسجيل المنظمة الدولية للتوحيد القياسي لشبكة دفع منافسة. راجع سجل المنظمة الدولية للتوحيد القياسي الحالي لأرقام تعريف جهة الإصدار للمزيد من المعلومات.

11.1.4 التزامات القابل فيما يتعلق بالتجار

يجب على جهة القبول الوفاء بالالتزامات المحددة في هذا القسم فيما يتعلق بكل من تجارها.

1.11.1.4 الدفع مقابل المعاملات

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب على جهة القبول أن تقوم بدفع المبلغ للتاجر (سواء المبلغ الإجمالي أو الصافي من خصم التاجر أو المقاصة) مقابل جميع المعاملات التي تكتسبها من التاجر وفقاً للعقد والمعايير المنصوص عليها. لا تبرأ ذمة جهة القبول من هذا الالتزام فيما يتعلق بالمعاملة حتى يتلقى التاجر الذي حصل على المعاملة المدفوعات منها، بغض النظر عن بنود عقد الدفع، بما في ذلك أي عقود بين الشركة التابعة وراعيها. يُسمح النص في العقد، بحق جهة القبول باحتجاز مبالغ لاحتياطات رد المبالغ المدفوعة أو أغراض مماثلة وفقاً للمعايير.

2.11.1.4 توريد المواد

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب أن تتحقق جهة القبول بانتظام من تزويد التاجر بجميع المواد اللازمة لإجراء معاملات نقاط البيع طبقاً للمعايير، وللتأكيد على قبول البطاقة. تشمل هذه المواد محطات نقاط البيع، ولوحات رقم التعريف الشخصي، وشارات قبول البطاقة، واللافتات، وما شابه.

4.1.11.3 Authorization of Transactions at Merchants

(Category A as per references set in chapter 1)

With respect to obtaining authorization, an Acquirer must treat all Transactions at a Merchant in the same manner.

4.2 ATM and Other Cash Transactions

This section contains rules applicable for ATM transactions, manual cash disbursements, Deposit Transactions and Instant Credit Transactions (ICT) if applicable.

4.2.1 Display of NUMO Logo at ATM

(Category B as per references set in chapter 1)

The NUMO Logo must be displayed on an ATM. On new or replacement signage incorporating other acceptance marks, the Logo must be afforded at least equal prominence and be at least as large.

The Acquirer must ensure that:

1. Use or display the Logo in accordance with the Standards, and
2. Cease all The Usage of Numo logo immediately upon termination of the ATM Acquirer Agreement, or upon notification by the National Scheme Operator to discontinue such use.

The use or display of any logo does not give an ATM Acquirer any ownership or interest in the Mark.

4.2.2 ATM Network Requirements

(Category A as per references set in chapter 1)

An Acquirer must ensure that its ATMs are connected to the Interchange System within at most 6 months following receipt of the License.

4.2.3 ATM and Bank Branch Terminal Requirements

(Category A as per references set in chapter 1)

Each ATM and Bank Branch Terminal must:

1. Offer cash withdrawals from an Account;
2. Permit the Cardholder to select the account, if the Card supports multiple accounts (e.g. current account and savings account);
3. Not automatically generate an online reversal for the full or partial amount of any authorized cash withdrawal or disbursement when the ATM or Bank Branch Terminal indicates that such Transaction was not completed because the Cardholder failed to collect some or all of the cash dispensed;
4. Have an online connection to the Acquirer host system;
5. Support online PIN for both magnetic stripe Transactions and Chip Transactions;
6. Encrypt the PIN at the point of entry and send the PIN to the Acquirer host system in encrypted form.

Both single-line and multi-line screens that have a screen width of at least 16 characters are acceptable. A minimum screen width of 40 characters is recommended.

3.11.1.4. تفويض المعاملات لدى التجار

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب على جهة القبول عند الحصول على التفويض، أن تقوم بمعاملة جميع المعاملات لدى التاجر بنفس الطريقة.

2.4. أجهزة الصراف الآلي والمعاملات النقدية الأخرى

يحتوي هذا القسم على القواعد المطبقة على معاملات أجهزة الصراف الآلي، والمدفوعات النقدية اليدوية، ومعاملات الإيداع والمعاملات الائتمانية الفورية إذا كان ذلك ممكنًا.

1.2.4. عرض علامة نمو على أجهزة الصراف الآلي

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب عرض علامة نمو على جهاز الصراف الآلي. وفي اللافتات الجديدة أو البديلة التي تتضمن علامات قبول أخرى، ويجب منح الشعار على الأقل أهمية متساوية وأن يكون كبيرًا.

تلتزم جهة القبول بضمان:

1. استخدم أو عرض الشعار وفقًا للمعايير المنصوص عليها.
 2. إيقاف جميع استخدامات شعار نمو فور إنتهاء عقد القابل على أجهزة الصراف الآلي، أو بناءً على إشعار من مشغل شبكة الدفع المحلية لوقف هذا الاستخدام.
- لا يمنح استخدام أو عرض أي شعار للقابل على أجهزة الصراف الآلي أي ملكية أو مصلحة في العلامة.

2.2.4. متطلبات شبكة أجهزة الصراف الآلي

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب على جهة القبول التحقق من أن أجهزة الصراف الآلي الخاصة بها، متصلة بنظام التبادل خلال 6 أشهر على الأكثر بعد استلام الترخيص.

3.2.4. متطلبات أجهزة الصراف الآلي و محطات فروع المصرف

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب على كل جهاز صراف آلي و محطة فرع المصرف:

1. توفير السحب النقدي من الحساب.
2. السماح لحامل البطاقة باختيار الحساب، إذا كانت البطاقة تدعم حسابات متعددة (مثل الحساب الجاري وحساب التوفير).
3. عدم القيام تلقائيًا بتوليد الانعكاس عبر الإنترنت للمبلغ الكامل أو الجزئي لأي سحب أو صرف نقدي مصرح به عندما يشير جهاز الصراف الآلي أو محطة فرع المصرف إلى أن هذه المعاملة لم تكتمل لأن حامل البطاقة فشل في تحصيل بعض أو كل الأموال النقدية التي تم صرفها.
4. أن يكون لديه اتصال عبر الإنترنت بنظام القابل المضيف.
5. دعم رقم التعريف الشخصي عبر الإنترنت لكل من معاملات الشريط المغناطيسي ومعاملات الشريحة.
6. تشفير رقم التعريف الشخصي عند نقطة الدخول وإرسال رقم التعريف الشخصي إلى نظام القابل المضيف بشكل مشفر.

تقبل الشاشات أحادية الخط ومتعددة الخطوط التي يبلغ عرضها 16 حرفًا على الأقل. يوصى بعرض شاشة بحد أدنى 40 حرفًا.

An ATM or Bank Branch Terminal may also support:

1. Merchandise Transactions;
2. Deposit Transactions; and
3. Instant Credit Transactions.

4.2.4 Use of a PIN for Transactions at ATMs and Bank Branch Terminals

(Category A as per references set in Chapter 1)

The following requirements apply at ATMs and Bank Branch Terminals.

1. At an ATM or Bank Branch Terminal, the Cardholder must be verified by online PIN, whether magnetic stripe or chip is used to initiate the Transaction. Online PIN is required for contactless ATM Transactions, regardless of the amount.
2. The Issuer must ensure that Chip Cards support online PIN for these Transactions and decline Transaction attempts where the PIN is entered incorrectly. For Chip Transactions, the Payment Application or Card may also be blocked if the Cardholder exceeds the number of PIN attempts permitted by the Issuer.

4.2.5 ATM Declines

(Category A as per references set in chapter 1)

If the Issuer declines authorization of the Transaction, the Acquirer must not dispense the cash to the Cardholder.

4.2.6 ATM Dispense Error

If the amount dispensed is less than the amount recorded in the ATM's Transaction log, the Issuer has a chargeback right.

If the amount dispensed is greater than the amount recorded in the ATM's Transaction log, the Acquirer may attempt in good faith to rectify the error by contacting the Issuer.

4.2.7 ATM Transaction Restrictions

(Category B as per references set in chapter 1)

ATM Incomplete Transactions Settlement

The National Scheme Operator obliges Acquirers to settle all incomplete Transactions within 4 business days from the Transaction date.

Settlement to be via Surplus Option provided by the National Scheme Operator on the NUMO portal.

Non settlement of incomplete Transactions would lead to a fine for the Acquirer if the Issuer raised a dispute against the unsettled Transaction.

Equally Issuers would be fined if raised disputes were finalized in the Acquirer's favor. For fees details, refer to the signed contract with the National Scheme Operator.

قد تدعم أجهزة الصراف الآلي أو محطات فرع المصرف أيضًا:

1. معاملات البضائع.
2. معاملات الإيداع.
3. المعاملات الائتمانية الفورية.

4.2.4 استخدام رقم التعريف الشخصي للمعاملات في أجهزة الصراف الآلي ومحطات فرع المصرف

(الفئة أ حسب المراجع المحددة في الفصل 1)

تنطبق الشروط التالية على أجهزة الصراف الآلي ومحطات فرع المصارف:

1. في جهاز الصراف الآلي، أو فرع المصرف، يجب التحقق من حامل البطاقة عن طريق رقم التعريف الشخصي عبر الإنترنت، سواء تم استخدام شريط مغناطيسي أو شريحة لبدء المعاملة. ويجب إدخال رقم التعريف الشخصي عبر الإنترنت لمعاملات أجهزة الصراف الآلي الغير متصلة، بغض النظر عن قيمة المبلغ.
2. يجب على جهة الإصدار التأكد من أن بطاقات الشريحة الإلكترونية تدعم رقم التعريف الشخصي عبر الإنترنت لهذه المعاملات، ورفض محاولات تكرار المعاملة عندما يتم إدخال رقم التعريف الشخصي بشكل غير صحيح. أما بالنسبة إلى معاملات الشريحة الإلكترونية، فقد يتم أيضًا حظر تطبيق الدفع أو البطاقة إذا تجاوز حامل البطاقة عدد محاولات تكرار إدخال رقم التعريف الشخصي التي تسمح بها جهة الإصدار.

5.2.4 رفض أجهزة الصراف الآلي

(الفئة أ حسب المراجع المحددة في الفصل 1)

إذا رفضت جهة الإصدار التفويض بالمعاملة، يجب على جهة القبول عدم صرف الأموال النقدية إلى حامل البطاقة.

6.2.4 خطأ صرف أجهزة الصراف الآلي

إذا كان المبلغ الذي تم صرفه أقل من المبلغ المسجل في سجل معاملات جهاز الصراف الآلي، فإن جهة الإصدار لديها حق رد المبالغ المدفوعة. أما إذا كان المبلغ الذي تم صرفه أكبر من المبلغ المسجل في سجل معاملات جهاز الصراف الآلي، فقد يحاول القابل بحسن نية تصحيح الخطأ عن طريق الاتصال بجهة الإصدار.

7.2.4 قيود معاملات أجهزة الصراف الآلي

(الفئة ب حسب المراجع المحددة في الفصل 1)

تسوية المعاملات غير المكتملة لأجهزة الصراف الآلي.

يُلزم مشغل شبكة الدفع المحلية جهات القبول بتسوية جميع المعاملات غير المكتملة خلال 4 أيام عمل من تاريخ المعاملة.

وتكون التسوية عبر خيار الفائض الذي يوفره مشغل شبكة الدفع المحلية على بوابة نمو.

قد يؤدي عدم تسوية المعاملات غير المكتملة إلى فرض غرامة على جهات القبول، إذا أثارت جهة الإصدار نزاعًا ضد المعاملة التي لم يتم تسويتها.

وبمفهوم المخالفة فإنه يتم توقيع غرامة على جهات الإصدار إذا أنتهى النزاع بحكم لصالح جهات القبول. للحصول على قيمة وتفاصيل الغرامات، يجب الرجوع إلى العقد الموقع مع مشغل شبكة الدفع المحلية.

Surplus Option on NUMO Portal.

Surplus option is provided by the National Scheme Operator to enable participants to settle incomplete ATM Transactions or deposit Transactions.

Incomplete ATM transactions

When ATM withdrawal dispensing failed while the Transaction was approved by the Issuer, the Acquirer must reverse the Transaction in order to inform the Issuer of the failed dispense.

Deposits settled to acquirer while being declined by the Issuer with a reason code other than 91

Acquirer bank must reverse back deposit amount to related Card via surplus option.

ICT payment settled to originator while being declined by the recipient with a reason code other than 91 If originating debit tool was a NUMO Card, originator bank must reverse back the ICT authorized amount to originating NUMO Card via surplus option.

4.2.8 ATM Balance Inquiry Service

(Category B as per references set in chapter 1)

The ATM balance inquiry service allows a Cardholder to check the available balance of funds in an Account. Balance inquiries are identified with a value of [TBD] in field [TBD] of authorization messages.

All ATMs that offer balance inquiry to cardholders of other networks must offer the balance inquiry functionality to NUMO Cardholders.

An ATM that offers balance inquiry must display the Account balance on the screen or provide the Cardholder an opportunity to receive a receipt reflecting the Account balance, or both.

4.2.9 ATM Access Fees

(Category B as per references set in chapter 1)

An Acquirer is permitted to charge a fee to the Cardholder for an ATM cash withdrawal. Such a fee is called an ATM Access Fee.

The following requirements apply to ATM Access Fees:

Transaction Field Specifications for ATM Access Fees

At the time of each Transaction on which an ATM Access Fee is imposed, the Acquirer must transmit, in the field specified by the applicable technical specifications then in effect, the amount of the ATM Access Fee separately from the amount of the cash disbursed in the Transaction.

Non-discrimination Regarding ATM Access Fees

An Acquirer must not charge an ATM Access Fee in connection with a Transaction that is greater than the amount of any ATM Access Fee charged by that Acquirer in connection with the transactions of any other network accepted at that ATM.

خيار الفائض على بوابة نمو

يتم توفير خيار الفائض من قبل مشغل شبكة الدفع المحلية، وذلك لتمكين المشاركين من تسوية معاملات أجهزة الصراف الآلي غير المكتملة أو معاملات الإيداع.

معاملات أجهزة الصراف الآلي غير المكتملة

عندما تفشل عملية صرف السحب من أجهزة الصراف الآلي، وكان قد تمت الموافقة على المعاملة من قبل جهة الإصدار، يجب على القابل عكس المعاملة لإبلاغ جهة الإصدار بفشل عملية الصرف.

تسوية الودائع للقابل بينما يتم رفضها من قبل جهة الإصدار برمز سبب غير 91 يجب على مصرف جهة القبول عكس مبلغ الإيداع إلى البطاقة ذات الصلة عبر خيار الفائض. تسوية مدفوعات تكنولوجيا المعلومات والاتصالات للمنشئ بينما يتم رفضها من قبل المستلم برمز سبب غير 91 إذا كانت أداة الخصم الأصلية عبارة عن بطاقة نمو، فيجب على المصرف الأصلي عكس المبلغ المصرح به لتكنولوجيا المعلومات والاتصالات إلى بطاقة نمو الأصلية عبر خيار الفائض.

8.2.4. خدمة الاستعلام عن رصيد أجهزة الصراف الآلي

(الفئة ب حسب المراجع المحددة في الفصل 1)

تتيح خدمة الاستعلام عن رصيد أجهزة الصراف الآلي لحامل البطاقة، التحقق من الرصيد المتاح في الحساب. ويتم تحديد استفسارات الرصيد بقيمة [TBD] في الحقل [TBD] لرسائل التفويض.

يجب على جميع أجهزة الصراف الآلي التي تقدم الاستعلام عن الرصيد لحاملي بطاقات الشبكات الأخرى، أن تقدم وظيفة الاستعلام عن الرصيد لحاملي بطاقات نمو. يجب أن تعرض أجهزة الصراف الآلي التي تقدم الاستعلام عن الرصيد رصيد الحساب على الشاشة، أو توفر لحامل البطاقة فرصة لتلقي إيصال يعكس رصيد الحساب، أو القيام بكليهما.

9.2.4. رسوم الدخول إلى أجهزة الصراف الآلي

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجوز لجهة القبول فرض رسوم على حامل البطاقة مقابل السحب النقدي من أجهزة الصراف الآلي. وتسمى هذه الرسوم برسوم الوصول إلى أجهزة الصراف الآلي.

تنطبق المتطلبات التالية على رسوم الدخول إلى أجهزة الصراف الآلي:

مواصفات حقل المعاملة لرسوم الوصول إلى أجهزة الصراف الآلي

عندما تقوم جهة القبول بفرض رسوم على كل معاملة عند الوصول إلى أجهزة الصراف الآلي، فإنه يجب عليها أن ترسل في الحقل المحدد بالمواصفات الفنية المعمول بها ثم السارية، قيمة مبلغ رسوم الوصول إلى أجهزة الصراف الآلي، بشكل منفصل عن مبلغ النقد المصروف في المعاملة.

عدم التمييز فيما يتعلق برسوم الوصول إلى أجهزة الصراف الآلي.

يجب ألا تتقاضى جهة القبول رسوم الوصول إلى أجهزة الصراف الآلي، فيما يتعلق بالمعاملات التي تكون قيمتها أكبر من مبلغ رسوم الوصول إلى أجهزة الصراف الآلي التي تفرضها جهة القبول، عندما تتعلق بمعاملات أي شبكة أخرى مقبولة في جهاز الصراف الآلي.

Notification of ATM Access Fee

An Acquirer that wishes to charge an ATM Access Fee must notify the National Scheme Operator, in writing, of its intent to do so prior to the planned first imposition of such ATM Access Fee

Cancellation of Transaction

Any Acquirer that plans to charge an ATM Access Fee must notify the Cardholder with a screen display that states the ATM Access Fee policy and provides the Cardholder with an option to cancel the requested Transaction. The Acquirer may additionally notify the Cardholder of the Access Fee via a sticker or other signage on the ATM.

Screen Display

An Acquirer that plans to charge an ATM Access Fee must present a screen display message that is clearly visible to Cardholders on all ATMs at which ATM Access Fees apply. If the Cardholder is given the option of choosing a preferred language in which to conduct the Transaction, the screen display message concerning ATM Access Fees must be presented to the Cardholder in that chosen language.

The National Scheme Operator has the right to review the ATM screen display.

Transaction Receipts

An Acquirer that charges an ATM Access Fee must make available to the Cardholder on the Transaction receipt the ATM Access Fee information required by this Rule, in addition to any other information the Acquirer elects to or is required to provide.

The minimum requirements for the Transaction receipt are:

1. A statement of the amount disbursed to the Cardholder;
2. A statement of the ATM Access Fee amount with language clearly indicating it is a fee imposed by the Acquirer;
3. A separate statement of the combined amount of the ATM Access Fee and the disbursed amount, with language clearly indicating that this amount will be deducted from the Cardholder's Account.

4.2.9.1 ATM Access Fee Fines

(Category B as per references set in chapter 1)

The National Scheme Operator has the right to fine an Acquirer that applies ATM Access Fees in violation of one or more of the above requirements.

4.2.10 Manual Cash Disbursement Transactions

(Category B as per references set in chapter 1)

A cash disbursement may be provided to a NUMO Cardholder by an Acquirer at its offices, via a Bank Branch Terminal, and through its authorized agents.

إخطار رسوم الدخول إلى أجهزة الصراف الآلي.

يجب على جهة القبول التي ترغب في فرض رسوم الوصول إلى أجهزة الصراف الآلي أن تقوم كتابياً بإخطار مشغل شبكة الدفع المحلية بفرض الرسوم، وذلك قبل الغرض الأول المخطط له لرسوم الوصول إلى أجهزة الصراف الآلي.

إلغاء المعاملة.

يجب على جهة القبول عندما تخطط لتحصيل رسوم الوصول إلى أجهزة الصراف الآلي، إخطار حامل البطاقة بعرض على الشاشة توضح سياسة رسوم الوصول إلى أجهزة الصراف الآلي، وتوفر لحامل البطاقة خيار إلغاء المعاملة المطلوبة. بالإضافة إلى ذلك، يجوز للجهة القابلة إخطار حامل البطاقة برسم الوصول عبر ملصق أو لافتة أخرى على جهاز الصراف الآلي.

شاشة العرض

يجب على جهة القبول التي تخطط لتحصيل رسوم الوصول إلى أجهزة الصراف الآلي أن تقدم رسالة عرض على الشاشة تكون مرئية بوضوح لحاملي البطاقات على جميع أجهزة الصراف الآلي التي تنطبق عليها رسوم الوصول إلى أجهزة الصراف الآلي. إذا تم منح حامل البطاقة خيار اختيار اللغة المفضلة لإجراء المعاملة، فيجب تقديم رسالة شاشة العرض المتعلقة برسوم الوصول إلى أجهزة الصراف الآلي إلى حامل البطاقة بتلك اللغة المختارة.

يجوز لمشغل شبكة الدفع المحلية مراجعة شاشة عرض أجهزة الصراف الآلي.

إيصالات المعاملات

يجب على جهة القبول التي تفرض رسوم الوصول إلى أجهزة الصراف الآلي، أن يتيح لحامل البطاقة في إيصال المعاملة معلومات رسوم الوصول إلى أجهزة الصراف الآلي المطلوبة بموجب هذه القاعدة، بالإضافة إلى أي معلومات أخرى يختارها القابل أو يطلب تقديمها.

الحد الأدنى لمتطلبات إيصال المعاملة هي:

1. بيان بالمبلغ المصروف لحامل البطاقة.
2. بيان بقيمة رسوم الوصول إلى أجهزة الصراف الآلي مع لغة تشير بوضوح إلى أنها رسوم مفروضة من قبل جهة القبول.
3. بيان منفصل بالمبلغ المجمع لرسوم الوصول إلى أجهزة الصراف الآلي والمبلغ المصروف، مع لغة تشير بوضوح إلى أنه سيتم خصم هذا المبلغ من حساب حامل البطاقة.

1.9.2.4. غرامات رسوم الوصول إلى أجهزة الصراف الآلي

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجوز لمشغل شبكة الدفع المحلية فرض غرامة على جهة القبول التي تطبق رسوم الوصول إلى أجهزة الصراف الآلي عند إخلالها بالمتطلبات المذكورة أعلاه.

10.2.4 معاملات الصرف النقدي اليدوية

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجوز لجهة القبول أن تقوم بتقديم مدفوعات نقدية إلى حامل بطاقة نمو في مقر عمله، عبر محطة فرع المصرف، ومن خلال وكلائه المعتمدين.

4.2.10.1 Non-discrimination Regarding Cash Disbursement Services

Each Acquirer and each of its authorized cash disbursement agents must comply with the following requirements at each office at which any cash disbursement services are afforded:

1. Not discriminate against or discourage the use of Cards in favor of any card or device bearing or otherwise issued or used in connection with another acceptance brand; and
2. Provide cash disbursement services to all Cardholders on the same terms and regardless of the Issuer.

4.2.10.2 Maximum Amount of Cash Disbursed

An Acquirer and each of its authorized cash disbursement Merchants is permitted to limit the amount of cash provided to any one Cardholder in one day at any individual office. Such limit must not be less than LYD XXX per Cardholder in one day and must be applied uniformly to all Cardholders.

If compliance with this Rule would cause hardship to one or more (but not all) of such individual offices that are required or permitted to provide cash disbursement services, the Acquirer is permitted to establish a maximum cash disbursement amount of less than LYD XXX per person in one day at each such office, provided that the maximum cash disbursement amount:

1. Is not less than LYD XXX;
2. Is not less than the maximum cash disbursement amount established for any other acceptance brand at the office; and
3. Applies only at those offices where the Acquirer can, if requested by the National Scheme Operator, demonstrate that a higher maximum would create a hardship.

4.2.10.3 Deductions or Charges

The Acquirer and each of its authorized cash disbursement Merchants must disburse all cash disbursements without any deduction and without any service or other charge to the Cardholder, unless the charge is imposed to comply with applicable law. Any charge imposed to comply with applicable law must be identified clearly and distinctly to the Cardholder.

4.2.10.4 NUMO Brand Must Be Displayed

An Acquirer and each of its authorized cash disbursement Merchants must display the NUMO Logo at each location where the Acquirer or any such Payment Service Provider provides cash disbursements to NUMO Cardholders.

4.2.11 Deposit Transactions

(Category A as per references set in chapter 1)

Deposit transactions are single message transactions that customers may process at ATMs or Service providers' POS Terminals.

Deposit Transactions are accepted through all NUMO network's ATMs and all announced Service Providers.

Deposit Transactions are subject to be disputed by the originating customer's bank according to the chargeback rules.

4.10.2.4.1 عدم التمييز فيما يتعلق بخدمات الصرف النقدي

يجب على كل جهة قابلة، وكل من وكلائها المعتمدين للصرف النقدي الامتثال للمتطلبات التالية في كل مقر عمل يتم فيه تقديم أي خدمات صرف نقدي:

1. عدم التمييز أو تثبيط استخدام البطاقات لصالح أي بطاقة أو جهاز يحمل أو تم إصداره أو استخدامه بطريقة أخرى فيما يتعلق بعلامة تجارية أخرى مقبولة.
2. تقديم خدمات الصرف النقدي لجميع حاملي البطاقات، وطبقاً للشروط نفسها، وبغض النظر عن جهة الإصدار.

4.10.2.4.2 الحد الأقصى للمبلغ النقدي المصروف

يجوز لجهة القبول، وكل من تجار الصرف النقدي المصرح لهم، لديها تعيين الحد الأقصى من المبلغ النقدي المقدم لحامل بطاقة خلال اليوم الواحد في مقر العمل. غير أنه يجب ألا يقل هذا الحد عن XXX دينار ليبي لكل حامل بطاقة في اليوم الواحد ويجب تطبيقه بشكل موحد على جميع حاملي البطاقات.

وإذا كان الامتثال لهذه القاعدة سيؤدي إلى خلق صعوبات لواحد أو أكثر (ولكن ليس كل) من مقار العمل المختلفة، والمطلوبة أو المسموح بها لتقديم خدمات الصرف النقدي، فيجوز لجهة القبول تحديد الحد الأقصى لمبلغ الصرف النقدي أقل من XXX دينار ليبي، مثلاً، لكل شخص في يوم واحد في مقر العمل من هذا القبيل، شريطة أن يكون الحد الأقصى لمبلغ الصرف النقدي:

1. لا يقل عن XXX دينار ليبي.
2. لا يقل عن الحد الأقصى لمبلغ الصرف النقدي المحدد لأي علامة تجارية مقبولة أخرى في المكتب.
3. ينطبق فقط على تلك المقار، حيث يمكن للقبائل، إذا طلب ذلك من قبل مشغل شبكة الدفع المحلية، إثبات أن الحد الأقصى الأعلى من شأنه أن يخلق صعوبة في التنفيذ.

4.10.2.4.3 الخصومات أو الرسوم

يجب على جهة القبول، وكل من تجار الصرف النقدي المصرح لهم، صرف جميع المدفوعات النقدية دون خصم ودون خدمة أو رسوم أخرى لحامل البطاقة، ما لم يتم فرض الرسوم للامتثال للقانون المعمول به. يجب تحديد أي رسوم مفروضة للامتثال للقانون المعمول به، بشكل واضح وواضح لحامل البطاقة.

4.10.2.4.4 يجب عرض علامة نمو التجارية

يجب على جهة القبول وكل من تجار الصرف النقدي المصرح لهم التابعين لها عرض علامة نمو في كل موقع، حيث توفر جهة القبول أو مقدم خدمة الدفع يقدم مدفوعات نقدية إلى حاملي بطاقات نمو.

4.11.2.4 معاملات الإيداع

(الفئة أ حسب المراجع المحددة في الفصل 1)

معاملات الإيداع هي معاملات ذات رسالة واحدة، يمكن للعملاء معالجتها في أجهزة الصراف الآلي، أو محطات نقاط البيع التابعة لمقدمي الخدمة.

ويتم قبول معاملات الإيداع من خلال جميع أجهزة الصراف الآلي التابعة لشبكة نمو وجميع مقدمي الخدمة المعلنين.

عند حدوث منازعة تتعلق بعملية الإيداع من قبل مصرف العميل، فيجب تسويتها وفقاً لقواعد رد المبالغ المدفوعة.

In addition to approved Transactions, the National Scheme Operator shall settle Transactions with response code 91 (time out response) to Issuer banks, and Issuers are obliged to post those settled Transactions to customers' accounts.

ATMs/Service Provider agents are prohibited from returning cash to the originating customer in case of non-receipt of a normal decline response from the recipient side. Time out response (code 91) or no response are not considered a decline. Such Transactions should be marked by the Acquirer's backend system as "Suspect Transaction", and customers must be informed that Transactions are pending for execution.

For suspect Transactions, acquirers should follow the below rules:

If Acquirer received no response, it is advised to match the Transaction with the network records and act according to the following situations:

- 1) In case Transaction was approved or denied with response code 91, to mark the Transaction as successful at his side.
- 2) In case Transaction was denied with any response code other than 91, Acquirer should initiate a surplus to return the amount to the Transaction originator.

4.2.12 Money Transfer and/or Instant Credit Transaction (ICT)

(Category A as per references set in chapter 1)

The National Payment Scheme/Network Operator is the hub of onus, off us, cross border and local brands money transfer transactions. Instant Credit Transaction (ICT) is one of services provided by the National Scheme/Network Operator that facilitates funds transfer within Libyan market.

A separate license shall be granted to participants in the Money Transfer and/or ICT service which is responsible for transferring funds.

ICT Originating Channels

Licensed Payment Service Providers may provide service through (but not limited to) any of the following channels:

- ATM (for pre-defined recipient list only)
- POS (for pre-defined recipient list only)
- Bank Branch
- PSP Location
- Mobile Application
- Internet Banking

ICT Provided Services

If funding Transaction is initiated from a NUMO Card, then both funding and payment Transactions would be processed via NUMO ICT service.

If funding Transaction is initiated from another financial tool, then only payment Transaction would be submitted via NUMO ICT service.

بالإضافة إلى المعاملات المصرح بها، يجب على مشغل شبكة الدفع المحلية تسوية المعاملات برمز الاستجابة 91 (استجابة المهلة) لمصارف جهات الإصدار، وتلتزم جهات الإصدار بترحيل تلك المعاملات التي تمت تسويتها إلى حسابات العملاء.

يحظر على وكلاء أجهزة الصراف الآلي، ومقدم الخدمة، إعادة الأموال النقدية إلى العميل الأصلي في حالة عدم تلقي استجابة رفض عادية من جانب المستلم. ولا تعتبر استجابة المهلة (الرمز 91) أو عدم الرد رفضاً. ويجب تمييز مثل هذه المعاملات من قبل النظام الأمني لجهة القبول على أنها "معاملة مشبوهة"، ويجب إبلاغ العملاء بأن المعاملات معقدة التنفيذ.

يجب على الجهات القابلة عند وجود معاملات مشبوهة، اتباع القواعد التالية:

إذا لم تتلقى جهة القبول رد، يُنصح بمطابقة المعاملة مع سجلات الشبكة والتصرف وفقاً للحالات التالية:

1. في حالة الموافقة على المعاملة أو رفضها برمز الاستجابة 91، توضع علامة على المعاملة على أنها ناجحة من جانبه.
2. في حالة رفض المعاملة بأي رمز استجابة بخلاف 91، يجب على جهة القبول الخصم من الفائض لإعادة المبلغ إلى منشئ المعاملة.

12.2.4. المعاملات الائتمانية الفورية

(الفئة أ حسب المراجع المحددة في الفصل 1)

مشغل شبكة الدفع المحلية هو محور معاملات تحويل الأموال عبر الحدود والعلامات التجارية المحلية. معاملة الائتمان الفورية هي خدمة يقدمها مشغل شبكة الدفع المحلية لتسهيل تحويل الأموال.

يمنح ترخيص منفصل للمشاركين في خدمة تكنولوجيا المعلومات والاتصالات الذين سيكونون مسؤولين عن تحويل الأموال، وتعتبر معاملة الائتمان الفورية طريقة أسرع وأسهل لتحويل الأموال من قنوات التحويل العادية.

القنوات المنشئة لتكنولوجيا المعلومات والاتصالات

يجوز لمقدمي خدمة الدفع المرخص لهم تقديم الخدمة من خلال (على سبيل المثال لا الحصر) أي من القنوات التالية:

- أجهزة الصراف الآلي (لقائمة المستلمين المحددة مسبقاً فقط).
- نقاط البيع (لقائمة المستلمين المحددة مسبقاً فقط).
- فرع المصرف.
- موقع مقدم خدمة الدفع.
- تطبيق الهاتف المحمول.
- الخدمات المصرفية عبر الإنترنت.

الخدمات التي تقدمها تكنولوجيا المعلومات والاتصالات

إذا تم البدء في معاملة التمويل من بطاقة نمو، فستتم معالجة معاملات التمويل والدفع عبر خدمة تكنولوجيا المعلومات والاتصالات نمو.

وإذا تم البدء في معاملة التمويل من أداة مالية أخرى، فسيتم إرسال معاملة الدفع فقط عبر خدمة تكنولوجيا المعلومات والاتصالات نمو.

Funding Transaction

Purchase dual message with no exceptional clearing handling; standard chargeback rules apply (Refer to chargeback rules.)

Payment Transaction

Credit transaction to the recipient NUMO Card.

Members' Responsibilities

ICT participants are responsible for monitoring ICT Transactions and ensure compliance with Libyan laws regarding Anti Money Laundering and terrorist financing, in addition to adherence to CENTRAL BANK OF LYBIA parameters regarding money transfers.

ICT Transaction data shall include full sender and receiver data in the initiated/responded request (Name, Address, City, etc.).

The National Scheme/Network Operator obliges participants to apply all KYC checks for all ICT Transactions as part of originator/recipient responsibilities.

ICT recipient shall post the transaction instantly to the receiving Account.

ICT data will be part of the data required to be reported to the National Scheme Operator.

Limitations

The National Scheme Operator forbids using ICT as a replacement for Card acceptance for purchase Transactions.

The National Scheme Operator will auto settle all approved payment requests to the recipients' bank in the next business day following the authorization date.

In addition to approved payment Transactions, the National Scheme Operator shall auto settle payment transactions with response code 91 (time out response) to recipients' banks, and recipients are obliged to post those settled transactions to customers' Accounts.

ATMs/Service Provider agents are prohibited from returning cash to the originating customer in case of not receiving a normal decline response from the recipient side for the payment Transaction. Time out response (code 91) or no response are not considered a decline; the payment Transaction should be marked by the originator bank's backend system as "Suspect Payment Transaction", and originating customers must be informed that the Transaction is pending for execution.

معاملة التمويل

هي شراء رسالة مزدوجة بدون معالجة مقاصة استثنائية؛ وتطبق القواعد المعيارية لرد المبالغ المدفوعة (راجع قواعد رد المبالغ المدفوعة).

معاملات الدفع

معاملة الائتمان إلى مستلم بطاقة نمو.

مسؤوليات الأعضاء

يعد المشاركون في تكنولوجيا المعلومات والاتصالات، مسؤولون بالتضامن عن مراقبة معاملات تكنولوجيا المعلومات والاتصالات، وضمان الامتثال للقوانين الليبية فيما يتعلق بمكافحة غسل الأموال وتمويل الإرهاب، بالإضافة إلى الالتزام بمعايير مصرف ليبيا المركزي فيما يتعلق بتحويلات الأموال. ويجب أن تتضمن بيانات معاملات تكنولوجيا المعلومات والاتصالات، البيانات الكاملة للمرسل والمستقبل في الطلب الذي تم البدء والرد عليه (الاسم والعنوان والمدينة وما إلى ذلك).

يُلزم مشغل شبكة الدفع المحلية، المشاركون بتطبيق جميع عمليات التحقق من "اعرف عميلك" على جميع معاملات تكنولوجيا المعلومات والاتصالات كجزء من مسؤوليات المنشئ والمستلم.

يجب على مستلم تكنولوجيا المعلومات والاتصالات إرسال المعاملة على الفور إلى الحساب المستلم.

ستكون بيانات تكنولوجيا المعلومات والاتصالات جزءًا من البيانات المطلوب إبلاغها لمشغل شبكة الدفع المحلية.

القيود

يحظر مشغل شبكة الدفع المحلية، استخدام تكنولوجيا المعلومات والاتصالات، كبديل لقبول البطاقة في معاملات الشراء.

يلتزم مشغل شبكة الدفع المحلية بتسوية جميع طلبات الدفع المصرح بها تلقائيًا لمصرف المستلمين في يوم العمل التالي بعد تاريخ التفويض.

بالإضافة إلى معاملات الدفع المصرح بها، يجب على مشغل شبكة الدفع المحلية تسوية معاملات الدفع تلقائيًا برمز الاستجابة 91 (استجابة المهلة) لمصرف المستلمين، ويلتزم المستلمون بترحيل تلك المعاملات التي تمت تسويتها إلى حسابات العملاء.

يحظر على وكلاء أجهزة الصراف الآلي، ومقدمي الخدمة، إعادة الأموال النقدية إلى العميل الأصلي في حالة عدم تلقي استجابة رفض عادية من جانب المستلم لمعاملة الدفع. ولا تعتبر استجابة المهلة (الرمز 91) أو عدم الرد، رفضًا؛ ويجب تمييز معاملة الدفع من خلال النظام الأمني للمصرف المنشئ على أنها "معاملة دفع مشبوهة"، ويجب إبلاغ العملاء الأصليين بأن المعاملة معلقة للتنفيذ.

For suspect payment Transactions, Acquirers must follow the below rules:

If originator received no response, to match the payment Transaction with the network records and act according to the following situations:

- 1) In case Transaction was approved or denied with response code 91, to mark the Transaction as successful at his side.
- 1) In case Transaction was denied with any response code other than 91 or not found in the network reconciliation report, originator should return the amount to the originating customer by reversing the amount through the originating channel.

The National Scheme Operator obliges originator banks to settle the denied ICT payment Transactions in 3 business days of the request date. If not, recipient may have a chargeback right for the unsettled deposit amount. (Refer to the chargeback rules.)

4.3 Merchant Requirements

This section contains the rules applicable to a Merchant that accepts NUMO. The Service Provider/Bank may not subcontract, sublicense, assign, license, franchise, or in any manner extend or transfer to any third party, any right or obligation of the Service Provider set forth in the Merchant Agreement.

4.3.1 The Usage of Numo Brand

(Category A as per references set in chapter 1)

A Merchant is only permitted to use the Brand in accordance with a Merchant Agreement with its Acquirer.

The Merchant Agreement must provide that:

1. Any Usage of Numo Brand by a Merchant in advertising, acceptance decals, or signs, must be in accordance with the Standards, including any reproduction, usage, and artwork Standards, which in effect from time to time; and
2. The Merchant's use or display of the Brand will terminate effective with the termination of the Merchant Agreement, or upon notification by the National Scheme Operator to discontinue such use or display.

A Merchant must:

1. Use or display the Logo only in accordance with the Standards, and
2. Cease all The Usage of Numo Brand immediately upon termination of the Merchant Agreement, or upon notification by the National Scheme Operator to discontinue such use.

The use or display of any Logo does not give a Merchant any ownership right or interest in the Brand.

4.3.2 Merchant Location

(Category A as per references set in chapter 1)

A Merchant has the right to accept NUMO Cards only in Libya.

The Merchant must hold all necessary permits to conduct business in Libya.

The Merchant's location is the address where the Merchant conducts the business described in and governed by the Merchant Agreement.

بالنسبة لمعاملات الدفع المشبوهة، يجب على القابلين اتباع القواعد التالية:

إذا لم يتلقى المصرف المنشئ رد، لمطابقة معاملة الدفع مع سجلات الشبكة والتصرف وفقًا للحالات التالية:

1. في حالة الموافقة على المعاملة أو رفضها برمز الاستجابة 91، توضع علامة على المعاملة على أنها ناجحة من جانبه.
2. في حالة رفض المعاملة بأي رمز استجابة بخلاف 91 أو لم يتم العثور عليها في تقرير تسوية الشبكة، يجب على المنشئ إعادة المبلغ إلى العميل الأصلي عن طريق عكس المبلغ من خلال القناة الأصلية.

على مشغل شبكة الدفع المحلية، إلزام المصارف المنشئة بتسوية معاملات مدفوعات تكنولوجيا المعلومات والاتصالات المرفوضة خلال 3 أيام عمل من تاريخ الطلب. وإذا لم يكن الأمر كذلك، فقد يكون لدى المستلم حق رد المبالغ المدفوعة لمبلغ الإيداع الذي لم يتم تسويته. (راجع قواعد رد المبالغ المدفوعة).

3.4 متطلبات التاجر

يحتوي هذا القسم على القواعد المطبقة على التاجر الذي يقبل نمو. يجوز لمقدم الخدمة / المصرف التعاقد من الباطن، أو الترخيص من الباطن، أو التنازل، أو الترخيص، أو الامتياز، أو بأي شكل من الأشكال تمديد أو نقل أي حق أو التزام لمقدم الخدمة المنصوص عليه في اتفاقية التاجر إلى أي طرف ثالث.

1.3.4 استخدام علامة نمو التجارية

(الفئة أ حسب المراجع المحددة في الفصل 1)

يُسمح للتاجر فقط باستخدام العلامة التجارية طبقاً للنصوص التعاقدية مع الجهة القابلة.

يجب أن ينص العقد على ما يلي:

1. يجب أن يكون استخدام علامة نمو التجارية من قبل التاجر في الإعلان، أو شارات القبول أو اللافتات وفقاً للمعايير، بما في ذلك معايير النسخ والاستخدام والأعمال الفنية التي تسري من وقت لآخر، وطبقاً لقوانين حماية الملكية الفكرية.
2. ينتهي حق استخدام التاجر أو عرضه للعلامة التجارية مع إنتهاء مدة التعاقد، أو بناءً على إشعار من مشغل شبكة الدفع المحلية لوقف هذا الاستخدام أو العرض.

يجب على التاجر:

1. استخدام أو عرض العلامة وفقاً للمعايير فقط.
 2. وقف جميع استخدامات علامة نمو التجارية فور إنتهاء مدة العقد، أو بناءً على إشعار من مشغل شبكة الدفع المحلية لوقف هذا الاستخدام.
- استخدام أو عرض العلامة لا يمنح للتاجر حق ملكية على العلامة التجارية.

2.3.4 موقع التاجر

(الفئة أ حسب المراجع المحددة في الفصل 1)

يكون للتاجر حق قبول بطاقات نمو في ليبيا فقط.

يجب على التاجر أن يكون حاملاً لجميع التراخيص اللازمة لممارسة الأعمال التجارية في ليبيا. موقع التاجر هو العنوان الذي يدير فيه التاجر أعماله التجارية، والموضحة في العقد.

4.3.2.1 Disclosure of Merchant Name and Location

(Category B as per references set in chapter 1)

A Merchant must prominently and clearly disclose to the Cardholder at all points of interaction:

1. its name, so that the Cardholder can easily distinguish the Merchant from any other party, such as a supplier of products or services to the Merchant; and
2. Its location (physical address). The Merchant location must be disclosed before the Cardholder is prompted to provide Card information.

The Merchant name and location, as disclosed to the Cardholder at the POI and on Transaction receipts, must be the same as what is provided in authorization and clearing Transaction messages.

4.3.3 Agent Location

(Category A as per references set in chapter 1)

An Agent has the right to accept NUMO Cards only in Libya.

The Agent must hold all necessary permits to conduct business in Libya.

The Agent's location is the address where the Agent conducts the business described in and governed by the Agent Agreement.

4.3.2.2 Disclosure of Agent Name and Location

(Category B as per references set in chapter 1)

Each Agent must prominently and clearly disclose to the Cardholder at all points of interaction:

- Its name, so that the Cardholder can easily distinguish the Agent from any other party, such as a supplier of products or services to the Agent; and
- Its location (physical address). The Agent location must be disclosed before the Cardholder is prompted to provide Card information.

The Agent name and location, as disclosed to the Cardholder at the POI and on Transaction receipts, must be the same as what is provided in authorization and clearing Transaction messages.

4.3.4 Responsibility for Transactions

(Category B as per references set in chapter 1)

Each Merchant must ensure that the Cardholder is easily able to understand that the Merchant is responsible for the Transaction, including delivery of the goods (whether physical or digital) or provision of the services that are the subject of the Transaction, and for customer service and dispute resolution, all in accordance with the terms applicable to the Transaction.

4.3.5 Merchant Obligations for Card Acceptance

4.3.5.1 Honor All Cards Rule

(Category A as per references set in chapter 1)

A Merchant must honor all valid Cards without discrimination when properly presented for payment. A Merchant must maintain a policy that does not discriminate among Acquirers seeking to make purchases with a Card.

1.2.3.4 الإفصاح عن اسم التاجر وموقعه

1. (الفئة ب حسب المراجع المحددة في الفصل 1)

يجب على التاجر الإفصاح بشكل واضح وبارز لحامل البطاقة في جميع نقاط التفاعل:

1. اسمه، حتى يتمكن حامل البطاقة من تمييز التاجر بسهولة عن غيره من التجار، مثل مورد المنتجات أو الخدمات للتاجر.
2. موقعه (العنوان الفعلي). يجب الكشف عن موقع التاجر قبل مطالبة حامل البطاقة بتقديم معلومات البطاقة.

يجب أن يكون اسم التاجر وموقعه، كما تم الكشف عنه لحامل البطاقة في نقطة التفاعل وفي إيصالات المعاملة، مطابقاً لما هو منصوص عليه في رسائل معاملة التفويض والمقاصة.

3.3.4 موقع الوكيل

(الفئة أ حسب المراجع المحددة في الفصل 1)

يكون للوكيل حق قبول بطاقات نمو في ليبيا فقط.

يجب أن يكون الوكيل حاملاً لجميع التراخيص اللازمة لممارسة الأعمال التجارية في ليبيا.

موقع الوكيل هو العنوان الذي يدير فيه الأعمال التي يحكمها والموضحة في عقد الوكالة.

2.2.3.4 الإفصاح عن اسم الوكيل وموقعه

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب على كل وكيل الإفصاح بشكل واضح وبارز لحامل البطاقة في جميع نقاط التفاعل:

- اسمه، بحيث يمكن لحامل البطاقة تمييز الوكيل بسهولة عن أي طرف آخر، مثل مورد المنتجات أو الخدمات للوكيل.
- موقعه (العنوان الفعلي). يجب الكشف عن موقع الوكيل قبل مطالبة حامل البطاقة بتقديم معلومات البطاقة.

يجب أن يكون اسم الوكيل وموقعه، كما تم الكشف عنه لحامل البطاقة في نقطة التفاعل وفي إيصالات المعاملة، مطابقاً لما تم توفيره في رسائل معاملة التفويض والمقاصة.

4.3.4 المسؤولية عن المعاملات

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب على كل تاجر التحقق من أن حامل البطاقة قادراً بسهولة على فهم أن التاجر مسؤول عن المعاملة، بما في ذلك تسليم البضائع (سواء كانت مادية أو رقمية) أو توفير الخدمات محل المعاملة، وخدمة العملاء وحل النزاع، كل ذلك وفقاً للشروط المطبقة على المعاملة.

5.3.4 التزامات التاجر لقبول البطاقة

1.5.3.4 احترام قاعدة جميع البطاقات

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب على التاجر الالتزام بمبدأ المساواة بين جميع البطاقات الصالحة، عدم التمييز عند تقديمها بشكل صحيح للدفع. ويجب على التاجر الالتزام بمبدأ عدم التمييز بين الجهات القابلة التي تسعى لإجراء عمليات شراء باستخدام البطاقة.

4.3.5.2 Limited Acceptance

(Category A as per references set in chapter 1)

A Merchant that does not deal with the public at large (for example, a private club) is permitted to limit acceptance to valid and properly presented Cards of Cardholders that have purchasing privileges with the Merchant.

4.3.5.3 Obtain an Authorization

(Category A as per references set in chapter 1)

The Merchant must obtain authorization from the Issuer before completing a Transaction, with the exception of refunds.

A Merchant must inform the Cardholder of any estimated amount for which authorization will be requested and must obtain the Cardholder's consent to the amount before initiating the authorization request, unless authorization is requested for an amount otherwise approved by the Cardholder as the final Transaction amount.

4.3.5.4 Cardholder Verification Method (CVM)

The CVM depends on whether the Transaction is Card-present or Card-not-present.

In a Card-not-present Transaction environment, the Merchant is permitted to complete the Transaction without using a CVM.

No CVM is required for a refund Transaction.

4.3.5.5 Consumer Device CVM

(Category A as per references set in chapter 1)

A Consumer Device CVM (CDCVM) is only permitted to be used as a CVM for Transactions if:

1. The CDCVM has been approved by the National Scheme Operator; and
2. The person authenticated has been identified and verified as an authorized Cardholder in accordance with Issuer-approved parameters.

When a CVM is requested or required for a Transaction and a CDCVM is used, the Issuer must either perform CDCVM verification or confirm that CDCVM verification was successful.

4.3.5.6 Additional Cardholder Identification

(Category B as per references set in chapter 1)

A Merchant is permitted to request but must not require a Cardholder to provide additional identification information as a condition of Card acceptance, unless such information is required to complete the Transaction, such as for shipping purposes, or the Standards specifically permit or require such information to be collected.

2.5.3.4 القبول المحدود

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجوز للتاجر الذي لا يتعامل مع الجمهور بشكل عام (على سبيل المثال، نادٍ خاص) الحد من القبول بطاقات حاملي البطاقات الصالحة، والمقدمة بشكل صحيح والتي تتمتع بامتيازات شراء مع التاجر.

3.5.3.4 الحصول على تفويض

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب أن يحصل التاجر على تفويض من جهة الإصدار قبل إتمام المعاملة، باستثناء المبالغ المستردة.

يجب على التاجر إبلاغ حامل البطاقة بأي مبلغ تقديري سيتطلبه التفويض، ويجب أن يحصل على موافقة حامل البطاقة على المبلغ قبل الشروع في طلب التفويض، ما لم يتطلب التفويض مبلغ وافق عليه حامل البطاقة باعتباره المبلغ النهائي للمعاملة.

4.5.3.4 طريقة التحقق من حامل البطاقة (CVM)

يعتمد رمز التحقق من البطاقة على ما إذا كانت معاملة البطاقة موجودة أو معاملة بطاقة غير الموجودة.

في حالة معاملات البطاقة غير الموجودة، يجوز للتاجر إكمال المعاملة دون استخدام رمز التحقق من البطاقة.

لا يلزم استخدام رمز التحقق من البطاقة لمعاملة الاسترداد.

5.5.3.4 جهاز المستهلك CVM

(الفئة أ حسب المراجع المحددة في الفصل 1)

يُسمح باستخدام جهاز المستهلك CVM (CDCVM) فقط باعتباره طريقة التحقق من حامل البطاقة للمعاملات في الحالات التالية:

1. إذا تمت الموافقة على جهاز المستهلك CVM من قبل مشغل شبكة الدفع المحلية.
2. إذا تم تحديد الشخص المصرح به، والتحقق منه كحامل بطاقة المصرح له وفقًا للمعايير المعتمدة من جهة الإصدار.

عندما يتم طلب التحقق من حامل البطاقة، أو كان مطلوبًا لمعاملة معينة، وتم استخدام جهاز المستهلك CVM، يجب على جهة الإصدار إما إجراء تحقق CDCVM أو التأكيد أن تحقق CDCVM كان ناجحًا.

6.5.3.4 التعريف الإضافي لحامل البطاقة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجوز للتاجر أن يطلب من حامل البطاقة تقديم معلومات تعريف إضافية كشرط لقبول البطاقة، ولكن يجب ألا يطلب منه ذلك، إلا إذا كانت معلومات التعريف الإضافية مطلوبة لإكمال المعاملة، مثل أغراض الشحن، أو تسمح المعايير على وجه التحديد أو تطلب هذه المعلومات التي يتم جمعها.

4.3.5.7 Prohibited Merchant Practices

A. Merchant Surcharging

(Category B as per references set in chapter 1)

A Merchant must not directly or indirectly require any Cardholder to pay a surcharge or any part of any Merchant discount or any contemporaneous finance charge in connection with a Transaction.

The above rule may be disregarded in the following situations:

- If the additional fee is added to all other payment types. The fee could be, without limitation, any of the following: (postage, expedited service, convenience fees, etc.)
- A surcharge fee may be allowed when payment by NUMO Card is an alternative form of payment not ordinarily accepted by a Merchant or Payment Service provider. The Acquirer must obtain a special approval from the National Scheme Operator for the specific Merchant or merchant Category C as per references set in chapter 1.

A Merchant is permitted to provide a discount to its customers for cash payments.

For purposes of this Rule:

1. A surcharge is any fee charged in connection with a Transaction that is not charged if another payment method is used.
2. The Merchant discount fee is any fee a Merchant pays to an Acquirer so that the Acquirer will acquire the Transactions of the Merchant.

B. Discrimination/Cardholder Choice

(Category B as per references set in chapter 1)

A Merchant must not engage in any acceptance practice that discriminates against or discourages the use of a Card in favor of any other acceptance brand or that prevents or discourages the Cardholder from choosing to pay with NUMO.

C. Discounts at POI

(Category B as per references set in chapter 1)

A discount or other benefit may be applied at the POI upon presentation of a particular NUMO Card for payment. Promotion of any such discount or other benefit is permitted provided such promotion does not result in discrimination against other NUMO Cards. The National Scheme Operator has the sole right to determine whether a promotion discriminates against other NUMO Cards.

D. Minimum/Maximum Transaction Amount Prohibited

(Category B as per references set in chapter 1)

A Merchant must not require, or indicate that it requires, a minimum or maximum Transaction amount to accept a valid and properly presented Card.

This rule applies to both the contact and contactless payment functionalities of a Dual Interface POS Terminal.

7.5.3.4 ممارسات التاجر المحظورة

أ. رسوم التاجر الإضافية

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب على التاجر ألا يطلب بشكل مباشر أو غير مباشر من حامل البطاقة، دفع رسوم إضافية أو جزء من خصم لتاجر أو رسوم تمويل معاصرة فيما يتعلق بالمعاملة. ويجوز عدم تطبيق هذه القاعدة في الحالات التالية:

- إذا تم إضافة الرسوم الإضافية إلى جميع أنواع الدفع الأخرى. ويمكن أن تكون الرسوم، على سبيل المثال (رسوم البريد، الخدمة العاجلة، رسوم الراحة، إلخ).
- قد يُسمح بدفع رسوم إضافية عندما يكون الدفع بواسطة بطاقة نمو طريقة بديلة للدفع لا يقبلها التاجر أو مقدم خدمة الدفع عادةً. ويجب أن تحصل جهة القبول في هذه الحالة على موافقة خاصة من مشغل شبكة الدفع المحلية للتاجر أو التاجر المحدد من الفئة ج وفقًا للمراجع المحددة في الفصل 1.

يجوز للتاجر تقديم خصم لعملائه على المدفوعات النقدية.

لأغراض تطبيق هذه القاعدة، يجب مراعاة الآتي:

1. التكلفة الإضافية هي رسوم يتم تحصيلها فيما يتعلق بمعاملة مالية لا يتم تحصيلها في حالة استخدام طريقة دفع أخرى.
2. رسوم خصم التاجر هي رسوم يدفعها التاجر إلى جهة القبول حتى تكتسب الأخيرة معاملات التاجر.

ب. التمييز/اختيار حامل البطاقة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب على التاجر عدم القيام بالممارسات التي من شأنها أن تميز، أو لا تشجع على استخدام البطاقة لصالح علامة قبول تجارية أخرى، أو تمنع حامل البطاقة أو تدفعه على اختيار الدفع بنمو.

ت. الخصومات في نقاط الدفع

(الفئة ب حسب المراجع المحددة في الفصل 1)

قد يتم تطبيق خصم، أو ميزة أخرى في نقاط البيع عند تقديم بطاقة نمو معينة للدفع. ويُسمح بالترويج لأي خصم أو ميزة أخرى، شريطة ألا يؤدي هذا الترويج إلى التمييز ضد بطاقات نمو الأخرى. ويختص مشغل شبكة الدفع المحلية وحده بتقدير ما إذا كان العرض الترويجي يميز ضد بطاقات نمو الأخرى.

ث. الحد الأدنى والأقصى لمبلغ المعاملة المحظورة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب على التاجر ألا يطلب أو يشير إلى أنه يتطلب حدًا أدنى أو أقصى لمبلغ المعاملة لقبول بطاقة صالحة ومعرضة بشكل صحيح. تنطبق هذه القاعدة على كل من وظائف الدفع عن بعد، والدفع لمحطة نقاط البيع ذات الواجهة المزدوجة.

E. Cardholder Right of Dispute

(Category B as per references set in chapter 1)

A Merchant must not impose, as a condition of NUMO Card acceptance, a requirement that the Cardholder waive a right to dispute a Transaction.

F. Illegal or Brand-Damaging Transactions

(Category A as per references set in chapter 1)

A Merchant must not submit to its Acquirer, and an Acquirer must not submit to the Interchange System, any Transaction that is illegal, or in the sole discretion of the National Scheme Operator, could damage the goodwill of the National Scheme Operator or reflect negatively on the Brand.

The National Scheme Operator considers any of the following activities to be in violation of this Rule:

1. The sale or offer of sale of a product or service other than in full compliance with law then applicable to the Acquirer, Issuer, Merchant, Cardholder, Cards, or the National Scheme Operator.
2. The sale of a product or service, including an image, which is patently offensive and lacks serious artistic value (such as, by way of example and not limitation, images of nonconsensual sexual behavior, sexual exploitation of a minor, nonconsensual mutilation of a person or body part, and bestiality), or any other material that the National Scheme Operator deems unacceptable to sell in connection with the Brand.

An Acquirer that has been notified of a Merchant's noncompliance with this Rule and that fails promptly to cause the noncompliant practice to cease, or that has been notified multiple times regarding violations of this Rule, is subject, at the Acquirer's expense, and in addition to any other noncompliance measures, to one or both of the following:

- 1) A risk review carried out by the National Scheme Operator.
- 2) An audit at the sole expense of the Acquirer by a third party selected by the National Scheme Operator, of the Acquirer's acquiring practices.

In addition to or in lieu of any other disciplinary action by the National Scheme Operator, an Acquirer found to be in violation of this Rule may be assessed, with respect to each Merchant, entity, or person on whose behalf the Acquirer submits illegal or brand-damaging Transactions into interchange:

- LYD XXXX or
- LYD XXX per day, retroactive to the first day of the noncompliant practice, provided the Acquirer can show clear and convincing evidence that such noncompliant practice began less than 30 days prior to the date of the National Scheme Operator's notification to the Acquirer.

G. Valid Transactions

(Category A as per references set in chapter 1)

A Merchant must submit to its Acquirer only records of valid Transactions between the Merchant and a legitimate Cardholder.

A Merchant must not submit to its Acquirer a Transaction that the Merchant knows or should have known to be fraudulent or not authorized by the Cardholder, or that it knows or should have known to be authorized by a Cardholder colluding with the Merchant for a fraudulent purpose. For purposes of this Rule, the Merchant is deemed to be responsible for the conduct of its employees, agents, and representatives.

ج. حق حامل البطاقة في الاعتراض

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب على التاجر ألا يفرض على حامل البطاقة، كشرط لقبول بطاقة نمو أن يتنازل عن حقه في الاعتراض على معاملة.

ج. المعاملات غير القانونية أو التي تضر بالعلامة التجارية

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب على التاجر ألا يقدم إلى جهة القبول، وعلى جهة القبول ألا تقدم إلى نظام التبادل، أي معاملة غير قانونية، أو كانت من الممكن وفقًا لتقدير مشغل شبكة الدفع المحلية، إنها تلحق الضرر بالسمعة الحسنة مشغل شبكة الدفع المحلية، أو تنعكس سلبيًا على العلامة التجارية. تعتبر الأنشطة التالية في تقدير مشغل شبكة الدفع المحلية إخلالًا بتطبيق هذه القاعدة:

1. بيع أو عرض بيع منتج أو خدمة بخلاف الامتثال الكامل للقانون المطبق آنذاك على جهة القبول أو جهة الإصدار أو التاجر أو حامل البطاقة أو البطاقات أو مشغل شبكة الدفع المحلية.
2. بيع منتج أو خدمة، بما في ذلك صورة، مسيئة بشكل واضح وتفقر إلى قيمة فنية جادة على سبيل المثال (صور السلوك الجنسي غير الرضائي، والاستغلال الجنسي لقاصر، والتشويه غير الرضائي لشخص أو جزء من الجسم والوحشية)، أو أي مادة أخرى يقدر مشغل شبكة الدفع المحلية أنها غير مقبولة للبيع فيما يتعلق بالعلامة التجارية.

تعد جهة القبول التي تم إخطارها بعدم امتثال التاجر لهذه القاعدة، والتي فشلت في إيقاف الممارسة غير الممتثلة على الفور، أو التي تم إخطارها عدة مرات فيما يتعلق بالاخلال بهذه القاعدة خاضعة، على نفقتها، بالإضافة إلى أي إجراءات عدم امتثال أخرى، إلى أحد الإجراءين التاليين أو كليهما:

1. مراجعة المخاطر التي يقوم بها مشغل شبكة الدفع المحلية.
2. تدقيق على حساب جهة القبول وحدها، من قبل طرف ثالث يختاره مشغل شبكة الدفع المحلية، لممارسات القبول الخاصة بالقابل.

وبدلاً من إتخاذ الإجراءات التأديبية في مواجهة جهة القبول، يجوز لمشغل شبكة الدفع المحلية، إجراء تقييم لجهة القبول التي يثبت أنها لم تلتزم بهذه القاعدة، فيما يتعلق بكل تاجر أو جهة أو شخص يقدم القابل نيابةً عنه المعاملات غير القانونية أو الإضرار بعلامة تجارية في التبادل:

- XXXX دينار ليبي.
- XXX دينار ليبي لليوم الواحد، وبأثر رجعي حتى اليوم الأول من ممارسة عدم الامتثال، شريطة أن يثبت بشكل قاطع أن جهة القبول قامت بهذه الممارسة غير الممتثلة وإنها قد بدأت قبل أقل من 30 يومًا من تاريخ إخطار مشغل شبكة الدفع المحلية إلى القابل.

خ. المعاملات الصالحة

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب على التاجر أن يقدم إلى جهة القبول فقط، سجلات المعاملات الصالحة بين التاجر وحامل البطاقة الشرعي.

يجب على التاجر أن لا يقوم بارسال معاملة إلى جهة القبول يعلم أو كان ينبغي أن يعلم أنها احتيالية أو غير مصرح بها من قبل حامل البطاقة، أو أنه يعلم أو كان ينبغي أن يكون قد علم بأنه مصرح له من قبل حامل البطاقة الذي يتواطأ مع التاجر لغرض احتيالي. لأغراض هذه القاعدة، يعتبر التاجر مسؤولاً عن سلوك موظفيه ووكلائه وممثليه.

4.3.5 Multiple Transaction

(Category B as per references set in chapter 1)

All products and services purchased in a single Transaction must be included in one total amount on a single Transaction receipt and reflected in a single Transaction record, with the following exceptions:

- A Merchant is permitted to accept more than one payment method for a single purchase, provided that the Transaction record and receipt reflects only the portion of the purchase to be paid by means of an Account.
- A Merchant is permitted to complete a consumer's purchase of multiple products or services by individually billing the products or services in separate Transactions to the same Account, in accordance with the acceptance procedures.

4.3.6 Partial Payment

(Category B as per references set in chapter 1)

A Merchant is prohibited from effecting a Transaction where only a part of the total purchase amount is included on the Transaction record and receipt, except in the following circumstances:

- The customer pays a portion of the total purchase amount by means of an Account and pays the remaining balance by another payment method, such as cash or check.
- The products or services will be delivered or performed after the Transaction date, one Transaction receipt represents a deposit, and the second Transaction receipt represents payment of the balance. The Merchant must note the words “deposit” and “balance” on the Transaction receipts as appropriate. The second Transaction receipt is contingent on the delivery or performance of the products or services, and must not be presented until after the products or services are delivered or performed.
- The Cardholder has agreed in writing to be billed by the Merchant in installments, and has specified the installment payment schedule and/or each installment payment amount to be billed to the Account

4.3.7 Specific Terms of a Transaction

(Category B as per references set in chapter 1)

The Merchant is permitted to impose specific terms governing a Transaction by, for example:

1. Legible printing of the specific terms on the Transaction receipt; or
2. Disclosing the specific terms by other means, such as by signage or literature, provided the disclosure is sufficiently prominent and clear so that a reasonable person would be aware of and understand the disclosure before the Transaction is completed.

Specific Transaction terms include, for example, such words as “No Refunds,” “Exchange Only,” “In-Store Credit Only,” or “Original Packaging Required for Returns.” Specific terms may address such matters as late delivery, delivery charges, or insurance charges.

The specific terms printed on the Transaction receipt offered to the Cardholder will govern in the event of a dispute, subject to compliance with other Standards.

5.3.4 معاملات متعددة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب تضمين جميع المنتجات والخدمات المشتراة في معاملة واحدة، في مبلغ إجمالي واحد، في إيصال معاملة واحد، وأن تنعكس في سجل معاملة واحد، مع الاستثناءات التالية:

- يُسمح للتاجر بقبول أكثر من طريقة دفع لعملية شراء واحدة، بشرط أن يعكس سجل المعاملة والإيصال فقط الجزء من الشراء الذي يتعين دفعه عن طريق حساب.
- يُسمح للتاجر بإكمال عملية شراء العميل لمنتجات أو خدمات متعددة عن طريق فوترة المنتجات أو الخدمات، بشكل فردي في معاملات منفصلة لنفس الحساب، وفقًا لإجراءات القبول.

6.3.4 السداد الجزئي

(الفئة ب حسب المراجع المحددة في الفصل 1)

يُحظر على التاجر إجراء معاملة حينما يتم تضمين جزء فقط من إجمالي مبلغ الشراء في سجل المعاملة والإيصال، باستثناء الحالات التالية:

- عندما يدفع العميل جزءًا من إجمالي مبلغ الشراء عن طريق الحساب، ويدفع الرصيد المتبقي بطريقة دفع أخرى، مثل نقدًا أو عن طريق الصك.
- عندما يتم تسليم المنتجات أو الخدمات أو تنفيذها بعد تاريخ المعاملة، ويعتبر إيصال المعاملة الواحدة وديعة، ويعتبر إيصال المعاملة الثاني سداد الرصيد. ويجب على التاجر ملاحظة الكلمات “إيداع” و “رصيد” في إيصالات المعاملة حسب الاقتضاء. وإيصال المعاملة الثاني مشروط بتسليم أو أداء المنتجات أو الخدمات، ويجب عدم تقديمها إلا بعد تسليم المنتجات أو الخدمات أو تنفيذها.
- إذا وافق حامل البطاقة كتابيًا على دفع الفواتير من قبل التاجر على أقساط، وحدد جدول سداد الأقساط و/أو كل مبلغ قسط يتم دفعه إلى الحساب.

7.3.4 الشروط المحددة للمعاملة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجوز للتاجر فرض شروط محددة تحكم المعاملة، على سبيل المثال:

1. طباعة واضحة للشروط المحددة على إيصال المعاملة.
2. الكشف عن المصطلحات المحددة بوسائل أخرى، مثل اللافتات أو الأدبيات، بشرط أن يكون الكشف بارزًا وواضحًا بدرجة كافية؛ بحيث يكون الشخص العادي على دراية بالإفصاح ويفهمه قبل إتمام المعاملة.

وقد تتضمن شروط المعاملة المحددة، على سبيل المثال، كلمات مثل “لا توجد عمليات استرداد أموال” أو “استبدال فقط” أو “رصيد في المتجر فقط” أو “تعبئة أصلية مطلوبة للإرجاع”. وقد تتناول الشروط المحددة مسائل مثل التسليم المتأخر أو رسوم التسليم أو رسوم التأمين.

وتحكم الشروط المحددة المطبوعة على إيصال المعاملة المقدم لحامل البطاقة في حالة حدوث نزاع، مع مراعاة الامتثال للمعايير الأخرى.

4.3.8 Floor Limit

(Category B as per references set in chapter 1)

The floor limit for all transactions is zero.

A Merchant or Acquirer that does not obtain an authorization from the Issuer for any Transaction shall have financial responsibility in case of a resulting authorization-related dispute of the Transaction.

4.3.9 Returned Products and Canceled Services

(Category B as per references set in chapter 1)

A Merchant is required to accept the return of products or the cancellation of services unless specific disclosure was provided at the time of the Transaction.

Upon the return in full or in part of products or the cancellation of a service purchased with a Card, or if the Merchant agrees to a price adjustment on a purchase made with a Card, the Merchant must not provide a price adjustment by any means other than a credit to the same Card Account used to make the purchase (or a Card reissued by the same Issuer to the same Cardholder).

In a Card-present environment, the Merchant should ask the Cardholder for a Transaction receipt identifying (by means of a truncated PAN) the payment card used for the original purchase Transaction. If an Access Device was used, the PAN on a Card linked to the same Account might not match the PAN on the receipt. If the Card used to make the purchase is no longer available, the Merchant must act in accordance with its policy for adjustments, refunds, returns or the like.

4.3.10 Refund Transactions

(Category B as per references set in chapter 1)

A Merchant must process a refund Transaction only for the purpose of crediting funds to a Cardholder for returned products, cancelled services, or a price adjustment related to a prior purchase. The refund Transaction must not exceed the authorized amount of the related purchase POS Transaction.

If the original POS Transaction was a Card-not-present Transaction, then the presentation of a Card is not required for the refund Transaction. The proportional interchange fee associated with the original POS Transaction is reversed in the refund Transaction.

4.3.11 Transaction Records

(Category A as per references set in chapter 1)

Each Transaction record must reflect a valid and accurate Transaction date. A Merchant must provide all products and services included in a Transaction record to the Cardholder at the time of the Transaction unless, prior to completion of the Transaction, the Cardholder agrees to a delayed delivery of products or performance of services.

The following applies with respect to POS Transactions:

1. The Merchant must submit each Transaction record to its Acquirer no later than three business days after the Transaction date.
2. As an exception to the foregoing, a Merchant with multiple locations that uses a central facility to accumulate Transaction records completed with manually recorded (imprinted or handwritten) Card data must submit such Transaction records to its Acquirer within 7 calendar days of the Transaction date.

8.3.4. الحد الأدنى

(الفئة ب حسب المراجع المحددة في الفصل 1)

الحد الأدنى لجميع المعاملات هو صفر.

يتحمل التاجر أو جهة القبول التي لم تحصل على تفويض من جهة الإصدار للقيام بالمعاملة، مسؤولية مالية في حالة نشوء نزاع متعلق بالترخيص للمعاملة.

9.3.4. المنتجات المرتجعة، والخدمات الملغاة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يُطلب من التاجر قبول المنتجات المرتجعة أو الخدمات الملغاة، ما لم يتم تقديم إفصاح محدد في وقت المعاملة.

عند إعادة المنتجات كلها أو جزء منها، أو إلغاء خدمة تم شراؤها ببطاقة، أو إذا وافق التاجر على تعديل السعر على عملية شراء تم إجراؤها باستخدام بطاقة، يجب على التاجر ألا يقدم تعديلًا للسعر بأي وسيلة أخرى غير الإئتمان إلى نفس حساب البطاقة المستخدم في الشراء (أو بطاقة أعادت إصدارها نفس جهة الإصدار إلى نفس حامل البطاقة).

في حالة البطاقة الموجودة، يجب على التاجر أن يطلب من حامل البطاقة إيصال معاملة يحدد (عن طريق رقم حساب أساسي مقطوع) بطاقة الدفع المستخدمة لمعاملة الشراء الأصلية. وإذا تم استخدام جهاز وصول، فقد لا يتطابق رقم الحساب الأساسي الموجود على البطاقة المرتبطة مع الحساب نفسه مع رقم الحساب الأساسي الموجود في الإيصال. وإذا لم تعد البطاقة المستخدمة في الشراء متاحة، يجب على التاجر التصرف وفقًا لسياسته الخاصة بالتعديلات أو المبالغ المستردة أو العوائد أو ما شابه ذلك.

10.3.4. معاملات الاسترداد

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب على التاجر معالجة معاملة استرداد فقط لغرض إيداع الأموال لحامل البطاقة مقابل المنتجات المعادة أو الخدمات الملغاة أو تعديل السعر المتعلق بعملية شراء سابقة. ويجب ألا تتجاوز معاملة الاسترداد المبلغ المصرح به لمعاملة نقاط البيع ذات الصلة بالشراء.

إذا كانت معاملة نقاط البيع الأصلية، معاملة البطاقة غير الموجودة، فلن يكون تقديم البطاقة مطلوبًا لمعاملة الاسترداد. وتتم المعالجة عن طريق عكس رسوم التبادل النسبي المرتبطة بمعاملة نقاط البيع الأصلية في معاملة الاسترداد.

11.3.4. سجلات المعاملات

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب أن يعكس كل سجل معاملة، تاريخ معاملة صالحًا ودقيقًا. ويجب على التاجر تقديم جميع المنتجات والخدمات المدرجة في سجل المعاملة إلى حامل البطاقة في وقت المعاملة ما لم يوافق حامل البطاقة، قبل إتمام المعاملة، على تأخير تسليم المنتجات أو أداء الخدمات.

ينطبق ما يلي فيما يتعلق بمعاملات نقاط البيع:

1. يجب على التاجر تقديم كل سجل معاملة إلى جهة القبول في موعد لا يتجاوز ثلاثة أيام عمل بعد تاريخ المعاملة.
2. كاستثناء لما سبق، يجب على التاجر الذي لديه مواقع متعددة، أن يستخدم سجلًا مركزيًا لتجميع سجلات المعاملات المكتملة ببيانات البطاقة المسجلة يدويًا (المطبوعة أو المكتوبة بخط اليد) وأن يقدم سجلات المعاملات هذه إلى الجهة القابلة خلال 7 أيام تقويمية من تاريخ المعاملة.

3. Upon providing a full or partial refund for returned products or cancelled services, the Merchant must submit the refund Transaction record to its Acquirer within 15 days of the refund Transaction receipt date, in order to avoid a chargeback.

4.4 Card Present Environment

4.4.1 Chip Card Acceptance – General Requirements

In a Chip Transaction, the Terminal reads the chip through the contact interface.

A Chip Transaction occurs at a Hybrid Terminal with PIN acceptance capability for a PIN-preferring card.

The National Scheme Operator recommends that Issuers mandate online PIN for all purchase Transactions.

The National Scheme Operator also recommends that Acquirers should urge Merchants to ask Cardholders to provide online PIN as the CVM when carrying out a Transaction.

If an Issuer permits PIN bypass, then the issuer will hold liability for any resulting Transaction that is disputed as fraudulent. (Refer to chargeback rules.)

If an Issuer approves a technical fallback Transactions, then the Issuer will hold liability for any resulting Transaction that is disputed as fraudulent. (Refer to chargeback rules.)

A Hybrid Terminal is a Terminal that supports both Chip Card and magnetic stripe Card acceptance. Technical fallback occurs when the chip on the Card fails to authenticate and the Merchant then processes the Transaction using the magnetic stripe.

Chip Authorization

(Category B as per references set in chapter 1)

Online authorization from the Issuer must be obtained for a Chip Transaction.

4.4.2 Contactless Chip Transaction

In a Contactless Transaction, the Terminal reads the chip through the contactless interface.

The contactless mark must be displayed on a contactless-enabled Terminal.

For a contactless Purchase Transaction that exceeds LYD XX, online PIN is mandatory.

A Contactless purchase Transaction is permitted to be processed with no CVM when the Transaction amount is less than or equal to XX LYD (Tap & Go).

A daily transaction limit for contactless transactions with no PIN can be set later on

There is no maximum Transaction amount for a contactless Transaction.

4.4.3 Magnetic Stripe Transaction

A magnetic stripe Transaction may be completed at a Terminal that is magnetic-stripe-capable only with either a Chip Card or a magnetic stripe Card, or at a Hybrid Terminal if the Card is magnetic stripe only. Regarding liability for such Transactions, refer to the chargeback rules.

3. عند تقديم استرداد كامل أو جزئي للقيمة مقابل المنتجات المعادة أو الخدمات الملغاة ، يجب على التاجر إرسال سجل معاملة الاسترداد إلى جهة القبول خلال 15 يومًا من تاريخ استلام معاملة الاسترداد، وذلك لتجنب تحمل التكاليف.

4.4. حالة البطاقة الموجودة

1.4.4. قبول بطاقة الشريحة - المتطلبات العامة

في معاملة الشريحة، يقرأ الجهاز الشريحة من خلال واجهة الاتصال.

تحدث معاملة الشريحة في محطة هجينة مع إمكانية قبول رقم التعريف الشخصي لبطاقة تفضيل رقم التعريف الشخصي.

يوصي مشغل شبكة الدفع المحلية بأن تطلب جهات الإصدار رقم تعريف شخصي عبر الإنترنت لجميع معاملات الشراء.

يوصي مشغل شبكة الدفع المحلية أيضًا بأن تحت جهات القبول التجار على مطالبة حاملي البطاقات بتقديم رقم تعريف شخصي عبر الإنترنت باعتباره رمز التحقق من البطاقة عند تنفيذ أي معاملة.

وإذا سمحت جهات الإصدار بتجاوز رقم التعريف الشخصي، فإنها تتحمل المسؤولية عن المعاملات الاحتيالية. (راجع قواعد رد المبالغ المدفوعة).

وإذا وافقت جهة الإصدار على المعاملات الفنية الاحتيالية، فإنها تتحمل المسؤولية عن المعاملات الاحتيالية. (راجع قواعد رد المبالغ المدفوعة).

المحطة الهجينة هي محطة تدعم قبول كل من بطاقة الشريحة، وبطاقة الشريط المغناطيسي. وعندما يحدث الخطأ التقني وتفشل الشريحة الموجودة على البطاقة في المصادقة، يقوم التاجر بعد ذلك بمعالجة المعاملة باستخدام الشريط المغناطيسي.

ترخيص الشريحة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب الحصول على التفويض عبر شبكة الإنترنت من جهة الإصدار لمعاملة الشريحة.

2.4.4 معاملة الشريحة غير المتصلة

في المعاملات غير المتصلة، تقرأ المحطة الشريحة من خلال واجهة عدم الاتصال.

يجب عرض علامة عدم الاتصال على المحطة المزودة بتقنية عدم الاتصال.

بالنسبة لمعاملة الشراء غير المتصلة التي تتجاوز XX دينار ليبي، فإن رقم التعريف الشخصي عبر الإنترنت هو رقم إلزامي.

يُسمح بمعالجة معاملة الشراء غير المتصلة بدون CVM عندما يكون مبلغ المعاملة أقل من أو يساوي XX دينار ليبي (Tap & Go).

يمكن تعيين حد للمعاملات اليومية غير المتصلة بدون رقم تعريف شخصي في وقت لاحق،

ولا يوجد حد أقصى لمبلغ المعاملة للمعاملة غير المتصلة.

3.4.4 معاملة الشريط المغناطيسي

يمكن إتمام معاملة الشريط المغناطيسي في محطة قادرة على قراءة الشريط المغناطيسي فقط، إما ببطاقة شريحة أو بطاقة شريط مغناطيسي، أو في محطة هجينة إذا كانت البطاقة عبارة عن شريط مغناطيسي فقط. وفيما يتعلق بالمسؤولية عن مثل هذه المعاملات، (ارجع إلى قواعد رد المبالغ المدفوعة).

4.4.4 Merchant Procedures – Card-Present Transactions

(Category B as per references set in chapter 1)

The following steps are performed to determine the validity of a Card:

- Check for the presence of the NUMO brand on the Card.
- If the POS Terminal displays the PAN encoded on the magnetic stripe, then compare the last four digits of the PAN on the Card front with the four-digit truncated PAN displayed on the POS Terminal.

A Merchant is not required to accept a Card if neither the magnetic stripe nor the contact or contactless chip on the Card can be read for any reason.

The manual completion of a Transaction, whether by means of a manual imprinter, electronic key entry of the Card information, or both, does not provide sufficient proof of Card presence in a fraud-related dispute.

Suspicious Cards

When suspicious that a presented Card might not be valid, the Merchant or Acquirer accepting the Card should follow the pre-defined “suspicious Card” procedures.

4.4.5 Purchase with Cash Back Transactions

(Category B as per references set in chapter 1)

Purchase with cash back is an optional service that a Merchant may offer, subject to applicable law or regulation and with the prior approval of its Acquirer, at the Point of Interaction (POI) in a Card-present, face-to-face Transaction environment only.

The following requirements apply to purchase with cash back Transactions:

1. In a purchase with cash back Transaction, cash may only be provided in combination with a purchase. The cash back service must not be offered in combination with a Manual Cash Disbursement Transaction or the sale of a quasi-cash instrument.
2. An education program must be established for the staff of any Merchant that chooses to offer purchase with cash back Transactions, including but not limited to POS Terminal operators.
3. An offer of purchase with cash back that is promoted at the POI must be available to all Cardholders. The Merchant may prompt the Cardholder to use this service.
4. Acquirers or Merchants may establish a minimum and/or maximum cash back amount for the purchase with cash back Transaction, provided that:
 - a. Any minimum or maximum amount is applied uniformly to all Cardholders.
 - b. Any minimum amount is not greater than the minimum amount established for any other payment means accepted at the Merchant location.
 - c. Any maximum amount is not less than the maximum amounts established for any other payment means at the Merchant location.
 - d. The maximum cash back amount must be no more than LYD XXX per Transaction.
5. The Acquirer must obtain online authorization approval for the full Transaction amount including both the purchase amount and the cash-back amount; support for authorization of the purchase amount only is optional.

4.4.4. إجراءات التاجر - معاملات البطاقة الموجودة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يتم تنفيذ الخطوات التالية لتحديد صلاحية البطاقة:

- تحقق من وجود العلامة نمو التجارية على البطاقة.
- إذا كانت نقاط البيع تعرض رقم الحساب الأساسي المشفر على الشريط المغناطيسي، فتتم المقارنة بين الأرقام الأربعة الأخيرة من رقم الحساب الأساسي على مقدمة البطاقة، مع رقم الحساب الأساسي المقطع المكون من أربعة أرقام والمعروض على طرف نقاط البيع.

لا يُطلب من التاجر قبول البطاقة، إذا لم يكن من الممكن قراءة الشريط المغناطيسي أو جهة الاتصال أو الشريحة غير المتصلة على البطاقة لأي سبب من الأسباب.

لا يعد الإكتمال اليدوي للمعاملة، سواء عن طريق آلة الطباعة اليدوية أو إدخال مفتاح إلكتروني لمعلومات البطاقة، أو كليهما، دليلاً كافياً على وجود البطاقة في نزاع متعلق بشبهة الاحتيال.

بطاقات مشبوهة

عند الشك في أن البطاقة المقدمة قد لا تكون صالحة، يجب على التاجر أو القابل الذي يقبل البطاقة اتباع إجراءات “البطاقة المشبوهة” المحددة مسبقاً.

5.4.4. الشراء باستخدام طريقة معاملات الاسترداد النقدي

(الفئة ب حسب المراجع المحددة في الفصل 1)

الشراء باسترداد نقدي هو خدمة اختيارية قد يقدمها التاجر، وفقاً للقانون أو اللوائح المعمول بها وبموافقة مسبقة من جهة القبول، في نقطة التفاعل في حالة معاملات لبطاقة الموجودة وجهاً لوجه فقط.

تطبق القواعد التالية على الشراء باستخدام معاملات الاسترداد النقدي:

1. في عملية شراء، مع معاملة استرداد نقدي، لا يجوز تقديم النقد إلا مع عملية الشراء. ويجب عدم تقديم خدمة الاسترداد النقدي جنباً إلى جنب مع معاملة الصرف النقدي اليدوية، أو بيع أداة شبه نقدية.
2. يجب إنشاء برنامج تعليمي لموظفي التاجر الذي يختار عرض الشراء مع معاملات استرداد نقدي، بما في ذلك على سبيل المثال لا الحصر مشغلي نقاط البيع.
3. يجب أن يكون عرض الشراء مع الاسترداد النقدي الذي يتم الترويج له في نقطة التفاعل متاحاً لجميع حاملي البطاقات. يجوز للتاجر مطالبة حامل البطاقة باستخدام هذه الخدمة.
4. يجوز للجهات القابلة أو التجار تحديد حد أدنى أو أقصى لمبلغ استرداد نقدي لعملية الشراء باستخدام معاملة الاسترداد النقدي، وفق الشروط التالية:
 - أ. أن يتم تطبيق وتحديد مبلغ الحد الأدنى أو الأقصى بشكل موحد لجميع حاملي البطاقات.
 - ب. أن يكون المبلغ الأدنى لا يزيد عن الحد الأدنى للمبلغ المحدد لأي وسيلة دفع أخرى مقبولة في موقع التاجر.
 - ت. أن يكون مبلغ الحد الأقصى لا يقل عن الحد الأقصى للمبالغ المحددة لأي وسيلة دفع أخرى في موقع التاجر.
 - ث. يجب ألا يزيد الحد الأقصى لمبلغ الاسترداد النقدي عن XXX دينار ليبي لكل معاملة.
5. يجب أن تحصل جهة القبول على موافقة التفويض عبر الإنترنت لكامل مبلغ المعاملة، بما في ذلك مبلغ الشراء ومبلغ استرداد النقود؛ دعم التفويض بمبلغ الشراء هو اختياري فقط.

6. The authorization and clearing messages of each purchase with cash back Transaction must indicate the cash-back amount in the data field designated for this purpose.

4.5 Card-Not-Present Environment

(Category B as per references set in chapter 1)

The physical presentation of a Card or Access Device is not required and must not be requested to complete a Transaction conducted in a Card-not-present environment, including any e-commerce, (mail order & phone order subject to a prior specified approval), or Credential-on-file Transaction.

4.5.1 E-Commerce Transactions

(Category B as per references set in chapter 1)

An e-commerce Transaction occurs when a Cardholder uses his Card to pay for goods/ services from the Internet.

A Merchant must not refuse to complete an e-commerce Transaction solely because the Cardholder does not have a digital certificate or other secured protocol.

Card verification method for this type of Transaction would be Card number, Expiry date of card and CVV2.

If an additional cost is added to the final price, the Cardholder must be informed prior to processing the payment and consent to the additional charge (for example: delivery charges, additional taxes, insurance fees.....etc.)

Refund/Cancelation policy must be clearly displayed before processing the Transaction and the Cardholder's acknowledgement of it must be obtained.

The PAN must be truncated upon entry, last 4 digits only may be displayed.

An e-commerce Transaction requires authorization by the Issuer.

An e-commerce Transaction must not be affected using contactless payment functionality or as a purchase with cash back Transaction.

The Merchant must display the Logo on its website where payment methods are listed.

The Merchant must provide a mailing address and a contact telephone number or email address for customer queries. This information shall be displayed on any page within the Merchant's website, but must be readily accessible to a Cardholder, and remain displayed for at least 90 calendar days after the last day on which a Transaction was performed.

The Merchant must clearly display price information, including currency, and the details of the timing of billing and fulfillment of Transactions, and provide a function for Cardholders to confirm a purchase before the completion of the sale.

The Transaction amount used in the authorization message must match the value of the products and services in an individual shipment, including any additional charges for packing and shipment, etc.

6. يجب أن تشير رسائل التفويض والمقاصة لكل عملية شراء مع معاملة استرداد نقدي إلى مبلغ الاسترداد النقدي في حقل البيانات المخصص لهذا الغرض.

5.4. حالة البطاقة غير الموجودة

(الفئة ب حسب المراجع المحددة في الفصل 1)

التقديم المادي للبطاقة أو جهاز الوصول غير مطلوب، ولا يجب أن يُطلب لإكمال معاملة تم إجراؤها في حالة البطاقة غير الموجودة، بما في ذلك معاملات التجارة الإلكترونية (طلب عبر البريد وطلب عبر الهاتف يخضع لموافقة محددة مسبقًا) ، أو معاملة بيانات الاعتماد في الملف.

1.5.4. معاملات التجارة الإلكترونية

(الفئة ب حسب المراجع المحددة في الفصل 1)

تحدث معاملة التجارة الإلكترونية عندما يستخدم حامل البطاقة بطاقته لدفع ثمن البضائع، والخدمات عن طريق الإنترنت.

يجب ألا يرفض التاجر إتمام معاملة تجارة إلكترونية فقط، لأن حامل البطاقة ليس لديه شهادة رقمية أو بروتوكول آمن آخر.

تكون طريقة التحقق من البطاقة لهذا النوع من المعاملات، هي رقم البطاقة، وتاريخ انتهاء صلاحية البطاقة و CVV2.

وفي حالة إضافة تكلفة إضافية إلى السعر النهائي، يجب إبلاغ حامل البطاقة قبل معالجة الدفع والموافقة على الرسوم الإضافية (على سبيل المثال: رسوم التوصيل والضرائب الإضافية ورسوم التأمين... إلخ).

يجب على التاجر عرض سياسة الاسترداد والإلغاء بوضوح قبل معالجة المعاملة، ويجب الحصول على إقرار حامل البطاقة بها.

يجب على التاجر اقتطاع رقم الحساب الأساسي عند الإدخال، وقد يتم عرض آخر 4 أرقام فقط.

تتطلب معاملة التجارة الإلكترونية الحصول على تفويض من جهة الإصدار.

يجب ألا تتأثر معاملة التجارة الإلكترونية باستخدام وظيفة الدفع بدون الاتصال، أو كشراء بمعاملة استرداد نقدي.

يجب على التاجر عرض العلامة على موقعه على الإنترنت حيث يتم سرد طرق الدفع.

يجب على التاجر تقديم عنوان بريدي، ورقم هاتف للاتصال، أو عنوان بريد إلكتروني لاستفسارات العملاء. ويجب عليه، عرض هذه المعلومات على أي صفحة داخل موقع التاجر على الويب، ولكن يجب أن تكون متاحة بسهولة لحامل البطاقة، وتظل معروضة لمدة 90 يومًا تقويميًا على الأقل بعد آخر يوم تم فيه إجراء المعاملة.

يجب على التاجر عرض معلومات الأسعار بوضوح، بما في ذلك عملة الدفع، وتفاصيل توقيت الفواتير وتنفيذ المعاملات، وتوفير وظيفة لحاملي البطاقات لتأكيد الشراء قبل إتمام البيع.

يجب أن يتطابق مبلغ المعاملة المستخدمة في رسالة التفويض مع قيمة المنتجات والخدمات في الشحنة الفردية، بما في ذلك رسوم إضافية للتعبئة والشحن، إلخ.

If the purchase will be delivered in multiple shipments, the Merchant must notify the Cardholder and ensure that the combined amount of all shipments does not exceed the total purchase amount agreed with the Cardholder. The Merchant must obtain the Cardholder's agreement to any increase in the purchase amount as a result of multiple or partial deliveries. Each shipment, and any increase to the original agreed purchase amount, must be processed by the Merchant as a separate authorized Transaction.

If the products or services purchased are not available at time of the Transaction, the Merchant must inform the Cardholder and obtain the Cardholder's agreement to a delayed delivery (specifying the anticipated delivery date) before proceeding with the Transaction.

The Merchant must advise the Cardholder if the products or services ordered will not be delivered within the time frame originally disclosed to and agreed with the Cardholder. The Cardholder must be notified of the new anticipated delivery timeframe and given an opportunity to cancel the Transaction. The information provided on any email acknowledgment of the Cardholder's order must comply with the Transaction receipt requirements described in this chapter.

4.5.1.1 Specific Terms of an E-commerce Transaction

(Category B as per references set in chapter 1)

In an e-commerce Transaction:

1. A Cardholder accepts specific Transaction terms by electronic means (for example, by checking a box or clicking a "Submit" button indicating the acceptance of terms and conditions); and
2. A Merchant must clearly communicate, and the Cardholder must specifically accept, any terms concerning a recurring payment Transaction arrangement separately from any other terms (for example, by checking a box or clicking a "Submit" button indicating the acceptance of recurring payment terms and conditions).

The specific Transaction terms will govern in the event of a dispute, subject to compliance with other Standards, provided that such specific terms were disclosed to and accepted by the Cardholder before completion of the Transaction.

4.5.1.2 3D-Secure Participation Requirements

Participation in 3-D Secure for e-commerce Transactions is a mandate.

4.5.1.3 3D-Secure Participation Non-Compliance Penalties

(Category A as per references set in chapter 1)

The National Scheme Operator has the right to fine Members that do not support 3D Secure.

4.5.2 Key-Entered Transactions

(Category B as per references set in chapter 1)

A key-entered Transaction in a non-face-to-face environment takes place when the Cardholder authorizes the Merchant to use his Card data (PAN and expiry date) while the Cardholder and Card are not at the Merchant premises.

As of today, Key Entered transactions are not permitted by the National Scheme Operator.

وإذا تم تسليم المشتريات في عدة شحنات، يجب على التاجر إخطار حامل البطاقة والتحقق من أن المبلغ الإجمالي لجميع الشحنات لا يتجاوز إجمالي مبلغ الشراء المتفق عليه مع حامل البطاقة. ويجب أن يحصل التاجر على موافقة حامل البطاقة على الزيادة في مبلغ الشراء نتيجة لعمليات التسليم المتعددة أو الجزئية. ويجب أن تتم معالجة كل شحنة وأي زيادة على مبلغ الشراء الأصلي المتفق عليه بواسطة التاجر كمعاملة منفصلة معتمدة.

وإذا كانت المنتجات أو الخدمات المشتراة غير متوفرة في وقت المعاملة، يجب على التاجر إبلاغ حامل البطاقة والحصول على موافقته على التسليم المتأخر (تحديد تاريخ التسليم المتوقع) قبل متابعة المعاملة.

يجب على التاجر إبلاغ حامل البطاقة إذا كانت المنتجات أو الخدمات المطلوبة لن يتم تسليمها خلال المواعيد المحددة التي تم الإفصاح عنها في الأصل والموافقة عليه مع حامل البطاقة. يجب إخطار حامل البطاقة بالمواعيد الجديدة المتوقعة للتسليم ومنحه فرصة لإلغاء المعاملة. يجب أن تتوافق المعلومات المقدمة في الإقرار بالبريد الإلكتروني لطلب حامل البطاقة، مع متطلبات استلام المعاملة الموضحة في هذا الفصل.

1.1.5.4 الشروط المحددة لمعاملة التجارة الإلكترونية

(الفئة ب حسب المراجع المحددة في الفصل 1)

في معاملة التجارة الإلكترونية:

1. يقبل حامل البطاقة شروط معاملة محددة بالوسائل الإلكترونية (على سبيل المثال، عن طريق تحديد صندوق، أو النقر فوق الزر "إرسال" للإشارة إلى قبول البنود والشروط).
2. يجب على التاجر التواصل بوضوح، ويجب على حامل البطاقة قبول الشروط التي تتعلق بترتيب معاملة الدفع المتكررة بشكل منفصل عن الشروط الأخرى (على سبيل المثال، عن طريق تحديد صندوق أو النقر فوق الزر "إرسال" للإشارة إلى قبول شروط الدفع المتكررة والشروط). ستحكم شروط المعاملة المحددة في حالة حدوث نزاع، وتخضع للامتنال مع معايير أخرى، شريطة أن يتم الإفصاح عن هذه الشروط المحددة، وقبولها من قبل حامل البطاقة قبل إتمام المعاملة.

2.1.5.4 متطلبات المشاركة الآمنة ثلاثية الأبعاد

تعد المشاركة الآمنة ثلاثية الأبعاد لمعاملات التجارة الإلكترونية بمثابة تفويض.

3.1.5.4 عقوبات عدم الامتنال للمشاركة الآمنة ثلاثية الأبعاد

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجوز لمشغل شبكة الدفع المحلية فرض غرامة نقدية على الأعضاء الذين لا يدعمون المشاركة الآمنة ثلاثية الأبعاد.

2.5.4 المعاملات المدخلة بالمفتاح

(الفئة ب حسب المراجع المحددة في الفصل 1)

تحدث المعاملة التي يتم إدخالها بالمفتاح في غير حالة الوجه لوجه، عندما يرخّص حامل البطاقة للتاجر باستخدام بيانات بطاقته (رقم الحساب الأساسي وتاريخ انتهاء الصلاحية) بينما لا يكون حامل البطاقة والبطاقة موجودون في مقر التاجر.

اعتبارًا من اليوم، لا يسمح مشغل شبكة الدفع المحلية بالمعاملات التي يتم إدخالها بالمفتاح.

4.5.3 Mail Order and Telephone Order (MO/TO) Transactions

(Category B as per references set in chapter 1)

As of today, Mail Order / Telephone Order transactions are not permitted by the National Scheme Operator.

4.5.4 Credential-On-File Transactions

(Category B as per references set in chapter 1)

A Credential-on-file Transaction occurs when a Cardholder expressly authorizes a Merchant to store the Cardholder's Account data (meaning PAN and expiration date) for subsequent use in connection with one or more later Transaction(s) with that Merchant and subsequently authorizes that Merchant to use the stored Account data in one or more Transaction(s).

Merchants running such service must be PCI-DSS certified.

The Acquirer should ensure that the Merchant retains the Cardholder's written agreement to the terms of a Credential-on-file Transaction arrangement.

A recurring payment is a type of Credential-on-file Transaction.

4.5.5 Recurring Payment Transactions

(Category B as per references set in chapter 1)

A recurring Transaction occurs when a Cardholder authorizes a Merchant to use his Card data periodically to debit an agreed amount on an ongoing basis.

A recurring Transaction agreement has no end date.

Recurring payment Transactions may occur periodically, such as on a monthly, quarterly, or annual basis, or as needed to "top up" the Cardholder's account with the Merchant.

A recurring payment Transaction may be for a variable or a fixed amount, as specified in the agreement.

A recurring payment Transaction differs from an installment Transaction in that the number of installment Transaction payments is specified.

The Merchant should keep all related documents proving the Cardholder's authorization for recurring transaction to be debited on his card.

The word "Recurring" or similar must be stated clearly in the documents that the Cardholder signed, or in the related correspondences, in addition to Cardholder consent to all terms.

If the Merchant receives cancelation notification from the Cardholder to the recurring Transaction, the Merchant should stop providing service/sending product related to the canceled Transaction.

This type of transaction could, by way of example and not limitation, be for:

- Cable Network
- Software Providers
- Telecommunication Services

Merchants running such service must be PCI-DSS certified.

4.6 Specific Transaction Types

4.6.1 T&E Charges

T&E charges are submitted by Merchants in the hotel, car rental, airline, cruise line and restaurant sectors.

3.5.4 معاملات الطلبات عبر البريد والطلبات عبر الهاتف

(الفئة ب حسب المراجع المحددة في الفصل 1)

اعتبارًا من اليوم، لا يسمح مشغل شبكة الدفع المحلية بمعاملات الطلب عبر البريد، والطلب عبر الهاتف.

4.5.4 معاملات الاعتماد في الملف

(الفئة ب حسب المراجع المحددة في الفصل 1)

تحدث معاملة بيانات الاعتماد في الملف عندما يرخّص حامل البطاقة صراحةً للتاجر بتخزين بيانات حساب حامل البطاقة (بمعنى رقم حساب أساسي وتاريخ انتهاء الصلاحية) للاستخدام اللاحق، فيما يتعلق بواحدة أو أكثر من المعاملات اللاحقة مع ذلك التاجر ويرخص ذلك التاجر لاحقًا باستخدام بيانات الحساب المخزنة في معاملة واحدة أو أكثر.

يجب أن يكون التجار الذين يقومون بتشغيل هذه الخدمة حاصلين على شهادة PCI-DSS.

يجب على جهة القبول التحقق من احتفاظ التاجر بموافقة حامل البطاقة المكتوبة على شروط ترتيب معاملة بيانات الاعتماد في الملف.

الدفع المتكرر هو نوع من معاملات الاعتماد في الملف.

5.5.4 معاملات الدفع المتكررة

(الفئة ب حسب المراجع المحددة في الفصل 1)

تحدث المعاملة المتكررة، عندما يرخّص حامل البطاقة للتاجر باستخدام بيانات بطاقته بشكل دوري لسحب المبلغ المتفق عليه بشكل مستمر.

عقد المعاملة المتكررة هو عقد غير محدد المدة.

قد تحدث معاملات الدفع المتكررة بشكل دوري، على سبيل المثال على أساس شهري، أو ربع سنوي، أو سنوي، أو حسب الحاجة "لتعبئة" حساب حامل البطاقة لدى التاجر.

قد تكون معاملة الدفع المتكررة بمبلغ متغير أو بمبلغ ثابت، كما هو محدد في العقد.

تختلف معاملة الدفع المتكرر، عن معاملة الأقساط في تحديد عدد مدفوعات معاملات الأقساط.

يجب على التاجر الاحتفاظ بجميع المستندات التي تثبت ترخيص حامل البطاقة للمعاملة المتكررة ليتم خصمها من بطاقته.

يجب ذكر كلمة "متكرر" أو ما شابه ذلك بوضوح في المستندات التي وقعها حامل البطاقة، أو في المراسلات ذات الصلة، بالإضافة إلى موافقة حامل البطاقة على جميع الشروط.

إذا تلقى التاجر إشعارًا بالإلغاء من حامل البطاقة للمعاملة المتكررة، يجب على التاجر التوقف عن تقديم الخدمة، وإرسال المنتج المتعلق بالمعاملة الملغاة.

يمكن أن يكون هذا النوع من المعاملات، على سبيل المثال، من أجل:

- شبكة الكابل.
- مقدمو البرمجيات.
- خدمات الاتصالات.

يجب أن يكون التجار الذين يقومون بتشغيل هذه الخدمة حاصلين على شهادة PCI-DSS.

6.4 أنواع المعاملات المحددة

1.6.4 رسوم السفر والترفيه

يتم تحديد رسوم السفر والترفيه من قبل التجار في قطاعات الفنادق، وتأجير السيارات وخطوط الطيران وخط الرحلات البحرية والمطاعم.

4.6.2 General T&E

(Category A as per references set in chapter 1)

As the final Transaction amount is often unknown at the time of authorization, T&E Merchants are permitted to request a preauthorization for an estimated Transaction amount, and may submit subsequent authorization requests for any additional estimated amounts as needed. If the Issuer declines an initial or subsequent authorization request, the Acquirer must not submit the corresponding clearing message.

The Transaction amount must not exceed the authorized amount.

4.6.3 T&E Authorizations – Exemptions

(Category A as per references set in chapter 1)

Authorization is required for all T&E Transactions, without exception.

4.6.4 Car Rental Merchants

(Category B as per references set in chapter 1)

Car rental Merchants must not include any charge in a Transaction that represents either the vehicle insurance deductible amount or an amount to cover potential or actual damages when the Cardholder waives insurance coverage at the time of the rental.

Before the Cardholder enters into a rental agreement, the Merchant must disclose to the Cardholder the amount of the preauthorization request to be sent to the Issuer.

Charges for loss, theft, or damage must be processed separately as set out below.

4.6.5 Charges for Loss, Theft, or Damage

(Category B as per references set in chapter 1)

A charge for loss, theft, or damage must be processed as a separate Transaction from the underlying rental, lodging, or other Transaction.

The Merchant must provide a reason for the charge and a reasonable estimate of the cost of repairs to the Cardholder. After gaining the Cardholder's authorization of the charge and the estimated cost, the Merchant must process the Transaction as one of the following:

- A Card-present Transaction with CVM
- A fully authenticated e-commerce Transaction

The Transaction receipt must include a statement indicating that the estimated amount charged for repairs will be adjusted upon completion of the repairs and submission of the invoice for such repairs.

The final amount of a Transaction relating to repairs must not exceed the Merchant's estimated amount. If the Merchant obtains a preauthorization for an estimated amount, and the Transaction amount exceeds the authorized amount, the Merchant is permitted to request an additional authorization. In connection with such Transactions, the Issuer must not place a hold on the Cardholder's Account in excess of the authorized amount.

4.6.6 Delayed or Amended Charges

(Category B as per references set in chapter 1)

A T&E Merchant is permitted to submit delayed or amended charges, such as traffic violations and mini-bar charges, in accordance with the terms and conditions agreed to by the Cardholder. Authorization is required for such charges.

2.6.4 السفر والترفيه العام

(الفئة أ حسب المراجع المحددة في الفصل 1)

نظرًا لأن مبلغ المعاملة النهائية غالبًا ما يكون غير معروف في وقت التفويض، لذا يُسمح لتجار السفر والترفيه بطلب تفويض مسبق لمبلغ المعاملة المقدّر، ويمكنهم تقديم طلبات تفويض لاحقة لأي مبالغ تقديرية إضافية حسب الحاجة. وإذا رفضت جهة الإصدار طلب تفويض أولي أو لاحق، يجب على جهة القبول عدم إرسال رسالة المقاصة المقابلة. يجب ألا يتجاوز مبلغ المعاملة المبلغ المصرح به.

3.6.4 تفويضات السفر والترفيه – الإعفاءات

(الفئة أ حسب المراجع المحددة في الفصل 1)

التفويض مطلوب لجميع معاملات السفر والترفيه ، دون استثناء.

4.6.4.4 تجار تأجير السيارات

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب ألا يدرج تجار تأجير السيارات أي رسوم في معاملة تمثل إما مبلغ التأمين على السيارة القابل للخصم، أو مبلغًا لتغطية الأضرار المحتملة أو الفعلية عندما يتنازل حامل البطاقة عن التغطية التأمينية في وقت الإيجار.

قبل أن يبرم حامل البطاقة عقد الإيجار، يجب على التاجر الإفصاح لحامل البطاقة عن مبلغ طلب التفويض المسبق الذي سيتم إرساله إلى جهة الإصدار.

يجب معالجة رسوم الضياع أو السرقة أو التلف بشكل منفصل على النحو المبين أدناه.

5.6.4 رسوم الفقد أو السرقة أو التلف

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب معالجة رسوم الفقد أو السرقة أو التلف، كمعاملة منفصلة عن الإيجار الأساسي أو الإقامة أو أي معاملة أخرى.

يجب على التاجر تقديم سبب طلب الرسوم، وتقدير معقول لتكلفة الإصلاحات لحامل البطاقة. بعد الحصول على التفويض من حامل البطاقة بالرسوم والتكلفة المقدرة، يجب على التاجر معالجة المعاملة كواحد مما يلي:

- معاملة بالبطاقة الموجودة مع CVM.
- معاملة تجارة إلكترونية مصدق عليها بالكامل.

يجب أن يتضمن إيصال المعاملة بيانًا يشير إلى أنه؛ سيتم تعديل المبلغ المقدّر الذي يتم تحصيله مقابل الإصلاحات عند الانتهاء من الإصلاحات، وتقديم الفاتورة الخاصة بهذه الإصلاحات.

يجب ألا يتجاوز المبلغ النهائي للمعاملة المتعلقة بالإصلاحات المبلغ المقدّر من قبل التاجر. إذا حصل التاجر على تفويض مسبق لتقدير المبلغ، وتجاوز مبلغ المعاملة المبلغ المصرح به، فيُسمح للتاجر بطلب تفويض إضافي. فيما يتعلق بهذه المعاملات، ويجب على جهة الإصدار ألا تحتجز حساب حامل البطاقة بما يزيد عن المبلغ المصرح به.

6.6.4 الرسوم المتأخرة أو المعدلة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يُسمح لتاجر السفر والترفيه بتقديم رسوم متأخرة أو معدلة، مثل مخالفات المرور ورسوم الميني بار، وفقًا للشروط والأحكام التي وافق عليها حامل البطاقة . ويجب عليه التفويض بمثل هذه الرسوم.

4.6.7 Car Rental Advance Deposit

(Category B as per references set in chapter 1)

A car rental may be paid in advance, in full or in part, in accordance with the terms and conditions agreed to by the Cardholder. The advance payment must be authorized. The Transaction amount must not exceed the authorized amount.

4.6.8 Hotel Guaranteed Reservations

(Category B as per references set in chapter 1)

When a Cardholder guarantees the reservation with a Card, the Merchant ensures that a room will be available upon arrival of the Cardholder.

Hotel Merchants have the following responsibilities when accepting a Guaranteed Reservation:

- The Merchant must keep a room available until check-out time on the day following the reservation.
- When accepting the Card as a guarantee, the Merchant will provide the Cardholder with a confirmation number for the reservation.
- Merchants must accept a cancellation from the Cardholder when provided prior to the agreed upon time frame. Upon acceptance of the cancellation, the Merchant will provide a cancellation number.

Cardholders who cancel beyond the cancellation policy may be billed for one night of room and tax only.

No-Show transactions must be authorized prior to billing.

In the event the Merchant is unable to provide a room to a Cardholder who guaranteed the stay with a Card, the Merchant must do all of the following:

- Not bill the Cardholder a No-Show charge
- Ensure the Cardholder is not charged more than the rate of the guaranteed stay
- Receive complimentary transportation to the new location, and
- A complimentary call when necessary for the Cardholder to inform others of the new location.

Merchants billing No-Show transactions are advised to note that the Transaction was a No-Show in the event of a dispute.

Should a Cardholder dispute a No-Show charge for any reason other than as an unauthorized Transaction, the Merchant must support their cancellation policy and No-Show billing only with documentation verifying the Cardholder received the cancellation policy and failed to adhere to it.

4.6.9 Timeshare Merchants

(Category B as per references set in chapter 1)

MCC 7012 must be used to identify timeshare merchants.

Timeshare Merchants must grant the Cardholder a 15-day “cooling-off” period after signature to cancel the timeshare agreement.

4.6.10 Education Payments

(Category A as per references set in chapter 1)

Education payments must be identified with MCC 8220.

7.6.4. الإيداع المسبق لتأجير السيارات

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجوز دفع إيجار السيارة مقدّمًا، كليًا أو جزئيًا، وفقًا للشروط والأحكام المتفق عليها من قبل حامل البطاقة. ويجب الموافقة على الدفعة المقدمة. والتي يجب ألا تتجاوز مبلغ المعاملة المصرح به.

8.6.4. حجوزات فندقية مضمونة

(الفئة ب حسب المراجع المحددة في الفصل 1)

عندما يضمن حامل البطاقة الحجز ببطاقة، فإن التاجر يضمن توفر غرفة عند وصول حامل البطاقة.

يتحمل تجار الفنادق المسؤوليات التالية عند قبول حجز مضمون:

- يجب أن يحتفظ التاجر بالغرفة متاحة حتى موعد تسجيل المغادرة في اليوم التالي للحجز.
- عند قبول البطاقة كضمان، سيقدم التاجر لحامل البطاقة رقم تأكيد للحجز.
- يجب على التجار قبول الإلغاء من حامل البطاقة عند تقديمها قبل الموعد المتفق عليه. عند قبول الإلغاء، سيقدم التاجر رقم إلغاء.

قد تتم محاسبة حاملي البطاقات الذين يقومون بالإلغاء بعد سياسة الإلغاء مقابل ليلة واحدة من الغرفة والضريبة فقط.

يجب الموافقة على معاملات عدم الحضور قبل إصدار الفواتير.

في حالة عدم تمكن التاجر من توفير غرفة لحامل البطاقة الذي ضمن الإقامة ببطاقة، يجب على التاجر القيام بكل ما يلي:

- عدم إصدار فاتورة لحامل البطاقة مقابل رسوم عدم الحضور.
 - تأكد من عدم فرض رسوم على حامل البطاقة أكثر من سعر الإقامة المضمونة.
 - الحصول على مواصلات مجانية إلى الموقع الجديد.
 - مكاملة مجانية عند الضرورة لحامل البطاقة لإبلاغ الآخرين بالموقع الجديد.
- يُنصح التجار الذين يقومون بفوترة معاملات عدم الحضور، بملاحظة أن المعاملة كانت عدم الحضور، في حالة حدوث نزاع.

وفي حالة اعتراض حامل البطاقة على رسوم عدم الحضور لأي سبب، بخلاف المعاملة غير المصرح بها، يجب على التاجر دعم سياسة الإلغاء، وفواتير عدم الحضور فقط مع الوثائق التي تثبت أن حامل البطاقة قد تلقى سياسة الإلغاء وأخل بالالتزام بها.

9.6.4. تجار المشاركة بالوقت

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب استخدام MCC 7012 لتحديد التجار بنظام المشاركة بالوقت.

يجب أن يمنح التجار بالوقت، لحامل البطاقة فترة “مهلة” لمدة 15 يومًا بعد التوقيع لفسخ عقد المشاركة بالوقت.

10.6.4. مدفوعات التعليم

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب تحديد مدفوعات التعليم مع MCC 8220.

4.6.11 Tax and Other Government Payments

(Category A as per references set in chapter 1)

The same rules apply for the use of NUMO Cards for government payments as for other payments. Such payments may be Card-present or Card-not-present.

4.6.12 Government Payment Requirements

(Category A as per references set in chapter 1)

Government payments must be identified with a proper MCC, such as 9211, 9222, 9223, 9311 or 9399.

4.6.13 Unattended Fuel Dispensers and Other Unattended Terminals

NUMO Card acceptance is not currently supported at unattended fuel dispensers or other unattended Terminals.

Terminal Requirements

4.6.14 Terminal Eligibility

(Category A as per references set in chapter 1)

The following types of terminals, when compliant with the applicable technical requirements and other Standards, are eligible to be Terminals:

1. Any ATM or Bank Branch Terminal that is owned, operated or controlled by an Acquirer;
2. Any ATM that is owned, operated or controlled by an entity that is ineligible to be a Member, provided that such ATM is connected to the Interchange System by a Principal or Affiliate;
3. Any POS Terminal that is owned, operated or controlled by a Merchant, provided that such POS Terminal is connected to the Interchange System by a Principal Member; and
4. Any other type of terminal which the National Scheme Operator authorizes. A terminal that dispenses scrip is ineligible to be a Terminal.

4.6.15 Terminal Requirements

(Category A as per references set in chapter 1)

Each Terminal must:

1. Have an online connection to the Acquirer host system for the authorization of Transactions. If online PIN is a supported CVM, the Terminal must be able to encrypt PINs at the point of entry and send them to the Acquirer host system in encrypted form.
2. Accept any Card that conforms with the encoding Standards, including but not limited to the acceptance of all valid PAN lengths, major industry identifier numbers and BINs, effective and expiration dates, chip application effective dates, service code values, and characters encoded in the discretionary data.
3. Support all required Transaction types and valid Transactions in accordance with the Standards; and
4. Have a magnetic stripe reader capable of reading Track 2 data encoded on the magnetic stripe of a Card, and transmit all such data for authorization;
5. Not perform tests or edits on Track 1 data for the purpose of disqualifying Cards from eligibility for Interchange System processing;
6. For magnetic stripe Transactions, perform a check (either at the Terminal or in the Acquirer host system) of the track layout, limited to the start sentinel, separator, end

11.6.4. الضرائب والمدفوعات الحكومية الأخرى

(الفئة أ حسب المراجع المحددة في الفصل 1)

تنطبق ذات القواعد على استخدام بطاقات نمو للمدفوعات الحكومية، والمدفوعات الأخرى. وقد تكون هذه المدفوعات بالبطاقة الموجودة أو البطاقة غير الموجودة.

12.6.4. متطلبات الدفع الحكومية

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب تحديد المدفوعات الحكومية MCC مناسب ، مثل 9211 أو 9222 أو 9223 أو 9311 أو 9399.

13.6.4. محطات الوقود غير المراقبة، والمحطات الأخرى غير المراقبة

قبول بطاقة نمو غير مدعوم حاليًا في محطات توزيع الوقود غير المراقبة، أو المحطات الأخرى غير المراقبة.

متطلبات المحطة

14.6.4. جهوزية المحطة

(الفئة أ حسب المراجع المحددة في الفصل 1)

أن الأنواع التالية من المحطات، إذا حققت المتطلبات الفنية المعمول بها والمعايير الأخرى، فإنها تكون مؤهلة لتكون محطات:

1. أي جهاز صراف آلي أو فرع مصرف تمتلكه جهة القبول أو تديره أو تتحكم فيه.
2. أي جهاز صراف آلي مملوك أو مُشغل أو تتحكم فيه جهة غير مؤهلة ليكون عضوًا، بشرط أن يكون جهاز الصراف الآلي هذا متصلًا بنظام التبادل من قبل مالك أو شركة تابعة له.
3. أي جهاز نقاط بيع يملكه أو يديره أو يتحكم فيه التاجر، بشرط أن يكون جهاز نقاط البيع متصل بنظام التبادل من قبل عضو رئيسي.
4. أي نوع آخر من المحطات التي يصرح بها مشغل شبكة الدفع المحلية. المحطة التي توزع السكريب غير مؤهلة لتكون محطة.

15.6.4. متطلبات المحطة

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب على كل محطة أن تفي بالمتطلبات التالية:

1. أن يكون لديها اتصال عبر الإنترنت بنظام مضيف القابل من أجل تفويض المعاملات. وإذا كان رقم التعريف الشخصي على الإنترنت عبارة عن أداة CVM مدعومة، فيجب أن تكون المحطة قادرة على تشفير أرقام التعريف الشخصية عند نقطة الدخول، وإرسالها إلى نظام مضيف القابل بشكل مشفر.
2. أن تقوم بقبول البطاقات التي تتوافق مع معايير التشفير، بما في ذلك على سبيل المثال؛ قبول جميع أطوال أرقام الحسابات الأساسية الصالحة، وأرقام معرفات الصناعة الرئيسية، وأرقام التعريف المصرفية، وتواريخ مدة السريان، وانتهاء الصلاحية، وتواريخ سريان تطبيق الشريحة، وقيم رمز الخدمة، والأحرف المشفرة في البيانات التقديرية.
3. أن تقوم بدعم جميع أنواع المعاملات المطلوبة والمعاملات الصحيحة وفقًا للمعايير.
4. أن يكون لديها قارئ شريط مغناطيسي قادر على قراءة بيانات المسار 2 المشفرة على الشريط المغناطيسي للبطاقة، ونقل جميع هذه البيانات للحصول على تفويض.
5. أن تلتزم بعدم إجراء اختبارات أو تعديلات على بيانات المسار 1 لغرض استبعاد البطاقات من الأهلية لمعالجة نظام التبادل.
6. بالنسبة لمعاملات الشريط المغناطيسي، يتم بإجراء فحص (إما في المحطة أو في نظام مضيف القابل) لتخطيط المسار، مقصورًا على حارس البداية، والفصل، وحارس النهاية، وفحص التكرار

sentinel, and Longitudinal Redundancy Check (LRC), to ensure that the Card conforms to the technical specifications . If an LRC error occurs or the track data cannot be interpreted correctly or verified, the Transaction must not be processed or recorded; and

7. Prevent additional Transactions from being entered into the system while a Transaction is being processed.

A Cardholder-facing or unattended Terminal additionally must:

1. Ensure privacy of PIN entry to the Cardholder (where PIN processing is required and/or supported);
2. Provide Cardholder operating instructions in Arabic. Other languages may optionally be supported; and
3. Have a screen display that enables the Cardholder to view the data (other than the PIN), entered into the Terminal by that Cardholder, or the response received as the result of the Cardholder's Transaction request. This data will include the application labels or preferred names on a multi-application Card, and the amount of the Transaction and must be PCI certified.

4.6.16 Terminal Function Keys

The support of the following function keys on a Terminal that supports entry of a PIN is recommended:

1. A key used to restart the process of PIN entry or entry of the Transaction amount. The preferred color is yellow, and the preferred label is CORR or CANCEL.
2. A key used to complete the process of PIN entry or entry of the Transaction amount. The preferred color is green, and the preferred label is OK.
3. A key used to terminate a Transaction. The preferred color is red, and the preferred label is STOP or CANCEL. The key must allow the Cardholder to cancel a Transaction prior to the final step that results in the submission of an authorization request.

4.6.17 Terminal Responses

(Category B as per references set in chapter 1)

A Terminal must be able to display or print the response required in the applicable technical specifications. The Acquirer or Merchant must provide an appropriate message to the Cardholder whenever the attempted Transaction is rejected, either with a specific reason or by referring the Cardholder to the Issuer.

4.6.18 Terminal Transaction Log

(Category A as per references set in chapter 1)

The Acquirer must maintain a Terminal Transaction log. The log must include, at a minimum, the same information provided on the Cardholder receipt, including the Card sequence number, if present. The log must include the full PAN, unless otherwise supported by supplementary reported data, and must not include the PIN or any discretionary data from the Card's magnetic stripe or chip. Only the data necessary for research should be recorded. An Issuer is permitted to request a copy of this information.

The Terminal must not electronically record a Card's full magnetic stripe or chip data for the purpose of allowing or enabling subsequent authorization requests, after the initial authorization attempt.

الطولي، للتأكد من أن البطاقة مطابقة للمواصفات الفنية. وفي حالة حدوث خطأ في فحص التكرار الطولي، أو تعذر تفسير بيانات المسار بشكل صحيح أو التحقق منها، يجب ألا تتم معالجة المعاملة أو تسجيلها.

7. أن تمنع المعاملات الإضافية من الدخول في النظام أثناء معالجة المعاملة.

بالإضافة إلى ذلك، يجب على المحطة المواجهة لحامل البطاقة أو غير المراقبة:

1. ضمان خصوصية إدخال رقم التعريف الشخصي لحامل البطاقة (حيث تكون معالجة رقم التعريف الشخصي مطلوبة أو مدعومة).
2. توفير تعليمات التشغيل الخاصة بحامل البطاقة باللغة العربية. وقد يتم توفير لغات أخرى اختياريًا.

3. الحصول على شاشة عرض تمكّن حامل البطاقة من عرض البيانات (بخلاف رقم التعريف الشخصي)، التي أدخلها حامل البطاقة في المحطة، أو الاستجابة التي تم تلقيها كنتيجة لطلب المعاملة الخاص بحامل البطاقة. وتشمل هذه البيانات تطبيق الملصقات أو الأسماء المفضلة على بطاقة متعددة التطبيقات، ومبلغ المعاملة ويجب أن تكون معتمدة من PCI.

16.6.4. مفاتيح وظيفة المحطة

في المحطات التي تدعم إدخال رقم التعريف الشخصي، يوصى بدعم مفاتيح الوظائف التالية:

1. مفتاح يُستخدم لإعادة تشغيل عملية إدخال رقم التعريف الشخصي أو إدخال مبلغ المعاملة. اللون المفضل هو الأصفر، والتسمية المفضلة هي CORR أو CANCEL.
2. مفتاح يستخدم لإكمال عملية إدخال رقم التعريف الشخصي أو إدخال مبلغ المعاملة. اللون المفضل هو الأخضر، والتسمية المفضلة هي OK.
3. مفتاح يستخدم لإنهاء المعاملة. اللون المفضل هو الأحمر والملصق المفضل هو STOP أو CAN-CEL. ويجب أن يسمح المفتاح لحامل البطاقة بإلغاء المعاملة قبل الخطوة الأخيرة التي تؤدي إلى تقديم طلب التفويض.

17.6.4. استجابات المحطة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب أن تكون المحطة قادرة على عرض أو طباعة الاستجابة المطلوبة في المواصفات الفنية المعمول بها، ويجب على جهة القبول أو التاجر إرسال رسالة مناسبة إلى حامل البطاقة متى تم رفض محاولة إجراء المعاملة، إما لسبب محدد أو بإحالة حامل البطاقة إلى جهة الإصدار.

18.6.4. سجل معاملات المحطة

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب أن تحتفظ جهة القبول بسجل معاملات المحطة. ويجب أن يتضمن السجل، كحد أدنى، نفس المعلومات المقدمة في إيصال حامل البطاقة، بما في ذلك الرقم التسلسلي للبطاقة، إن وجد. ويجب أن يشتمل السجل على رقم حساب أساسي بالكامل، ما لم يتم دعمه بخلاف ذلك بواسطة البيانات الإضافية المبلغ عنها، ويجب ألا يتضمن رقم التعريف الشخصي أو أي بيانات تقديرية من الشريط المغناطيسي للبطاقة أو الشريحة. ويجب تسجيل البيانات اللازمة للبحث فقط. يُسمح لجهة الإصدار بطلب نسخة من هذه المعلومات.

يجب ألا تسجل المحطة بيانات الشريط المغناطيسي الكامل للبطاقة أو بيانات الشريحة إلكترونيًا بغرض السماح أو تمكين طلبات التفويض اللاحقة، بعد محاولة التفويض الأولي.

When an attempted Transaction is rejected, an indication or reason for the rejection must be included on the Terminal Transaction log.

4.6.19 POS Terminal Requirements

Each Merchant is responsible for the maintenance arrangements of its POS Terminals, unless the Acquirer undertakes this function.

4.6.20 Hybrid Terminal Requirements

(Category A as per references set in chapter 1)

A Hybrid Terminal must:

1. Read required data from the chip when present in Chip Cards, and either transmit or process, as appropriate, all required data for authorization processing;
2. Complete the Transaction using the EMV chip if present;
3. Read and process the EMV-compliant NUMO Payment Application when a Card containing such Payment Application is presented, if the Hybrid Terminal reads and processes any other EMV-compliant payment application;
4. Request a cryptogram for all chip-read Transactions; and
5. If the Transaction is approved, transmit an application cryptogram and related data.

A chip-capable Terminal that does not satisfy all of the requirements to be a Hybrid Terminal is deemed by the National Scheme Operator to be a magnetic stripe-only Terminal, and must be identified in Transaction messages as such.

4.6.20.1 Hybrid POS Terminal Requirements

In addition to complying with the above section, a Hybrid POS Terminal must:

1. At a minimum, support online authorization.
2. Support online PIN as the CVM.
3. Perform Card velocity checking.
4. Support online mutual authentication (OMA) and script processing if connected to a debit acquiring network.

A Hybrid POS Terminal is identified in Transaction messages as follows: (technical information to be completed by SCHEME OPERATOR)

A PIN-capable Hybrid POS Terminal is identified in Transaction messages as follows: (technical information to be completed by SCHEME OPERATOR)

A chip-capable POS Terminal that does not satisfy all of the requirements to be a Hybrid POS Terminal is deemed by the National Scheme Operator to be a magnetic stripe-only POS Terminal and must be identified in Transaction messages as such.

4.6.20.2 Hybrid POS Terminal and Chip-only MPOS Terminal Displays

A Hybrid POS Terminal (including any Hybrid MPOS Terminal) and a Chip-only MPOS Terminal must:

1. Display to the Cardholder all mutually supported application labels or preferred names. Multiple matching applications must be displayed in the Issuer's priority sequence.
2. Allow the Cardholder to select the application to be used when multiple matching applications exist.

وعندما يتم رفض محاولة معاملة، يجب تضمين إشارة أو سبب الرفض في سجل معاملات المحطة.

19.6.4. متطلبات محطة نقاط البيع

كل تاجر مسؤول عن القيام بإجراءات الصيانة لمحطات نقاط البيع الخاصة به، ما لم تتولى جهة القبول هذه المهمة.

20.6.4. متطلبات المحطة الهجينة

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب أن تقوم المحطة الهجينة بما يلي:

1. قراءة البيانات المطلوبة من الشريحة عندما تكون موجودة في بطاقات الشريحة الإلكترونية، وأن تقوم بإرسال أو معالجة، حسب الاقتضاء، جميع البيانات المطلوبة لمعالجة التفويض.
2. إكمال المعاملة باستخدام شريحة EMV إن وجدت.
3. قراءة ومعالجة تطبيق نمو للدفع المتوافق مع معيار EMV عند تقديم بطاقة تحتوي على تطبيق هذا الدفع، وإذا كانت المحطة الهجينة تقرأ وتعالج أي تطبيق دفع آخر متوافق مع معيار EMV؛ طلب تشفير لجميع معاملات قراءة الشرائح.
4. في حالة الموافقة على المعاملة، يتم إرسال تطبيق تشفير والبيانات ذات الصلة.
5. يعتبر مشغل شبكة الدفع المحلية المحطة القادرة على قراءة الشريحة والتي لا تلبى جميع المتطلبات لتكون المحطة الهجينة محطة ذات شريط مغناطيسي فقط، ويجب تحديدها في رسائل المعاملات على هذا النحو.

1.20.6.4. متطلبات محطة نقاط البيع الهجينة

بالإضافة إلى الامتثال للقسم أعلاه، يجب على محطة نقاط البيع الهجينة:

1. كحد أدنى، دعم التفويض عبر الإنترنت.
2. دعم رقم التعريف الشخصي عبر الإنترنت باعتباره CVM.
3. إجراء فحص سرعة البطاقة.
4. دعم المصادقة المتبادلة عبر الإنترنت، ومعالجة البرنامج النصي إذا كان متصلًا بشبكة الحصول على الخصم.

يتم تحديد محطة نقاط البيع الهجينة في رسائل المعاملات على النحو التالي: (يجب إكمال المعلومات الفنية بواسطة مشغل شبكة الدفع المحلية).

يتم تحديد محطة نقاط البيع الهجينة القادرة على إدخال رقم التعريف الشخصي في رسائل المعاملات على النحو التالي: (يجب إكمال المعلومات الفنية بواسطة مشغل شبكة الدفع المحلية).

تعتبر محطة نقاط البيع القادرة على قراءة الشريحة، والتي لا تفي بجميع المتطلبات فأنها تكون محطة نقاط بيع هجينة من قبل مشغل شبكة الدفع المحلية، محطة نقاط بيع ذات شريط مغناطيسي فقط، ويجب تحديدها في رسائل المعاملات على هذا النحو.

2.20.6.4 محطات نقاط البيع الهجينة وشاشات محطات نقاط البيع المتنقلة (MPOS) ذات الشريحة فقط

يجب أن تكون محطة نقاط البيع الهجينة (بما في ذلك أي محطة MPOS الهجينة) ومحطة MPOS ذات الشريحة فقط:

1. العرض على حامل البطاقة جميع شعارات التطبيقات المدعومة بشكل متبادل أو الأسماء المفضلة. ويجب عرض تطبيقات المطابقة المتعددة في تسلسل أولوية جهة الإصدار.
2. السماح لحامل البطاقة باختيار وتحديد التطبيق الذي سيتم استخدامه عند وجود عدة تطبيقات مطابقة.

3. Display to the Cardholder the Transaction amount and Transaction currency, if different from the Merchant's or cash disbursement Payment Service Provider's local currency.

4.6.20.3 Hybrid ATM and Bank Branch Terminal Requirements

Each Hybrid ATM and Hybrid Bank Branch Terminal must:

1. Obtain online authorization from the Issuer for each Transaction, whether the magnetic stripe or the chip of the Card is used to initiate the Transaction.
2. Support online PIN as the CVM for all ATM Transactions and for all Manual Cash Disbursement Transactions.
3. Support full use of the multi-application capabilities of Chip Cards by:
 - a. Maintaining a complete list of all Application Identifiers (AIDs) for all products they accept;
 - b. Receiving and retaining updates of AIDs;
 - c. Attempting to match all AIDs contained in the ATM or Bank Branch Terminal with those on the EMV-compliant Chip Card used;
 - d. Displaying all matching application labels or preferred names to the Cardholder;
 - e. Allowing the Cardholder to select the application to be used when multiple matching applications exist; and
 - f. Applying the required key exchange to ensure security and encryption in addition to being PCI compliant,
 - g. Providing the Cardholder the option of approving or canceling a Merchandise Transaction before the products are dispensed or the services are performed.

4.6.21 Contactless-enabled POS Terminals

(Category B as per references set in chapter 1)

If the contact interface of the POS Terminal supports online PIN, then the contactless interface of the POS Terminal must support online PIN for Transactions exceeding the CVM limit. CDCVM may also be supported.

Each acquirer must ensure of uploading the latest AID of NUMO as well as CA PK announced and published by the network

4.6.22 Contactless-only POS Terminals

(Category B as per references set in chapter 1)

When approved by the National Scheme Operator, an Acquirer is permitted to sponsor Merchants that deploy contactless-only POS Terminals or MPOS Terminals. In such event, the Acquirer must ensure that, should such Merchants subsequently deploy POS Terminals or MPOS Terminals with contact payment functionality, such POS Terminals and MPOS Terminals accept and properly process Contact Chip Transactions.

A POS Terminal that utilizes only contactless payment functionality, , must comply with all of the requirements set forth in section 4.7 except those applicable to contact functionality. In addition, such a POS Terminal must:

1. Request a cryptogram for all Contactless Transactions, and if the Transaction is approved, transmit an application cryptogram and related data; and
2. Support online authorization.

3. العرض على حامل البطاقة مقدار مبلغ المعاملة وعملته، إذا كانت مختلفة عن العملة الوطنية لمقدم خدمة الدفع النقدي أو التاجر.

3.20.6.4 متطلبات محطة أجهزة الصراف الآلي الهجينة ومحطة فروع المصرف

يجب على كل محطة جهاز صراف آلي هجينة، ومحطة فرع مصرف هجينة:

1. الحصول على ترخيص عبر الإنترنت من جهة الإصدار لكل معاملة، سواء تم استخدام الشريط المغناطيسي أو شريحة البطاقة لبدء المعاملة.
2. دعم رقم التعريف الشخصي على الإنترنت باعتباره رمز التحقق من البطاقة لجميع معاملات أجهزة الصراف الآلي، ولجميع معاملات الصرف النقدي اليدوية.
3. دعم الاستخدام الكامل لإمكانات التطبيقات المتعددة لبطاقات الشريحة من خلال:
 - أ. الاحتفاظ بقائمة كاملة لجميع معرّفات التطبيقات لجميع المنتجات التي يقبلونها.
 - ب. تلقي تحديثات معرّفات التطبيقات والاحتفاظ بها.
 - ت. محاولة مطابقة جميع معرّفات التطبيقات المساعدة الموجودة في محطة جهاز الصراف الآلي أو فرع المصرف مع تلك الموجودة على بطاقة الشريحة المتوافقة مع معيار EMV المستخدمة.
 - ث. عرض جميع ملصقات التطبيق أو الأسماء المفضلة المطابقة لحامل البطاقة.
 - ج. السماح لحامل البطاقة باختيار التطبيق المراد استخدامه عند وجود عدة تطبيقات مطابقة.
 - ح. تطبيق تبادل المفاتيح المطلوب لضمان الأمان والتشفير بالإضافة إلى التوافق مع PCI،
 - خ. تزويد حامل البطاقة بخيار الموافقة على معاملة البضائع أو إلغاؤها قبل الاستغناء عن المنتجات أو تنفيذ الخدمات.

21.6.4. دعم محطات نقاط البيع غير المتصلة

(الفئة ب حسب المراجع المحددة في الفصل 1)

إذا كانت واجهة جهات الاتصال الخاصة بمحطات نقاط البيع تدعم رقم التعريف الشخصي عبر الإنترنت، فيجب أن تدعم الواجهة غير المتصلة لمحطة نقاط البيع رقم التعريف الشخصي عبر الإنترنت للمعاملات التي تتجاوز حد CVM. يمكنها أيضًا دعم CDCVM. يجب على جهات القبول التحقق من تحميل أحدث معرّفات التطبيقات لنمو بالإضافة إلى CA PK التي تم الإعلان عنها ونشرها من قبل الشبكة.

22.6.4. محطات نقاط البيع الغير متصلة فقط

(الفئة ب حسب المراجع المحددة في الفصل 1)

عند الموافقة عليها من قبل مشغل شبكة الدفع المحلية، يُسمح لجهة القبول برعاية التجار الذين ينشرون محطات نقاط البيع أو محطات MPOS الغير متصلة. وفي مثل هذه الحالة، يجب على جهة القبول التحقق من أنه إذا قام هؤلاء التجار لاحقًا بنشر محطات نقاط البيع أو محطات MPOS مع وظائف الدفع للاتصال، فإن محطات نقاط البيع ومحطات MPOS تقبل معاملات شريحة جهات الاتصال وتعالجها بشكل صحيح.

يجب أن تمثل محطة نقاط البيع التي تستخدم وظيفة الدفع بدون اتصال فقط، مع جميع المتطلبات المحددة في القسم 7.4 باستثناء تلك المطبقة على وظيفة الاتصال. بالإضافة إلى ذلك، يجب على محطة نقاط البيع هذه:

1. تطلب تشفيرًا لجميع المعاملات غير المتصلة، وإذا تمت الموافقة على المعاملة، يتم إرسال تطبيق التشفير والبيانات ذات الصلة؛ و
2. دعم التفويض عبر الإنترنت.

4.6.23 Mobile POS (MPOS) Terminals

(Category B as per references set in chapter 1)

Any Merchant and any Acquirer or cash disbursement Payment Service Provider conducting Manual Cash Disbursement Transactions is permitted to use a Mobile POS (MPOS) Terminal that complies with the POS Terminal Standards.

A Merchant is permitted to use an MPOS Terminal that does not support electronic signature capture and cannot print a paper Transaction receipt at the time the Transaction is conducted.

However, the Merchant must have a means by which to provide a receipt to the Cardholder upon request (for example, in an email or text message). If such means involves the storage, transmission, or processing of Card data, then it must comply with the Payment Card Industry Data Security Standard (PCI DSS).

If the MPOS Terminal or Chip-only MPOS Terminal does not support electronic signature capture, then signature is not required; and if the Merchant has less than LYD XXX in annual Transaction volume and the MPOS Terminal has a contact chip reader and magnetic stripe-reading capability but does not support PIN as a CVM for Contact Chip Transactions, then PIN is not required.

The use of an MPOS Terminal or Chip-only MPOS Terminal lacking such capabilities confers no chargeback protection.

Only a Merchant with less than LYD xxx in annual POS Transaction Volume is permitted to use an MPOS Terminal with any of the following characteristics, for POS Transaction processing only:

1. Has a contact chip reader and magnetic stripe-reading capability but does not support PIN as a CVM for Contact Chip Transactions; or
2. Is a Chip-only MPOS Terminal.

An MPOS Terminal must support online PIN for Manual Cash Disbursement Transactions.

PIN verification, if supported by an MPOS Terminal, must be conducted by means of a PIN entry device (PED) that complies with applicable PIN security requirements.

A Chip Transaction that occurs at an MPOS Terminal must be authorized online by the Issuer, resulting in the generation of a unique Authorization Request Cryptogram (ARQC). All authorization and clearing messages for Transactions occurring at an MPOS Terminal must contain the MPOS acceptance device indicator.

A Chip-only MPOS Terminal must be properly identified in Transaction messages.

4.6.24 Terminals without a Printer

The approval of the National Scheme Operator is required to deploy Terminals without a printer.

4.7 Transaction Receipts

4.7.1 General Requirements

(Category B as per references set in chapter 1)

A Transaction receipt must be provided to the Cardholder upon completion of the Transaction.

All products and services purchased or cash disbursed in the same Transaction must be included on a single Transaction receipt. A Transaction receipt must also be produced for a refund Transaction.

23.6.4. محطات نقاط البيع المتنقلة (MPOS)

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجوز لأي تاجر وأي قابل أو مقدم خدمة دفع مدفوعات نقدية يجري معاملات الصرف النقدي اليدوية باستخدام أجهزة نقاط البيع المتنقلة (MPOS) التي تتوافق مع معايير محطات نقاط البيع.

يُسمح للتاجر باستخدام محطة MPOS التي لا تدعم التقاط التوقيع الإلكتروني، ولا يمكنها طباعة إيصال معاملة ورقية في وقت إجراء المعاملة.

ومع ذلك، يجب أن يكون لدى التاجر وسيلة لتقديم إيصال لحامل البطاقة عند الطلب (على سبيل المثال، في رسالة بريد إلكتروني أو رسالة نصية). وإذا كانت هذه الوسائل تتضمن تخزين بيانات البطاقة أو نقلها أو معالجتها، فيجب أن تمثل لمعيار أمان بيانات صناعة بطاقات الدفع (PCI DSS).

إذا كانت محطة MPOS أو محطة MPOS ذات الشريحة فقط لا تدعم التقاط التوقيع الإلكتروني فإن التوقيع غير مطلوب. إذا كان لدى التاجر أقل من XXX دينار ليبي في حجم المعاملات السنوية، وكان لدى محطة MPOS قارئ شرائح اتصال وإمكانية قراءة الشريط المغناطيسي، ولكنه لا يدعم رقم التعريف الشخصي باعتباره CVM لمعاملات شريحة الاتصال، فلن يكون رقم التعريف الشخصي مطلوبًا. لا يمنح استخدام محطة MPOS أو محطة MPOS ذات الشريحة فقط التي تفتقر إلى مثل هذه الإمكانيات أي حماية لرد المبالغ المدفوعة.

يُسمح فقط للتاجر الذي لديه أقل من xxx دينار ليبي في حجم معاملات نقاط البيع السنوية باستخدام محطة MPOS مع أي من الخصائص التالية، لمعالجة معاملات نقاط البيع فقط:

1. لديه قارئ شرائح اتصال وإمكانية قراءة شريط مغناطيسي، ولكنه لا يدعم رقم التعريف الشخصي باعتباره CVM لمعاملات شريحة الاتصال.
2. عبارة عن محطة MPOS تحتوي على شريحة فقط.

يجب أن تدعم محطة MPOS رقم التعريف الشخصي عبر الإنترنت لمعاملات الصرف النقدي اليدوية.

يجب إجراء التحقق من رقم التعريف الشخصي، إذا كان مدعومًا من خلال محطة MPOS، عن طريق جهاز إدخال رقم التعريف الشخصي (PED) الذي يتوافق مع متطلبات أمان رقم التعريف الشخصي المعمول بها.

يجب أن يتم التفويض بمعاملة الشريحة التي تحدث في محطة MPOS عبر الإنترنت من قبل جهة الإصدار، مما يؤدي إلى إنشاء برنامج تشفير طلب التفويض (ARQC).

يجب أن تحتوي جميع رسائل التفويض والمقاصة للمعاملات التي تحدث في محطة MPOS على مؤشر جهاز قبول MPOS.

يجب تحديد محطة MPOS ذات الشريحة فقط بشكل صحيح في رسائل المعاملات.

24.6.4. المحطات الطرفية بدون طباعة

يجب الحصول على موافقة مشغل شبكة الدفع المحلية للقيام بنشر المحطات الطرفية بدون طباعة.

7.4. إيصالات المعاملات

1.7.4. المتطلبات العامة

(الفئة ب حسب المراجع المحددة في الفصل 1)

يجب تقديم إيصال المعاملة إلى حامل البطاقة عند إتمام المعاملة.

يجب تضمين جميع المنتجات والخدمات التي تم شراؤها أو صرفها نقدًا في نفس المعاملة، في إيصال معاملة واحد. ويجب أيضًا إصدار إيصال معاملة لمعاملة استرداد.

At POS Terminals

At a POS Terminal, a Transaction receipt must be provided to the Cardholder automatically, unless:

- The Merchant offers and the Cardholder declines to receive a Transaction receipt; or
- The Transaction is a Contactless Transaction that is equal to or less than the CVM limit of LYD 300, and the Cardholder does not request a Transaction receipt; or
- The Cardholder requests to receive a Transaction receipt by email or other electronic means; or
- The Transaction occurs at an unattended POS Terminal and the Cardholder selects NO when offered the options to receive or not receive a Transaction receipt.

An unattended contactless-only POS Terminal is not required to provide a Transaction receipt at the time the Transaction is conducted, provided the Merchant has a means by which to provide a Transaction receipt at a later date upon Cardholder request, for example by e-mail or SMS.

If the means by which the Merchant will provide a Transaction receipt involves the storage, transmission, or processing of Card data, then the Acquirer must ensure such means comply with the Payment Card Industry Data Security Standard (PCI DSS). The manner in which to request a Transaction receipt must be clearly displayed at the Merchant location.

An unattended contactless-only POS Terminal using MCC 8398 (Organizations, Charitable and Social Service) offering a Transaction equal to or less than LYD XXX is permitted to be deployed without the capability to provide a Transaction receipt at the time the Transaction is conducted or at a later date. The inability to provide a receipt must be clearly displayed on the Terminal prior to the Transaction being completed.

At ATM and Bank Branch Terminals

A receipt must be provided for a cash withdrawal or other financial Transaction occurring at an ATM or Bank Branch Terminal. ATM cash withdrawals without receipts are allowed when the device is out of paper, the Cardholder being duly advised before completion of the Transaction. The Cardholder's choice to either continue or cancel the Transaction must be requested and respected.

A receipt is not required for a balance inquiry.

Card-Not-Present Transactions

A receipt must be provided for each Card-not-present Transaction. For each completed e-commerce Transaction, a printable receipt page must be displayed after the Cardholder confirms a purchase. With respect to an e-commerce Transaction, non-face-to-face recurring payment Transaction, or any other Card-not-present Transaction upon Cardholder request, a receipt is permitted to be sent to the Cardholder by email or other electronic means.

Refunds

The refund Transaction receipt must contain:

- The date of the refund;
- A description of the returned products, canceled services, or adjustment made; and
- The amount of the refund.

في محطات نقاط البيع

في محطات نقاط البيع، يجب تقديم إيصال المعاملة إلى حامل البطاقة تلقائيًا، ما لم:

- يعرض التاجر، ويرفض حامل البطاقة استلام إيصال المعاملة.
- المعاملة عبارة عن معاملة تتم عن بعد، تساوي أو تقل عن حد CVM البالغ 300 دينار ليبي، ولا يطلب حامل البطاقة إيصالًا للمعاملة.
- أن يطلب حامل البطاقة استلام إيصال المعاملة عن طريق البريد الإلكتروني أو وسيلة إلكترونية أخرى.
- تحدث المعاملة في محطة نقاط البيع غير الخاضعة للرقابة ويختار حامل البطاقة "لا" عند عرض الخيارات عليه لاستلام أو عدم استلام إيصال المعاملة.

لا يُطلب من محطة نقاط البيع بدون اتصال فقط غير المراقبة، تقديم إيصال المعاملة في وقت إجراء المعاملة، بشرط أن يكون لدى التاجر وسيلة لتقديم إيصال المعاملة في تاريخ لاحق بناءً على طلب حامل البطاقة، على سبيل المثال عن طريق البريد الإلكتروني أو الرسائل القصيرة.

وإذا كانت الوسيلة التي سيقدم بها التاجر إيصال المعاملة تتضمن تخزين بيانات البطاقة أو نقلها أو معالجتها، فيجب على جهة القبول التحقق من أن هذه الوسائل تتوافق مع معيار أمان بيانات صناعة بطاقات الدفع (PCI DSS). ويجب عرض طريقة طلب إيصال المعاملة بوضوح في موقع التاجر.

يُسمح بنشر محطة نقاط البيع بدون اتصال فقط غير المراقبة والتي تستخدم MCC 8398 (المنظمات والخدمات الخيرية والاجتماعية) التي تقدم معاملة تساوي أو تقل عن XXX دينار ليبي بدون القدرة على تقديم إيصال معاملة في وقت إجراء المعاملة أو في وقت لاحق. ويجب عرض عدم القدرة على تقديم إيصال بوضوح على المحطة قبل إتمام المعاملة.

في محطات أجهزة الصراف الآلي وفروع المصارف

يجب تقديم إيصال لسحب نقدي، أو معاملة مالية أخرى في محطة جهاز الصراف الآلي أو فرع المصرف. ويُسمح بالسحب النقدي من أجهزة الصراف الآلي بدون إيصالات عند نفاذ الورق، ويتم إخطار حامل البطاقة على النحو الواجب قبل إتمام المعاملة. ويجب طلب واحترام اختيار حامل البطاقة إما لمواصلة المعاملة، أو إلغائها.

الإيصال غير مطلوب للاستعلام عن الرصيد.

معاملات البطاقة غير الموجودة

يجب تقديم إيصال لكل معاملة بطاقة غير موجودة. ولكل معاملة تجارة إلكترونية مكتملة، ويجب عرض صفحة إيصال قابلة للطباعة بعد تأكيد حامل البطاقة على الشراء.

وفيما يتعلق بمعاملة التجارة الإلكترونية، أو معاملة الدفع المتكررة غير المباشرة، أو أي معاملة أخرى بالبطاقة غير موجودة بناءً على طلب حامل البطاقة، يُسمح بإرسال إيصال إلى حامل البطاقة عن طريق البريد الإلكتروني أو وسيلة إلكترونية أخرى.

المبالغ المستردة

يجب أن يحتوي إيصال معاملة الاسترداد على البيانات التالية:

- تاريخ الاسترداد.
- وصف للمنتجات المعادة أو الخدمات الملغاة أو التعديل الذي تم إجراؤه.
- مبلغ الاسترداد.

4.7.2 Transaction Receipt Contents

(Category B as per references set in chapter 1)

4.7.2.1 POS and Manual Cash Disbursement Transaction Receipts

The following information must be included on the Transaction receipt:

1. Acquirer Name.
2. Chip Application ID, in case of a Chip Transaction
3. Merchant Name/Area/Country,
4. Device ID: POS number, Receipt number/RRN (Retrieval Reference Number) and Transaction Batch Number.
5. Truncated card number (last 4 digits to be displayed).
6. Card Expiry (preferably truncated as well).
7. Network name: NUMO network.
8. Transaction amount, Transaction Currency LYD.
9. Authorization Code if transaction was approved by issuer.
10. Transaction processing method (Chip read, magnetic stripe read, fall back, contactless or key-entered).
11. Transaction status (approved, declined, referral, etc.) may be displayed in Arabic language.
12. Transaction Verification method (On-Line PIN entered, or signature if PIN was bypassed or offline mode)
13. Cardholder name (preferable)
14. Print “Customer Copy” at the end of the customer copy of the receipt and “Merchant Copy” at the end of the Merchant copy of the receipt.

A space for the Cardholder’s signature is not required on a Transaction receipt if the Transaction is completed with a PIN or Consumer Device CVM (CDCVM) as the CVM. If a receipt is produced following an unsuccessful Transaction attempt, the receipt must indicate the response or failure reason.

Refund/Void Sale Receipt

Additional wording “REFUND/VOID SALE” to be stated on the receipt.

Transaction Receipt Specific Conditions

The Merchant may add special terms to the Transaction receipt, for example:

- Refund policy,
- In-Store refund only,
- Receipt is required for exchange/refund or
- No refund is allowed.

Recommended Standard Phrases

The National Scheme Operator recommends the addition of the following or similar standard wording to Transaction receipts:

- Goods/Services received inside the store in good condition.
- I authorize to debit the above amount from my card.
- I am informed of the cancellation/return policy.

2.7.4 محتويات إيصال المعاملة

(الفئة ب حسب المراجع المحددة في الفصل 1)

1.2.7.4. إيصالات معاملات الدفع النقدي اليدوي ونقاط البيع

يجب تضمين المعلومات التالية في إيصال المعاملة:

1. اسم جهة القبول.
2. معرف تطبيق الشريحة، في حالة معاملة الشريحة.
3. اسم التاجر/ المنطقة /البلد.
4. معرف الجهاز: رقم نقاط البيع، رقم الإيصال / RRN (الرقم المرجعي للاسترداد) ورقم دفعة المعاملة.
5. رقم البطاقة المقتطع (يتم عرض آخر 4 أرقام).
6. انتهاء صلاحية البطاقة (يفضل اقتطاعها أيضًا).
7. اسم الشبكة: شبكة نمو.
8. مبلغ المعاملة، عملة المعاملة دينار ليبي.
9. رمز التفويض إذا تمت الموافقة على المعاملة من قبل جهة الإصدار.
10. طريقة معالجة المعاملات (قراءة الشريحة، قراءة الشريط المغناطيسي، التراجع، عدم الاتصال أو إدخال المفتاح).
11. قد يتم عرض حالة المعاملة (موافق عليها، مرفوضة، إحالة، إلخ) باللغة العربية.
12. طريقة التحقق من المعاملة (إدخال رقم التعريف الشخصي عبر الإنترنت، أو التوقيع إذا تم تجاوز رقم التعريف الشخصي أو وضع غير متصل بالشبكة).
13. اسم حامل البطاقة (يفضل).
14. طباعة “نسخة العميل” في نهاية نسخة العميل من الإيصال و “نسخة التاجر” في نهاية نسخة التاجر من الإيصال.

لا يلزم وجود مساحة لتوقيع حامل البطاقة على إيصال المعاملة إذا تم إكمال المعاملة باستخدام رقم التعريف الشخصي أو CVM لجهاز المستهلك (CDCVM) باعتباره رمز التحقق من البطاقة (CVM). وإذا تم تقديم إيصال بعد محاولة معاملة غير ناجحة، فيجب أن يشير الإيصال إلى الاستجابة أو سبب الفشل.

إيصال استرداد/ بيع باطل

يجب ذكر الصياغة الإضافية “استرداد/بيع باطل” على الإيصال.

الشروط الخاصة بإيصال المعاملة.

يجوز للتاجر إضافة شروط خاصة إلى إيصال المعاملة، على سبيل المثال:

- سياسة الاسترجاع.
- رد الأموال في المتجر فقط،
- الإيصال مطلوب للاستبدال أو الاسترداد.
- لا يسمح برد.

العبارات المعيارية الموصى بها

يوصي مشغل شبكة الدفع المحلية بإضافة الصياغة المعيارية التالية أو ما شابهها إلى إيصالات المعاملات:

- استلام البضائع/الخدمات داخل المتجر بحالة جيدة.
- أصرح بخصم المبلغ أعلاه من بطاقتي.
- لقد تم إبلاغي بسياسة الإلغاء والإرجاع.

4.7.2.2 ATM and Bank Branch Terminal Transaction Receipt Requirements

The following information must be included on a Transaction receipt:

1. Acquirer name.
2. Chip Application ID, in case of a Chip Transaction
3. ATM Location/ATM Number/ATM Name.
4. Truncated card number (last 4 digits to be displayed)
5. Network name: NUMO network.
6. Transaction amount, Transaction Date and Time.
7. Authorization Code.
8. Transaction status (Approved/Declined) may be displayed in Arabic language.
9. Chip/Magnetic stripe /Contactless transaction, as applicable.

4.7.2.3 Primary Account Number and Expiration Date Omission

(Category A as per references set in chapter 1)

A Transaction receipt generated by an electronic Terminal, whether attended or unattended, must not include the Card expiration date. In addition, a Transaction receipt generated for a Cardholder by an electronic Terminal, whether attended or unattended, must reflect only the last four digits of the primary account number (PAN). All preceding digits of the PAN must be replaced with fill characters, such as “X,” “*,” or “#,” that are neither blank spaces nor numeric characters.

The National Scheme Operator strongly recommends that if an electronic POS Terminal generates Merchant copies of Transaction receipts, the Merchant copies should also reflect only the last four digits of the PAN, replacing all preceding digits with fill characters, such as “X,” “*,” or “#,” that are neither blank spaces nor numeric characters.

4.7.2.4 Prohibited Information

(Category A as per references set in chapter 1)

The Transaction receipt and any other Acquirer or Merchant document must not reflect:

- The PIN, any part of the PIN, or any fill characters representing the PIN; or
- The Card Verification Value 2 (CVV 2).

4.7.3 Transaction Receipts - CNP Transactions

(Category B as per references set in chapter 1)

At the final stage of the Transaction, detailed data of the order must be displayed for the Cardholder and must include all of following:

- Order Number/ID.
- Total amount to be charged to the Account, including delivery charges.
- Order date and Estimated date of delivery/service fulfillment.
- Summary of ordered merchandise/service.

The Merchant should maintain all related correspondences, order screens and any related document to support the Transaction.

2.2.7.4 متطلبات استلام معاملات محطات أجهزة الصراف الآلي وفروع المصرف

يجب تضمين المعلومات التالية في إيصال المعاملة:

1. اسم جهة القبول.
2. معرف تطبيق الشريحة، في حالة معاملة شريحة
3. موقع الصراف الآلي / رقم الصراف الآلي / اسم الصراف الآلي.
4. رقم البطاقة المقتطع (يتم عرض آخر 4 أرقام)
5. اسم الشبكة: شبكة نمو.
6. مبلغ المعاملة وتاريخ المعاملة والوقت.
7. رمز التفويض.
8. يمكن عرض حالة المعاملة (موافق عليها / مرفوض) باللغة العربية.
9. شريحة/ شريط مغناطيسي/ معاملة غير متصلة، حسب الاقتضاء.

3.2.7.4 رقم الحساب الأساسي وتاريخ انتهاء الصلاحية

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب ألا يتضمن إيصال المعاملة الذي تم إنشاؤه بواسطة جهاز إلكتروني، سواء أكان مراقب أم غير مراقب، تاريخ انتهاء صلاحية البطاقة. بالإضافة إلى ذلك، يجب أن يعكس إيصال المعاملة الذي تم إنشاؤه لحامل البطاقة بواسطة جهاز إلكتروني، سواء أكان مراقب أم غير مراقب، الأرقام الأربعة الأخيرة فقط من رقم الحساب الأساسي. ويجب استبدال جميع الأرقام السابقة من رقم الحساب الأساسي بأحرف تعبئة، مثل “X” أو “*” أو “#”، والتي هي ليست مسافات فارغة ولا أحرفاً رقمية. يوصي مشغل شبكة الدفع المحلية بشدة أنه في حالة قيام وحدة نقاط البيع الإلكترونية بإنشاء نسخ التاجر من إيصالات المعاملة، يجب أن تعكس نسخ التاجر أيضاً الأرقام الأربعة الأخيرة فقط من رقم الحساب الأساسي، مع استبدال جميع الأرقام السابقة بأحرف تعبئة، مثل “X”، “*” أو “أو” # ” والتي هي ليست مسافات فارغة ولا أحرفاً رقمية.

4.2.7.4 المعلومات المحظورة

(الفئة أ حسب المراجع المحددة في الفصل 1)

يجب ألا يحتوي إيصال المعاملة وأي جهة استحواذ أو مستند تاجر آخر ما يلي:

- رقم التعريف الشخصي أو أي جزء من رقم التعريف الشخصي أو أي أحرف تعبئة تمثل رقم التعريف الشخصي.
- قيمة التحقق من البطاقة 2 (CVV 2).

3.7.4 إيصالات المعاملات – معاملات البطاقة الغير الموجودة CNP

(الفئة ب حسب المراجع المحددة في الفصل 1)

في المرحلة الأخيرة من المعاملة، يجب عرض بيانات الطلب التفصيلية لحامل البطاقة، ويجب أن تتضمن كل ما يلي:

- رقم الطلب والتعريف.
- المبلغ الإجمالي الذي سيتم تحميله على الحساب، بما في ذلك رسوم التسليم.
- تاريخ الطلب والتاريخ التقديري للتسليم أو الوفاء بالخدمة.
- ملخص للبضائع، أو الخدمة المطلوبة.

يجب أن يحتفظ التاجر بجميع المراسلات ذات الصلة وشاشات الطلبات وأي مستندات ذات صلة لدعم المعاملة.

4.7.4 Delayed Delivery Transaction Receipt Requirements

(Category B as per references set in chapter 1)

When products or services will be delivered or performed after the Transaction date, and one Transaction receipt represents a deposit, and the second Transaction receipt represents payment of the balance, the Merchant must note the words “deposit” and “balance” on the Transaction receipts as appropriate. The second Transaction receipt is contingent on the delivery or performance of the products or services, and must not be presented until after the products or services are delivered or performed.

Regulatory Rules of The Libyan National Payment Scheme

Chapter 5- Authorization – Clearing & Settlement Management

This chapter contains information relating to the authorization, clearing, and settlement functions performed by the Interchange System, and describes Member obligations relating to these functions.

5.1 The Authorization Platform

Authorization is the process by which one Member requests to make a payment to or receive a payment from another Member, and to which the other Member responds with an approval, decline, or other appropriate response to the request.

An Issuer or Acquirer may contract with an Service Provider to perform any of a variety of authorization functions on its behalf. The Service Provider may assist a Member in such activities as issuing Cards, processing authorization Transactions, or processing Card portfolios. A Member must register each such Service Provider with the National Scheme Operator as its Service Provider.

NOTE: Throughout this Chapter, functional references to Issuers and Acquirers also refer to others acting as authorized Payment Service Providers for them. Members are responsible for the acts and omissions of their Payment Service Providers, including those with respect to National Scheme Operator rules, regulations, policies, and procedures.

5.1.1.1 Acquirer Responsibilities

An Acquirer must provide adequate and reasonable authorization services to each Merchant with whom Acquirer has entered into a Merchant Agreement, and to fulfill all responsibilities relating to authorization service, including:

- Access the Authorization Platform
- Create and send authorization request, reversal, and authorization completion advice messages as required pursuant to the National Scheme Operator authorization routing requirements, including Transactions involving expired Cards and invalid National Scheme Operator BINs
- Support all required authorization message types, as the Standards require
- Recognize and respond appropriately to all valid Transaction types, including purchase, purchase with cash back, refund, and cash disbursement Transactions.
- Receive the authorization response and pass the response to the Merchant or ATM

4.7.4. متطلبات استلام معاملات التسليم المتأخر

(الفئة ب حسب المراجع المحددة في الفصل 1)

عندما يتم تسليم المنتجات أو الخدمات أو تنفيذها بعد تاريخ المعاملة، ويمثل إيصال المعاملة الواحدة وديعة، ويمثل إيصال المعاملة الثاني دفع الرصيد، يجب على التاجر ملاحظة كلمتي “إيداع” و “رصيد” في إيصالات المعاملة حسب الاقتضاء. إيصال المعاملة الثاني مشروط بتسليم أو أداء المنتجات أو الخدمات، ويجب عدم تقديمه إلا بعد تسليم المنتجات أو الخدمات أو أدائها.

القواعد التنظيمية لشبكة الدفع المحلية الليبية

الفصل 5- التفويض – إدارة المقاصة والتسوية

يحتوي هذا الفصل على المعلومات التي تتعلق بوظائف التفويض، المقاصة والتسوية التي يؤديها نظام التبادل، ويصف التزامات الأعضاء المتعلقة بهذه الوظائف.

1.5. منصة التفويض

التفويض هو العملية التي يطلب من خلالها أحد الأعضاء إجراء دفعة أو تلقي دفعة من عضو آخر، ويستجيب لها العضو الآخر بالموافقة أو الرفض أو أي استجابة مناسبة أخرى للطلب.

يجوز لجهة الإصدار أو جهة القبول التعاقد مع مقدم خدمة، لأداء أي من وظائف التفويض المتنوعة نيابة عنها. ويجوز لمقدم الخدمة مساعدة العضو في أنشطة مثل إصدار البطاقات أو معالجة معاملات التفويض أو معالجة محافظ البطاقات. ويجب على العضو تسجيل كل مقدم خدمة لدى مشغل شبكة الدفع المحلية كمقدم خدمة له.

ملاحظة: خلال هذا الفصل، تشير المراجع الوظيفية لجهات الإصدار والقبولين أيضًا إلى آخرين يعملون كمقدمي خدمة دفع معتمدين لهم. والأعضاء مسؤولون عن أفعال وتقصير مقدمي خدمة الدفع، بما في ذلك تلك المتعلقة بقواعد مشغل شبكة الدفع المحلية ولوائحه وسياساته وإجراءاته.

5.1.1.1 مسؤوليات جهة القبول

يجب على جهة القبول أن تقوم بتقديم خدمات تفويض كافية ومعقولة لكل تاجر أبرم مع جهة القبول اتفاقية تاجر، والوفاء بجميع المسؤوليات المتعلقة بخدمة التفويض، بما في ذلك:

- الوصول إلى منصة التفويض.
- إنشاء وإرسال رسائل إرشاد بشأن طلب التفويض والعكس وإكمال التفويض كما هو مطلوب وفقًا لمتطلبات توجيه توجيه مشغل شبكة الدفع المحلية، بما في ذلك المعاملات التي تتضمن البطاقات منتهية الصلاحية وأرقام التعريف المصرفية لمشغل شبكة الدفع المحلية الوطني غير الصالحة.
- دعم جميع أنواع رسائل التفويض المطلوبة، طبقاً للمعايير المعمول بها.
- التعرف على جميع أنواع المعاملات الصالحة، والاستجابة لها بشكل مناسب، بما في ذلك الشراء، والشراء باسترداد نقدي، واسترداد الأموال، ومعاملات الصرف النقدي.
- تلقي رد التفويض وتميرير الرد إلى التاجر أو جهاز الصراف الآلي.

- Assisting in investigation of counterfeits and criminal cases
- Billing, which may include fees for use of the Authorization Platform (Acquirer access fees); use of value-added services; and call referral credits (for Acquirer response to call referrals within established time frames)

Authorization Logs

Acquirers must maintain, for at least [120] days, a record or log of all Transaction authorization requests and responses, including all relevant data files. Each log must contain the following information:

- Authorization approval code given by the Issuer, or the Transaction certificate (TC) given by the EMV chip Card (and any substitute value that may have additionally been provided by the Acquirer); and
- Indication that the Merchant reported that the Card may be stolen or counterfeit or that the Transaction caused the merchant to be suspicious, if this situation occurred.

5.1.1.2 Issuer Responsibilities

An Issuer must support authorization processing on behalf of its Cardholders and fulfill all responsibilities relating to authorization service, including:

- Encoding and validating the Card Validation Value1 (CVV 1) value and Chip CVV
- Imprinting and validating the Card Validation Value2 (CVV 2) value
- Personalizing and validating the Card Validation Value3 (CVV 3) value (dynamic CVV 3 for contactless devices)
- Generating and validating the Accountholder Authentication Value (AAV) for e-commerce Transactions
- Issuing and validating personal identification number (PIN) data
- Validating the authorization request cryptogram (ARQC) and generating the authorization response cryptogram (ARPC) for Chip Transactions
- Processing authorization requests
- File maintenance
- Billing, which may include fees for use of the Authorization Platform (Issuer access fees); use of value-added services; and call referral debits (for issuance of call referral responses and for receiving response calls from Acquirers)

File Maintenance

Issuers maintain the account listings of restricted, negative, and positive cards. Issuers can list accounts in the following files:

- Premium Listings
- Local Stoplist

5.1.2 Dual Message System and Single Message System Message Types

Message types processed on the Dual Message System and Single Message System of the Authorization Platform include dual message authorization request, single message financial transaction request, advice, response, acknowledgement, file update, administrative, and network management messages.

- المساعدة في إجراءات التحقيق في دعاوى التزوير الجنائية
- الفوترة، والتي قد تشمل رسوم استخدام منصة التفويض (رسوم وصول القابل)؛ استخدام الخدمات ذات القيمة المضافة؛ وأرصدة إحالة الاتصال (لاستجابة جهة القبول لإحالات المكالمات ضمن المواعيد الزمنية المحددة)

سجلات التفويض

يجب أن تحتفظ جهات القبول، لمدة لا تقل عن 120 يوماً بسجل طلبات تفويض المعاملات والاستجابات، بما في ذلك جميع ملفات البيانات ذات الصلة. ويجب أن يحتوي كل سجل على المعلومات التالية:

- رمز الموافقة على التفويض المقدم من جهة الإصدار، أو شهادة المعاملة (TC) المقدمة من بطاقة شريحة EMV (وأي قيمة بديلة قد تكون قدمها جهة القبول بالإضافة إلى ذلك)
- الإشارة إلى أن التاجر قد أبلغ أن البطاقة قد تكون مسروقة أو مزيفة أو أن المعاملة تسببت في لغت انتباه التاجر.

2.1.1.5 مسؤوليات جهة الإصدار

يجب على جهة الإصدار دعم معالجة التفويض نيابة عن حاملي البطاقات والوفاء بجميع المسؤوليات المتعلقة بخدمة التفويض، بما في ذلك:

- ترميز قيمة التحقق من صحة البطاقة (CVV 1) وقيمة التحقق من صحة بطاقة الشريحة Chip CVV.
- طباعة قيمة التحقق من صحة بطاقة (CVV 2).
- إضفاء الطابع الشخصي والتحقق من صحة قيمة التحقق من البطاقة 3 (CVV 3) (CVV 3) الديناميكي للأجهزة التي تقدم الخدمة عن بعد.
- إنشاء والتحقق من صحة قيمة مصادقة صاحب الحساب (AAV) لمعاملات التجارة الإلكترونية.
- إصدار والتحقق من صحة بيانات رقم التعريف الشخصي (PIN).
- التحقق من صحة طلب ترميز التفويض (ARQC) وإنشاء برنامج تشفير استجابة التفويض (ARPC) لمعاملات الشريحة.
- معالجة طلبات الإذن.
- صيانة الملف.
- الفوترة، والتي قد تتضمن رسومًا لاستخدام منصة التفويض (رسوم وصول جهة الإصدار)؛ واستخدام الخدمات ذات القيمة المضافة؛ وخصم إحالة المكالمات (للإصدار استجابات إحالة المكالمات وتلقي مكالمات الرد من المستقبلين).

صيانة الملف

تحتفظ جهات الإصدار بقوائم الحسابات الخاصة بالبطاقات المقيدة والسلبية والموجبة. ويمكن لجهات الإصدار سرد الحسابات في الملفات التالية:

- القوائم المميزة.
- قائمة التوقف المحلية.

2.1.5 أنواع الرسائل: نظام الرسائل المزدوجة ونظام الرسائل الواحدة

يشمل أنواع الرسائل التي تتم معالجتها على نظام الرسائل المزدوجة ونظام الرسائل الفردية لمنصة التفويض، على طلب تفويض مزدوج للرسائل، وطلب معاملة مالية برسالة واحدة واستشارة، استجابة، إقرار، تحديث ملف ورسائل إدارية وإدارة الشبكة.

About Authorization Request Messages—Dual Message System

Authorization/01xx messages transport authorization-related information. “Authorization” is a term applied to Transactions for which, by design, there is partial Transaction data contained within the individual messages; no actual posting of accounts at the Issuer processing system (IPS) occurs during this type of transmission. Consequently, all Authorization/01xx messages and advice Transactions assume that follow-up information (for example, paper or electronic clearing Transactions) will be used to effect actual settlement, Cardholder account posting, and Cardholder billing.

Authorization/01xx messages are defined as:

- Authorization Request messages
- Authorization Advice messages
- Authorization Response Acknowledgement messages

Authorization Request/0100 - 1100

The Authorization Request/0100 - 1100 message requests approval authorization or guarantee for a Transaction to proceed. The Authorization Request/0100 - 1100 message is not intended to permit the application of this Transaction to the Cardholder’s account for issuing a bill or statement.

(See appendix number 10)

Authorization Request Response/0110 - 1110

The Authorization Request Response must be sent in response to an Authorization Request/0100 - 1100 message; it carries the response information required to service (approve or deny) the Authorization Request/0100 - 1100 message.

(See appendix number 11)

About Authorization Advice Messages

The Authorization Platform uses guaranteed advice message delivery for all advice messages transmitted using the Authorization Platform.

Guaranteed advice message delivery provides a message routing facility. When an advice message is forwarded to the Authorization Platform, the Authorization Platform:

- Immediately secures the Transaction for future delivery
- Responds to the advice message initiator with an advice response message, indicating that it received and secured the message
- Forwards the advice message to the appropriate receiving entity

The Authorization Platform guarantees the delivery of all advice messages routed through the NUMO network. Occasionally, the Authorization Platform cannot immediately deliver an advice message (for example, because of a system or communication failure at the destination). In this case, the Authorization Platform stores the message on its store-and-forward (SAF) processing facilities and automatically delivers the message when communication is restored.

The receiver of an advice message must acknowledge receipt with an appropriate advice response message. When the Authorization Platform receives the advice response message, the National Scheme Operator considers advice delivery complete and removes the message from SAF processing queues.

حول رسائل طلب التفويض - نظام الرسائل المزدوجة

التفويض/ الرسائل 01xx نقل المعلومات المتعلقة بالتفويض. “التفويض” هو مصطلح ينطبق على المعاملات التي يوجد لها، حسب تصميمها، بيانات معاملة جزئية متضمنة في الرسائل الفردية؛ ولا يحدث ترحيل فعلي للحسابات في نظام معالجة جهة الإصدار (IPS) أثناء هذا النوع من الإرسال. وبالتالي، فإن جميع رسائل التفويض/ 01xx والمعاملات الاستشارية يفترض أنها سيتم استخدام معلومات المتابعة (على سبيل المثال، معاملات المقاصة الورقية أو الإلكترونية) لإحداث تسوية فعلية، وترحيل حساب حامل البطاقة، وفواتير حامل البطاقة.

يتم تعريف رسائل التفويض/ 01xx على النحو التالي

- رسائل طلب التفويض.
- رسائل إشعار التفويض.
- رسائل إقرار استجابة التفويض.

طلب تفويض/ 0100-1100

تطلب رسالة طلب التفويض/ 0100 - 1100 إذنًا بالموافقة، أو ضمانًا لمتابعة المعاملة. ولا تهدف رسالة طلب التفويض/ 0100-1100 إلى السماح بتطبيق هذه المعاملة على حساب حامل البطاقة لإصدار فاتورة أو بيان. (انظر الملحق رقم 10)

استجابة طلب التفويض / 0110 - 1110

يجب إرسال “استجابة طلب التفويض” ردًا على رسالة “طلب التفويض” / 0100-1100؛ يحمل معلومات الاستجابة المطلوبة لخدمة (الموافقة أو الرفض) على رسالة طلب التفويض/ 0100-1100. (انظر الملحق رقم 11)

حول رسائل نصائح التفويض

تستخدم منصة التفويض تسليم رسائل إخطارات مضمونة لجميع رسائل الإرشاد المرسل باستخدام منصة التفويض.

يوفر تسليم الرسائل الإرشادية المضمونة وسيلة توجيه الرسائل. عند إعادة توجيه رسالة إرشاد إلى منصة التفويض، فإن منصة التفويض:

- يؤمن المعاملة على الفور للتسليم في المستقبل
- يستجيب لمنشئ رسالة الإرشاد برسالة إرشاد للرد، مشيرًا إلى أنه استلم الرسالة وقام بتأمينها
- إعادة توجيه رسالة الإرشاد إلى الكيان المتلقي المناسب.

تضمن منصة التفويض تسليم جميع رسائل النصائح الموجهة عبر شبكة نمو. من حين لآخر، لا يمكن لمنصة التفويض تسليم رسالة إرشاد على الفور (على سبيل المثال، بسبب فشل النظام أو الاتصال في الوجهة). في هذه الحالة، يقوم برنامج التفويض بتخزين الرسالة في مرافق معالجة التخزين وإعادة التوجيه (SAF) الخاصة به ويقوم تلقائيًا بتسليم الرسالة عند استعادة الاتصال.

يجب أن يقر متلقي رسالة الإرشاد بالاستلام مع رسالة استجابة إرشادية مناسبة. عندما تتلقى منصة التفويض رسالة استجابة النصيحة، يعتبر مشغل شبكة الدفع المحلية أن تسليم المشورة قد اكتمل ويزيل الرسالة من قوائم انتظار معالجة SAF.

The Guaranteed Advice Message Delivery messages include:

- Authorization Advice/0120 - 1120—Acquirer-generated
- Authorization Advice/0120 - 1120—System-generated
- Authorization Advice Response/0130 - 1130 —Issuer-generated (Responding to a System-generated 0120 - 1120 from SAF)
- Authorization Advice Response/0130 - 1130—Issuer-generated (Responding to an Acquirer-generated 0120 - 1120)
- Authorization Advice Response/0130 - 1130 —System-generated

Authorization Advice/0120 - 1120—Acquirer-Generated

The Authorization Advice/0120 - 1120—Acquirer-generated message advises of an authorization that was carried out on the Issuer’s behalf. It is not intended to permit the application of this Transaction to the Cardholder’s account for issuing a bill or statement; for example, this is a non-posting advice message.
(See appendix number 12)

Authorization Advice/0120 - 1120—Issuer-Generated

Authorization Request/0100 - 1100 messages may contain Bank Identification Number (BINs) that Members have selected for scoring. For these Transactions, Issuers create and send Authorization Advice/0120 - 1120 messages to the risk scoring system. The risk scoring system sends to the Issuer an Authorization Advice Response/0130 - 1130 to acknowledge receipt of the Authorization Advice/0120 - 1120.
(See appendix number 13)

Authorization Advice/0120 - 1120—System-Generated

The Authorization Advice/0120 - 1120—System-generated message advises of an authorization that was carried out on the Issuer’s behalf. It is not intended to permit the application of this Transaction to the Cardholder’s account for issuing a bill or statement; for example, this is a non-posting advice message.
(See appendix number 14)

Authorization Advice Response/0130 - 1130—Issuer-Generated (Responding to an Acquirer-Generated 0120 - 1120)

The Authorization Advice Response/0130 - 1130—Issuer-generated message indicates positive receipt of an Authorization Advice/0120 - 1120—Acquirer-generated message.
(See appendix number 15)

Authorization Advice Response/0130 - 1130—Issuer-Generated (Responding to a System-Generated 0120 - 1120 from SAF)

The Authorization Advice Response/0130 - 1130—Issuer-generated message indicates positive receipt of an Authorization Advice/0120 - 1120—System-generated message from store-and-forward (SAF).
(See appendix number 16)

تتضمن رسائل تسليم رسائل المشورة المضمونة ما يلي:

- نصيحة التفويض / 0120 - 1120 - تم إنشاء القابل
 - نصيحة التفويض / 0120 - 1120 - تم إنشاؤه بواسطة النظام
 - استجابة نصيحة التفويض / 0130 - 1130 - مصدرها جهة الإصدار (استجابة لنظام تم إنشاؤه بواسطة النظام 0120-1120 من SAF)
 - استجابة نصيحة التفويض / 0130 - 1130 - جهة الإصدار التي تم إنشاؤها (استجابة لمكتسب تم إنشاؤه 0120-1120)
 - استجابة نصيحة التفويض / 0130 - 1130 - تم إنشاؤه بواسطة النظام
 - نصيحة التفويض / 0120 - 1120 - أنشأتها جهة القبول
- نصيحة التفويض 0120 - 1120 - تنصح الرسالة التي أنشأتها جهة القبول على التفويض الذي تم تنفيذه نيابة عن جهة الاصدار. ولا يُقصد بها السماح بتطبيق هذه المعاملة على حساب حامل البطاقة لإصدار فاتورة أو بيان؛ على سبيل المثال، هذه رسالة إرشاد لا تتعلق بالنشر.
(انظر الملحق رقم 12)

إشعار التفويض / 0120 - 1120 — أنشأتها جهة الاصدار

قد تحتوي رسالة طلب التفويض / 0100-1100 على رقم تعريف مصرفي (BINs) الذي حدده الأعضاء للتسجيل. بالنسبة لهذه المعاملات، تنشئ جهات الاصدار وترسل إشعار التفويض / 0120 - 1120 رسالة إلى نظام تسجيل المخاطر. ويرسل نظام تسجيل المخاطر إلى جهة الإصدار استجابة إشعار التفويض / 0130 - 1130 للإقرار باستلام إشعار التفويض / 0120 - 1120.
(انظر الملحق رقم 13)

نصيحة التفويض / 0120 - 1120 - أنشأها النظام

إشعار التفويض / 0120 - 1120 —إشعار رسالة تم إنشاؤها من قبل النظام بالتفويض الذي تم تنفيذه نيابة عن جهة الاصدار. ولا يُقصد بها السماح بتطبيق هذه المعاملة على حساب حامل البطاقة لإصدار فاتورة أو بيان؛ على سبيل المثال، هذه رسالة إرشاد لا تتعلق بالنشر.
(انظر الملحق رقم 14)

استجابة نصيحة التفويض / 0130 - 1130 - أنشأتها جهة الإصدار (استجابة إلى التي أنشأتها الجهة قابلة 0120-1120)

استجابة نصيحة التفويض / 0130 - 1130 - تشير الرسالة التي أنشأتها جهة الاصدار إلى استلام إيجابي لنصيحة التفويض / 0120 - 1120 —الرسالة التي أنشأتها جهة القبول.
(انظر الملحق رقم 15)

استجابة نصيحة التفويض / 0130 - 1130 - أنشأتها جهة الإصدار (استجابة لـ 0120-1120 التي أنشأها النظام من SAF)

استجابة نصيحة التفويض / 0130 - 1130 - تشير الرسالة التي أنشأتها جهة الاصدار إلى استلام إيجابي لإشعار التفويض / 0120 - 1120 - رسالة تم إنشاؤها بواسطة النظام من المخزن وإعادة التوجيه (SAF).
(انظر الملحق رقم 16)

Authorization Advice Response/0130 – 1130—System-Generated

The Authorization Advice Response/0130 – 1130—System-generated message indicates positive receipt of an Authorization Advice/0120 – 1120 message.
(See appendix number 17)

About Authorization Response Acknowledgement Messages

The Authorization Platform provides optional interactive response acknowledgement for Authorization/0100 – 1100 messages. Acknowledgement messages indicate positive receipt of a response or advice message.
Acquirers are required to support Authorization Response Acknowledgement/0180 messages, but the National Scheme Operator encourages Acquirer Members to select this option and to support these messages. Members have the possibility to select this option at network configuration time.

The Authorization Response Acknowledgement messages include:

- Authorization Response Acknowledgement/0180 – 1180
- Authorization Response Negative Acknowledgement/0190 – 1190

Authorization Acknowledgement/0180

The Authorization Advice Acknowledgement/0180 message indicates positive acknowledgement that it received a previous Authorization Request Response/0110 – 1110 message.

The Authorization Acknowledgement/0180 message is optional for an Acquirer processing system APS.

(See appendix number 18)

Authorization Negative Acknowledgement/0190

The Authorization Platform sends to an IPS an Authorization Negative Acknowledgement/0190 message only in response to late or invalid Authorization Request Response/0110 – 1110 messages from an IPS. This informs the IPS that the Authorization Platform has timed-out or rejected the Authorization Request Response/0110 – 1110 message and initiated Stand-In processing or alternate authorization services on the Issuer's behalf. The Authorization Platform also may send the Authorization Negative Acknowledgement/0190 in response to a late or invalid Reversal Request Response/0410 message. In this scenario, the Authorization Negative Acknowledgement/0190 message informs the IPS that the Authorization Platform responded to the Acquirer.

(See appendix number 19)

About Financial Transaction Messages—Single Message System

The term “financial transaction” applies when there is sufficient data contained within the individual transaction message to provide actual posting of accounts at the issuer processing system (IPS). Financial Transaction/02xx messages are used for the following:

- Financial transaction requests
- Financial transaction request responses
- Financial transaction advices
- Financial transaction advice responses

The Single Message System processes all Financial Transaction/02xx – 12xx messages assuming that upon successful completion no subsequent information is required to perform actual Cardholder Account posting and Cardholder billing.

استجابة نصيحة التفويض / 0130 - 1130 - أنشأها النظام

تشير استجابة نصيحة التفويض / 0130 - 1130 —الرسالة التي تم إنشاؤها بواسطة النظام إلى استلام إيجابي لرسالة "إشعار التفويض" / 0120 - 1120.
(انظر الملحق رقم 17)

حول رسائل إقرار استجابة التفويض

يوفر برنامج التفويض إقرار استجابة تفاعلية اختياريًا لرسائل التفويض / 0100-1100. تشير رسائل الاستلام إلى استلام إيجابي لرد، أو رسالة إرشاد.
يُطلب من جهات القبول دعم رسائل إقرار استجابة التفويض / 0180، لكن مشغل شبكة الدفع المحلية يشجع أعضاء جهات القبول على تحديد هذا الخيار ودعم هذه الرسائل. ويمكن للأعضاء تحديد هذا الخيار في وقت تكوين الشبكة.
تتضمن رسائل إقرار استجابة التفويض ما يلي:

- إقرار استجابة التفويض / 0180 – 1180.
- الإقرار السلبي لاستجابة التفويض / 0190 – 1190.

إقرار التفويض / 0180

تشير رسالة إقرار إشعار التفويض / 0180 إلى إقرار إيجابي بأنه تلقى استجابة طلب تفويض سابقة / 0110-1110.

رسالة إقرار التفويض / 0180 اختيارية لنظام معالجة القابل APS.

(انظر الملحق رقم 18)

الإقرار السلبي للتفويض / 0190

يرسل نظام التفويض إلى IPS رسالة إقرار سلبي للترخيص / 0190 فقط استجابةً لطلب التفويض المتأخر أو غير الصحيح / 0110 - 1110 رسائل من IPS. ويُعلم هذا IPS أن منصة التفويض قد انتهت فترة القبول أو رفضت رسالة استجابة طلب التفويض / 0110-1110 وبدأت المعالجة الاحتياطية أو خدمات التفويض البديلة نيابة عن جهة الإصدار. وقد ترسل منصة التفويض أيضًا الإقرار السلبي للتفويض / 0190 ردًا على رسالة رد طلب الإلغاء المتأخرة أو غير الصالحة / 0410. في هذه الحالة، تُعلم رسالة الإقرار السلبي للتفويض / 0190 IPS أن منصة التفويض استجابت للقابل.
(انظر الملحق رقم 19)

حول رسائل المعاملات المالية - نظام رسالة واحدة

ينطبق مصطلح "معاملة مالية" عندما تكون هناك بيانات كافية مضمنة في رسالة المعاملة الفردية لتوفير ترحيل فعلي للحسابات في نظام معالجة جهة الإصدار. (IPS) تُستخدم رسائل المعاملات المالية / 02 xx لما يلي:

- طلبات المعاملات المالية.
- استجابات طلبات المعاملات المالية.
- اخطارات المعاملات المالية.
- استجابات المشورة بشأن المعاملات المالية.

يقوم نظام الرسالة الواحدة بمعالجة جميع المعاملات المالية / 02 12xx - xx رسائل بافتراض أنه عند الانتهاء بنجاح، لن تكون هناك حاجة إلى معلومات لاحقة لإجراء الترحيل الفعلي لحساب حامل البطاقة، وفواتير حامل البطاقة.

NOTE: Chip Card Transactions at an ATM must be authorized online with a PIN. Financial Transaction Advice/0220 messages from an Acquirer for offline Chip Card Transactions at an ATM will be declined with a DE 39 (Response Code) value of 12 (Invalid Transaction). The following figure illustrates the standard message flow for interactive financial Transaction processing.

(See appendix number 20)

1. The Acquirer initiates a Financial Transaction Request/0200 message to the Single Message System.
2. The Single Message System forwards the Financial Transaction Request/0200 message to the Issuer.
3. The Issuer generates a Financial Transaction Request Response/0210 message and sends it to the Single Message System.
4. The Single Message System forwards the Financial Transaction Request Response/0210 message to the Acquirer.

The following information lists the definitions of all ISO 8583-1993 Financial Transaction/02xx messages supported on the network.

Financial Transaction Request/0200 Message

This message is used to request approval of a Transaction that, if approved, will permit the application of the Transaction financial data to the Cardholder's Account for issuing a bill or statement.

(See appendix number 21)

Financial Transaction Request Response/0210 Message

This message must be sent in response to a Financial Transaction Request/0200 message. It carries the response by the recipient as to whether the request has been approved or denied.

(See appendix number 22)

Financial Transaction Advice/0220 Message

The Single Message System forwards a Financial Transaction Advice/0220 message to an affected Issuer when an authorization request occurs during Stand-In processing or a correction is processed to reverse a representment adjustment (valid for network-initiated adjustments only).

(See appendix number 23)

Financial Transaction Advice Response/0230 Message

This message must be sent in response to a Financial Transaction Advice/0220 message to indicate receipt of a Financial Transaction Advice/0220 message.

(See appendix number 24)

File Update Messages

Issuers use Issuer File Update/03xx messages to update individual data files or system parameter tables that the Authorization Platform maintains on their behalf. The Authorization Platform uses these data files to control the operation of standard and optional features that Members select when they participate in one or more of the network's program and service offerings.

ملاحظة: يجب اعتماد معاملات البطاقة ذات الشريحة في أجهزة الصراف الآلي عبر الإنترنت باستخدام رقم التعريف الشخصي. وسيتم رفض إشعار المعاملات المالية/ 0220 رسالة من أحد جهات القبول لمعاملات بطاقة الشريحة غير المتصلة بالإنترنت في جهاز الصراف الآلي بقيمة DE 39 (رمز الاستجابة) بقيمة 12 (معاملة غير صالحة).

يوضح الشكل التالي تدفق الرسائل القياسي لمعالجة المعاملات المالية التفاعلية:

(انظر الملحق رقم 20)

1. تقوم جهة القبول بالبدا برسالة طلب معاملة مالية/ 0200 إلى نظام الرسالة الواحدة.
2. يقوم نظام الرسالة الواحدة بإعادة توجيه رسالة طلب المعاملة المالية/ 0200 إلى جهة الإصدار.
3. تقوم جهة الإصدار بإنشاء رسالة استجابة لطلب المعاملة المالية/ 0210 وإرسالها إلى نظام الرسالة الواحدة.
4. يقوم نظام الرسالة الواحدة بإعادة توجيه رسالة استجابة طلب المعاملة المالية/ 0210 إلى جهة القبول.

تسرد المعلومات التالية تعريفات جميع رسائل ISO 8583-1993 المعاملات المالية/ 02xx المدعومة على الشبكة.

طلب معاملة مالية/ رسالة 0200

تُستخدم هذه الرسالة لطلب الموافقة على معاملة، وفي حالة الموافقة عليها، ستسمح بتطبيق البيانات المالية للمعاملة على حساب حامل البطاقة لإصدار فاتورة أو بيان.

(انظر الملحق رقم 21)

استجابة طلب معاملة مالية/ رسالة 0210

يجب إرسال هذه الرسالة ردًا على رسالة 0200 طلب معاملة مالية. ويحمل استجابة المستلم فيما إذا تمت الموافقة على الطلب أو رفضه.

(انظر الملحق رقم 22)

إشعار المعاملات المالية/ رسالة 0220

يقوم نظام الرسالة الفردية بإعادة توجيه رسالة "إشعار المعاملات المالية / 0220" إلى جهة الإصدار المتأثر عند حدوث طلب تفويض أثناء معالجة الاستعداد أو معالجة تصحيح لعكس تعديل التمثيل (صالح للتعديلات التي تبدأ من الشبكة فقط).

(انظر الملحق رقم 23)

استجابة إشعار المعاملات المالية/ رسالة 0230

يجب إرسال هذه الرسالة استجابةً لرسالة "إرشاد المعاملات المالية/ 0220" للإشارة إلى استلام رسالة "إرشاد المعاملات المالية/ 0220".

(انظر الملحق رقم 24)

رسائل تحديث الملف

تستخدم جهات الإصدار رسائل "تحديث ملف جهة الإصدار/ 03xx" لتحديث ملفات البيانات الفردية أو جداول معلمات النظام التي يحتفظ بها "منصة التفويض" نيابة عنهم. وتستخدم منصة التفويض ملفات البيانات هذه للتحكم في تشغيل الميزات القياسية والاختيارية التي يختارها الأعضاء عند مشاركتهم في برامج الشبكة وعروض الخدمة.

The Issuer File Update messages include:

- Issuer File Update Request/0302 – 1320
- Issuer File Update Request Response/0312 – 1312.

Issuer File Update Request/0302

The Issuer File Update Request/0302 message requests an Issuer File Update or inquiry action to be initiated on the Issuer’s behalf.

(See appendix number 25)

Issuer File Update Request Response/0312

The Issuer File Update Request Response/0312 message must be sent in response to an Issuer File Update Request/0302; it indicates the disposition of the Issuer File Update Request/0302 message.

(See appendix number 26)

About Reversal Messages—Dual Message System Processing

Reversal/04xx messages include:

- Reversal Request/0400
- Reversal Request Response/0410
- Reversal Advice/0420
- Reversal Advice Response/0430

Reversal Request/0400

Reversal Request/0400 messages are generated on the dual message system by an Acquirer when the Acquirer is unable to deliver an Issuer’s Authorization Request Response/0110 to a Merchant. Merchants also initiate a Reversal Request/0400 message to cancel the full or partial amount of the original authorization amount.

The Reversal Request/0400 message reverses fully or partially an earlier authorization request.

(See appendix number 27)

Reversal Request Response/0410

The Reversal Request Response/0410 message is sent in response to a Reversal Request/0400 message and denotes the disposition of the Reversal Request/0400 message.

(See appendix number 28)

Reversal Advice/0420

The Reversal Advice/0420 message fully reverses a previous Authorization Request/0100 – 1100. It advises an Issuer of a Reversal Request/0400 responded to by the Authorization Platform.

The Authorization Platform may generate this message:

- on detection of an exception condition while processing a previous Authorization Request Response/0110 message; or
- when an Issuer is unavailable to respond a Reversal Request/0400 or is delayed in providing a Reversal Request Response/0410 message.

(See appendix number 29)

تتضمن رسائل تحديث ملف جهة الإصدار ما يلي:

- طلب تحديث ملف جهة الإصدار/ 0302 – 1320.
- استجابة طلب تحديث ملف جهة الإصدار/ 0312 – 1312.

طلب تحديث ملف جهة الإصدار/ 0302

تتطلب رسالة تحديث ملف جهة الإصدار/ 0302 بدء إجراء استعلام أو تحديث ملف جهة الإصدار نيابةً عن جهة الإصدار.

(انظر الملحق رقم 25)

استجابة طلب تحديث ملف جهة الإصدار/ 0312

يجب إرسال استجابة طلب تحديث ملف جهة الإصدار/ 0312 استجابةً لطلب تحديث ملف جهة الإصدار/

0302 ؛ ويشير إلى التصرف في رسالة طلب تحديث ملف جهة الإصدار/ 0302

(انظر الملحق رقم 26)

حول إلغاء الرسائل - معالجة نظام الرسائل المزدوجة

تتضمن رسائل الإلغاء/ 04xx ما يلي:

- طلب الإلغاء / 0400.
- رد طلب الإلغاء / 0410.
- نصيحة الإلغاء / 0420.
- إستجابة نصيحة الإلغاء / 0430.

طلب الإلغاء/ 0400

يتم إنشاء رسائل طلب الإلغاء/ 0400 على نظام الرسائل المزدوجة من قبل جهة القبول عندما يتعذر على جهة القبول تسليم استجابة طلب التفويض/ 0110 من جهة الإصدار إلى التاجر. ويقوم التاجر أيضًا ببدء رسالة طلب التراجع/ 0400 لإلغاء المبلغ الكامل أو الجزئي لمبلغ التفويض الأصلي.

تعكس رسالة طلب الإلغاء / 0400 طلب تفويض سابق كليًا أو جزئيًا.

(انظر الملحق رقم 27)

رد طلب الإلغاء/ 0410

يتم إرسال رسالة استجابة طلب الإلغاء/ 0410 ردًا على رسالة طلب الإلغاء/ 0400، وتشير إلى التخلص من رسالة طلب الإلغاء/ 0400.

(انظر الملحق رقم 28)

إشعار الإلغاء/ 0420

تعكس رسالة “إشعار الإلغاء/ 0420” طلب التفويض السابق/ 0100-1100 بالكامل. وتنصح جهة إصدار طلب الإلغاء/ 0400 الذي تم الرد عليه بواسطة منصة التفويض.

قد تنشئ منصة التفويض هذه الرسالة في الحالات التالية:

- عند الكشف عن شرط استثناء أثناء معالجة رسالة سابقة لطلب استجابة تفويض/ 0110 .
- عندما لا تتمكن جهة الإصدار من الرد على طلب الإلغاء/ 0400 أو يتأخر في تقديم استجابة طلب الإلغاء/ 0410.

(انظر الملحق رقم 29)

Reversal Advice Response/0430

The Reversal Advice Response/0430 message must be sent in response to a Reversal Advice/0420 message to acknowledge positive receipt of that message.

(See appendix number 30)

About Reversal Messages—Single Message System Processing

Reversal Advice/04xx Messages

Reversal advice/04xx messages reverse the impact of a previous Authorization/01xx or Financial Transaction/02xx message.

These messages fall under the general category of advice messages, and as such, are subject to the Authorization Platform Guaranteed Advice Delivery procedures that are standard for all advice messages.

If the Authorization Platform cannot immediately deliver these messages to their intended destination, the Authorization Platform automatically assumes the responsibility for storing them in the store-and-forward (SAF) System. When network delivery-point communication has been reestablished and the receiver requests delivery of the advice messages, the Authorization Platform forwards them to the proper destination.

The reversal advice message and its response can be designated Acquirer (0420/0430 sequence) or Issuer (0422/0432 sequence), and the Single Message System enables several usages within these categories.

(See appendix number 31)

The Acquirer Reversal Advice/0420 message reverses (partially or wholly) an earlier Authorization/01xx or Financial Transaction/ 02xx message. The acquirer processing system usually generates this message upon detection of a malfunction at the point-of-interaction (POI).

The Single Message System sends the message to an issuer upon receipt of a reversal or upon receipt of an adjustment from the acquirer. For settlement purposes, this message contains “force-post” information. Thus, the reversal will be processed regardless of message receipt acknowledgment.

The Acquirer Reversal Advice/0420 message has five uses:

- Standard Reversal Advice—most commonly used to correct or cancel the amount dispensed or authorized from the original terminal request.
- Time-out-Induced Reversal Advice-Acquirer (before settlement)—available to acquirers when the Financial Transaction Request Response/0210 - 1210 does not arrive back to the acquirer in the required time.
- Time-out-Induced Reversal Advice-Issuer - available to inform issuers that the Single Message System did not receive a Financial Transaction Response/0210 - 1210 from the issuer in the required time interval (time-out condition) or that there were failed edit checks.
- Acquirer Reversal Advice—Exception, System Initiated (after settlement)—Authorized representatives of an acquirer, an issuer, or the National Scheme Operator use Single Message Transaction Manager to submit an adjustment, chargeback, or representment, which the Single Message System passes on to the issuer in the form of an Acquirer Reversal Advice/0420 - 1420 message.
- Online Exception—the following apply:
 - After settlement—available to acquirers to submit adjustments and representments after the settlement day of the original transaction. This abbreviated Acquirer

رد إشعار الإلغاء/ 0430

يجب إرسال رسالة رد إشعار الإلغاء/ 0430 ردًا على رسالة عكس الإشعار/ 0420 للإقرار بالاستلام الإيجابي لتلك الرسالة.

(انظر الملحق رقم 30)

حول إلغاء الرسائل - معالجة نظام رسالة واحدة

إلغاء نصيحة / رسائل 04xx

تعكس رسائل إشعار الإلغاء/ 04xx تأثير رسالة التفويض/ 01xx السابقة أو المعاملة المالية/ 02xx.. تندرج هذه الرسائل ضمن الفئة العامة لرسائل الإشعار، وبالتالي فهي تخضع لإجراءات تسليم المشورة المضمونة لمنصة التفويض، والتي تعد قياسية لجميع رسائل الإرشاد.

وإذا لم تتمكن منصة التفويض من تسليم هذه الرسائل على الفور إلى وجهتها المقصودة، فإن منصة التفويض تتحمل تلقائيًا مسؤولية تخزينها في نظام التخزين وإعادة التوجيه (SAF). عندما يتم إعادة إنشاء اتصالات نقطة تسليم الشبكة ويطلب المستلم تسليم رسائل الإرشاد، يقوم نظام التفويض بإعادة توجيهها إلى الوجهة الصحيحة.

يمكن تعيين رسالة إشعار الإلغاء واستجابتها “جهة استحواذ” (تسلسل 0420/0430) أو جهة إصدار (تسلسل 0422/0432)، ويتيح “نظام الرسالة الواحدة” استخدامات عديدة ضمن هذه الفئات.

(انظر الملحق رقم 31)

تعكس رسالة إشعار إلغاء جهة القبول/ 0420 (جزئيًا أو كليًا) تفويضًا سابقًا/ 01xx أو رسالة معاملة مالية/ 02xx. عادةً ما يُنشئ نظام معالجة القابل هذه الرسالة عند اكتشاف عطل في نقطة التفاعل (POI).

يرسل نظام الرسالة الواحدة هذه الرسالة إلى جهة الإصدار عند استلام عكس أو عند استلام تعديل من القابل. ولأغراض التسوية، فإن هذه الرسالة تحتوي على معلومات “إرسال القوة”. وبالتالي، سيتم معالجة الإلغاء بغض النظر عن إشعار استلام الرسالة.

تحتوي رسالة إشعار إلغاء جهة القبول / 0420 على خمسة استخدامات:

- إشعارات الإلغاء القياسية - الأكثر استخدامًا لتصحيح أو إلغاء المبلغ الذي تم الاستغناء عنه أو المصرح به من طلب المحطة الأصلي.
- إشعار الإلغاء الناجم عن انقضاء المهلة - جهة القبول (قبل التسوية) - متاح للقابلين عندما لا تصل استجابة طلب المعاملة المالية / 0210 - 1210 إلى القابل في الوقت المطلوب.
- إشعار الإلغاء الناجم عن انقضاء المهلة - جهة الإصدار - متاح للإبلاغ جهات الإصدار بأن نظام الرسالة الواحدة لم يتلق استجابة المعاملات المالية/ 0210 - 1210 من جهة الإصدار في المدة الزمنية المطلوبة (شرط المهلة) أو أن هناك فشلًا في تحرير الصكوك.
- إشعار إلغاء جهة القبول - الاستثناء أو بدء النظام (بعد التسوية) - يستخدم الممثلون المعتمدون، للقابل أو جهة الإصدار أو مشغل شبكة الدفع المحلية، مدير معاملة الرسالة الواحدة لإرسال تعديل أو رد المبالغ المدفوعة أو تمثيل، والذي يمرره نظام الرسائل الفردية لجهة الإصدار في شكل إشعار إلغاء جهة القبول/ 0420 - 1420.
- استثناء عبر الإنترنت - ينطبق ما يلي:
 - بعد التسوية - يكون متاح للقابلين لتقديم التسويات والإقرارات بعد يوم التسوية للمعاملة الأصلية. ويمكن إرسال هذه الرسالة المختصرة لعكس جهة القبول/ 0420 - 1420 إلى نظام

- Reversal Advice/0420 – 1420 message may be submitted to the Single Message System through the acquirer’s online processing facility, which the Single Message System will pass to the issuer as an Acquirer Reversal Advice/0420 message.
- For Instant Credit Transactions identified by DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) value 28, the Single Message System will support same-day reversals in online exceptions.

About Network Management Messages

The Authorization Platform, Member processing systems (CPSs), Acquirer processing systems (APSs), Issuer processing systems (IPs), and intermediate network facilities (INFs) use Network Management/08xx messages to coordinate system or network events or tasks. These systems also use these messages to communicate network status conditions.

- Network Management/08xx messages include:
- Network Management Request/0800
- Network Management Request Response/0810
- Network Management Advice/0820

Typical uses of Network Management/08xx messages include:

Sign on to and sign off from the Authorization Platform 1804 request and 1814 response for sign on and off

- Perform a Network Connection Status to the National Scheme Operator
- Perform Host Session Activation or Deactivation
- Perform encryption key management

The Authorization Platform routes Network Management/08xx messages from an originator to a receiver and, in general, does not distinguish whether the originator or receiver is an Issuer or an Acquirer.

Network Management Request/0800

The Network Management Request/0800 message controls the network by communicating or coordinating system condition or system security. DE 70, a mandatory data element in all Network Management/08xx messages, determines specific Network Management/08xx message functions.

(See appendix number 32)

Network Management Request Response/0810

The Network Management Request Response/0810 message must be sent in response to a Network Management Request/0800 to acknowledge positive receipt of that message. (See appendix number 33)

Network Management Advice/0820

The Network Management Advice/0820 – 1820 message advises of a previous Network Management Request/0800 – 1800 message. There is no response to a Network Management Advice/0820 – 1820 message.

(See appendix number 34)

5.1.3 Authorization Processing Functionality

Accessing the Authorization Platform

To process authorization activity, Acquirers and Issuers must access the Interchange

- الرسائل المفردة من خلال مرفق المعالجة عبر الإنترنت الخاص بالقابل، والذي سينقله نظام الرسالة الفردية إلى جهة الاصدار كرسالة عكس جهة القبول / 0420.
- بالنسبة للمعاملات الائتمانية الفورية المحددة بواسطة DE 3 (رمز المعالجة) ، قيمة الحقل الفرعي 1 (رمز نوع معاملة حامل البطاقة) 28، سيدعم نظام الرسائل الفردية عمليات الإلغاء في نفس اليوم في الاستثناءات عبر الإنترنت.

حول رسائل إدارة الشبكة

تستخدم منصة التفويض، وأنظمة معالجة الأعضاء (CPSs) وأنظمة معالجة جهة القبول (APS) وأنظمة معالجة جهة الاصدار (IPs) ومرافق الشبكة الوسيطة (INFs) رسائل إدارة الشبكة / 08 xx لتنسيق أحداث أو مهام النظام أو الشبكة. وتستخدم هذه الأنظمة أيضًا هذه الرسائل للتواصل مع حالات حالة الشبكة.

تتضمن رسائل إدارة الشبكة / 08 xx ما يلي:

- طلب إدارة الشبكة / 0800.
- استجابة طلب إدارة الشبكة / 0810.
- نصائح إدارة الشبكة / 0820.

تشمل الاستخدامات النموذجية لإدارة الشبكة / رسائل 08xx ما يلي:

- تنفيذ حالة اتصال الشبكة لمشغل شبكة الدفع المحلية.
- إجراء تنشيط جلسة المضيف أو إلغاء التنشيط.
- أداء إدارة مفتاح التشفير.

تقوم منصة التفويض بتوجيه رسائل إدارة الشبكة / 08xx من المنشئ إلى المستلم، وبشكل عام، لا تميز ما إذا كان المنشئ أو المستلم هو جهة الاصدار أو جهة القبول.

طلب إدارة الشبكة / 0800

تتحكم رسالة طلب إدارة الشبكة / 0800 في الشبكة عن طريق الاتصال أو تنسيق حالة وأمان النظام. ويحدد DE 70، عنصر البيانات الإلزامي لجميع رسائل إدارة الشبكة / 08xx، وظائف محددة لإدارة الشبكة / 08xx للرسائل.

(انظر الملحق رقم 32)

استجابة طلب إدارة الشبكة / 0810

يجب إرسال رسالة استجابة طلب إدارة الشبكة / 0810 استجابةً لطلب إدارة الشبكة / 0800 للإقرار باستلام إيجابي لتلك الرسالة.

(انظر الملحق رقم 33)

نصيحة إدارة الشبكة / 0820

تنصح رسالة إرشادات إدارة الشبكة / 0820 - 1820 بطلب إدارة شبكة السابق / 0800 - 1800 رسالة. لا توجد استجابة لرسالة "نصيحة إدارة الشبكة" / 0820 - 1820.

(انظر الملحق رقم 34)

3.1.5. وظيفة معالجة التفويض

الوصول إلى منصة التفويض

لمعالجة نشاط التفويض، يجب على جهات الاصدار وجهات القبول الوصول إلى نظام التبادل. هذا النظام

System. This network is the path by which they send and receive authorization messages and related data. Selecting a particular authorization processing access method depends on a number of factors, including:

- Physical installations present at the point-of-interaction and at the Member site
- Volume of incoming and outgoing authorizations
- Member location

For help in selecting an appropriate access method, contact an Implementation Services specialist.

Acquirer Methods

Online host-to-Member Interface Processor (MIP) access is available to Acquirers. There are several confirmations for connectivity to a Member Interface Processor (MIP) or Member Interface Processor (MIP)s for online access.

Acquirer Online—Direct Host to Member Interface Processor (MIP) Connectivity

To have direct connectivity to a Member Interface Processor (MIP), the Acquirer must have a host computer that can support this type of connectivity.

Issuer Methods

Issuers may choose the online host-to-Member Interface Processor (MIP) access to the NUMO Network.

Online Host-to-Member Interface Processor (MIP) Access

Online host-to-Member Interface Processor (MIP) Issuers receive authorization requests from the Authorization Platform via a Member Interface Processor (MIP) connected to the Issuer's host. These Issuers format and return authorization request responses directly using the prescribed message types.

5.1.4 Authorization Processing Flows

5.1.4.1 Basic Authorization Flow

Although the authorization process contains many variables for routing and authorizing, it is helpful to have an understanding of the basic flow of an authorization request.

1. The Cardholder presents the Card to the Merchant for a face-to-face Transaction or provides the Card number, expiration date, name, and address when placing a mail, phone, or electronic commerce (e-commerce) order.
2. The Merchant forwards the Transaction to the Acquirer for approval.
3. The Acquirer requests authorization for the Transaction by generating an authorization request message. The authorization request travels through an Acquirer Member Interface Processor to the NUMO Network, through an Issuer Member Interface Processor (MIP), and then to the Issuer's host.
4. The Issuer returns an authorization response message to the Acquirer to indicate what action the Merchant should take for the Transaction. The authorization response travels through the NUMO Network to the Acquirer.
5. Acquirers for ATM should send an authorization acknowledgement message confirming receipt of the response.
6. The Acquirer responds to the Merchant.
7. The Merchant completes the Transaction according to the authorization response returned.

أو الشبكة، هو المسار الذي يتم من خلاله إرسال واستقبال رسائل التفويض والبيانات ذات الصلة. والذي تعتمد فيه تحديد طريقة وصول معالجة التفويض الخاصة على عدد من العوامل، بما في ذلك:

- التركيبات المادية الموجودة في نقطة التفاعل، وفي مواقع الأعضاء.
- حجم التفويضات الواردة والصادرة.
- موقع العضو

للمساعدة في تحديد طريقة وصول مناسبة، اتصل بالمختصين بخدمات التنفيذ.

طرق جهة القبول

يتوفر الوصول عبر الإنترنت إلى معالج واجهة المضيف إلى الأعضاء (MIP) للقابلين. وهناك العديد من التأكيدات للاتصال بمعالج واجهة الأعضاء (MIP) أو معالجات واجهة الأعضاء (MIP)s للوصول عبر الإنترنت.

جهة القبول عبر الإنترنت - اتصال مباشر من المضيف إلى معالج واجهة الأعضاء (MIP)

للحصول على اتصال مباشر بمعالج واجهة الأعضاء (MIP)، يجب أن يكون لدى جهة القبول جهاز كمبيوتر مضيف يمكنه دعم هذا النوع من الاتصال.

طرق جهة الاصدار

يجوز لجهات الاصدار اختيار الوصول عبر الإنترنت إلى معالج واجهة مضيف إلى عضو (MIP) إلى شبكة نمو.

الوصول عبر الإنترنت إلى معالج واجهة المضيف إلى عضو (MIP)

تتلقى جهات الإصدار معالج واجهة المضيف عبر الإنترنت (MIP) طلبات الترخيص من منصة التفويض عبر معالج واجهة العضو (MIP) المتصل بمضيف جهة الاصدار. وتقوم جهات الاصدار بتنسيق واستجابات طلب الإذن بالعودة مباشرة باستخدام أنواع الرسائل المحددة.

4.1.5 تدفقات معالجة التفويض

1.4.1.5 تدفقات التفويض الأساسي

على الرغم من أن عملية التفويض تحتوي على العديد من المتغيرات للتوجيه والتفويض، إلا أنه من المفيد فهم التدفق الأساسي لطلب التفويض.

1. يقوم حامل البطاقة، بتقديم البطاقة إلى التاجر لإجراء معاملة وجهًا لوجه، أو يقدم رقم البطاقة وتاريخ انتهاء الصلاحية والاسم والعنوان عند تقديم طلب عبر البريد أو الهاتف أو التجارة الإلكترونية (التجارة الإلكترونية).
2. يقوم التاجر بإعادة توجيه المعاملة إلى الجهة القابلة للموافقة عليها.
3. تطلب جهة القبول التفويض للمعاملة عن طريق إنشاء رسالة طلب تفويض. ثم ينتقل طلب التفويض عبر معالج واجهة عضو جهة القبول إلى شبكة نمو، عبر معالج واجهة عضو جهة الاصدار (MIP)، ثم إلى مضيف جهة الاصدار.
4. تقوم جهة الاصدار بإرجاع رسالة رد التفويض إلى جهة القبول للإشارة إلى الإجراء الذي يجب على التاجر اتخاذه من أجل المعاملة. وتنتقل استجابة التفويض عبر شبكة نمو إلى جهة القبول.
5. يجب على القابلين عن طريق أجهزة الصراف الآلي إرسال رسالة إقرار تفويض تؤكد استلام الرد.
6. تستجيب جهة القبول على التاجر.
7. يكمل التاجر المعاملة وفقًا لاستجابة التفويض التي تم إرجاعها.

5.1.4.2 Variations on the Basic Authorization Flow

A. Issuer Is Online but the Transaction Cannot Follow the Primary Path

If a Transaction involving an online Issuer cannot follow the basic authorization flow, it follows a secondary path or a tertiary path.

If the Authorization Platform cannot route these Transactions via the primary path to the Issuer, it may result in a response indicating the requested service is not available. This can occur for any of the following services:

- Transactions that contain an Account Status Inquiry Service receive a response of service not available.
- Transactions that contain an authorization request and an AVS request—the authorization request receives the appropriate authorization response and the AVS request receives a response of service not available.
- Balance inquiry Transactions receive a response of service not available.
- PIN management Transactions receive a response of service not available.
- Funding Transactions at an ATM receive a response of service not available.
- Refund Transactions receive a response of service not available.

B. Secondary Path for Online Members—Stand-In System Processing

If any of the following conditions apply for online Issuers that support the Stand-In System as their secondary path, the system routes the Transaction to Stand-In processing:

- The Issuer is not signed in.
- The Transaction could not be delivered to the Issuer.
- The Issuer does not respond with an Authorization Request Response/0110-1110 message in the allotted amount of time, causing a time out at the acquiring Member Interface Processor (MIP). For more information about response times, refer to Routing Timer Values.
- The Issuer's response message contains invalid formatting or information resulting in an Issuer edit error.

C. Secondary Path for Online Members—To Stand-In System Processing

1. After receiving the Merchant request for authorization, the Acquirer generates an authorization request, which travels through the NUMO Network.
2. The NUMO Network, unable to route the authorization request to the online Issuer, routes it to Stand-In processing.
3. Stand-In processing generates an authorization response, based on the Issuer's parameters. Stand-In processing also generates authorization advice messages, as appropriate, and stores them in a store-and-forward (SAF) queue.
4. The NUMO Network routes the Stand-In authorization response to the Acquirer.
5. Online Acquirers may send an authorization acknowledgement message confirming receipt of the response.
6. When Issuer connectivity is re-established, the Issuer will retrieve the SAF messages generated by Stand-In processing to adjust Cardholder available-to-buy positions appropriately.

2.4.1.5. الاختلافات في تدفقات التفويض الأساسي

أ. جهة الإصدار متصلة، ولكن لا يمكن للمعاملة أن تتبع المسار الأساسي

إذا لم تتمكن المعاملة التي تتضمن جهة إصدار عبر الإنترنت من اتباع مسار التفويض الأساسي، فإنها تتبع مسارًا ثانويًا أو مسارًا ثالثًا.

إذا لم تتمكن منصة التفويض من توجيه هذه المعاملات عبر المسار الأساسي إلى جهة الإصدار، فقد يؤدي ذلك إلى استجابة تشير إلى أن الخدمة المطلوبة غير متوفرة. يمكن أن يحدث ذلك للخدمات التالية:

- المعاملات التي تحتوي على خدمة الاستعلام عن حالة الحساب تتلقى ردًا على الخدمة غير متوفرة.
- المعاملات التي تحتوي على طلب تفويض وطلب AVS - يتلقى طلب التفويض استجابة التفويض المناسبة ويتلقى طلب AVS استجابة الخدمة غير المتاحة.
- معاملات الاستعلام عن الرصيد تتلقى ردًا على الخدمة غير متوفرة.
- معاملات إدارة رقم التعريف الشخصي تتلقى استجابة الخدمة غير متوفرة.
- معاملات التمويل في أجهزة الصراف الآلي تتلقى استجابة الخدمة غير متوفرة.
- معاملات الاسترداد تتلقى استجابة الخدمة غير متوفرة.

ب. المسار الثانوي للأعضاء المتصلين عبر الإنترنت - معالجة النظام الاحتياطية

إذا تم تطبيق أي من الشروط التالية على جهات الإصدار عبر الإنترنت التي تدعم النظام الاحتياطي كمسار ثانوي، يقوم النظام بتوجيه المعاملة إلى المعالجة الاحتياطية:

- لم تقم جهة الإصدار بتسجيل الدخول.
- لا يمكن تسليم المعاملة إلى جهة الإصدار.
- لا تستجيب جهة الإصدار لرسالة استجابة طلب التفويض / 0110-1110 في الفترة الزمنية المخصصة، مما يتسبب في انقضاء المهلة في الحصول على معالج واجهة العضو (MIP) للمزيد من المعلومات حول أوقات الاستجابة، راجع قيم مؤقت التوجيه.
- تحتوي رسالة استجابة جهة الإصدار على تنسيق أو معلومات غير صالحة تؤدي إلى خطأ في تحرير جهة الإصدار.

ج. المسار الثانوي للأعضاء المتصلين عبر الإنترنت - لمعالجة النظام الاحتياطية

1. بعد تلقي طلب التاجر للحصول على تفويض، تقوم جهة القبول بإنشاء طلب تفويض، والذي ينتقل عبر شبكة نمو.
2. شبكة نمو غير قادرة على توجيه طلب التفويض إلى جهة الإصدار عبر الإنترنت، وتوجهه إلى المعالجة الاحتياطية.
3. تؤدي المعالجة الاحتياطية إلى استجابة التفويض، بناءً على معلمات جهة الإصدار. تؤدي المعالجة الاحتياطية أيضًا إلى إنشاء رسائل إرشادات التفويض، حسب الاقتضاء، وتخزينها في قائمة انتظار التخزين وإعادة التوجيه (SAF).
4. تقوم شبكة نمو بتوجيه استجابة التفويض الاحتياطي إلى جهة القبول.
5. قد ترسل جهات القبول عبر الإنترنت رسالة إقرار تفويض تؤكد استلام الرد.
6. عند إعادة إنشاء اتصال بجهة الإصدار، ستقوم جهة الإصدار باسترداد رسائل SAF التي تم إنشاؤها من خلال المعالجة الاحتياطية لتعديل أوضاع حامل البطاقة المتاحة للشراء بشكل مناسب.

D. No Secondary Path for Online Members If a secondary authorization path does not exist for an Issuer or is not allowed based on program or service rules and the online Issuer does not respond or responds late to an Authorization Request/0100 – 1100 message, which causes a time out, the Authorization Platform responds to the Acquirer with a decline response.

E. No Secondary Path for Online Members—No Issuer Response

1. The Acquirer sends the Authorization Request/0100 – 1100 message to the Authorization Platform, and the Authorization Platform forwards the Authorization Request/0100 – 1100 message to the Issuer.
2. The Authorization Platform does not receive the Issuer's Authorization Request Response/0110 within the response time allowed for the Issuer.
3. The Authorization Platform sends the Authorization Request Response/0110 to the Acquirer where DE 39 (Response Code) = 91 (Issuer Authorization System or Issuer Inoperative).
4. The Authorization Platform sends a Reversal Advice/0420 message containing the following values to the Issuer because no Issuer response is received:
 - DE 39 = 82 (Time out at Issuer)
 - DE 60, subfield 1 = 402 (Network advice: IPS time-out error)
5. When the Issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.

F. No Secondary Path for Online Members—Late Issuer Response

1. The Acquirer sends the Authorization Request/0100 – 1100 message to the Authorization Platform, and the Authorization Platform forwards the Authorization Request/0100 – 1100 message to the Issuer.
2. The Authorization Platform does not receive the Authorization Request Response/0110 message within the time limits from the Issuer.
3. The Authorization Platform generates an Authorization Request Response/0110 message where DE 39 (Response Code) = 91 (Issuer Authorization System or Issuer Inoperative) and forwards it to the Acquirer.
4. The Authorization Platform sends a Reversal Advice/0420 message containing the following values to the Issuer because no Issuer response is received:
 - DE 39 = 82 (Time out at Issuer)
 - DE 60, subfield 1 = 402 (Network advice: IPS time-out error)
5. When the Issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.
6. The Authorization Platform receives a late Authorization Request Response/0110 – 1110 message from the Issuer.
7. The Authorization Platform sends an Authorization Response Negative Acknowledgement/0190 message to the Issuer, indicating it has no record of a corresponding Authorization Request/0100 – 1100 message.

NOTE: A response is not necessary from the Issuer after the Authorization Platform sends an Authorization Response Negative Acknowledgement/0190 message.

د. لا يوجد مسار ثانوي للأعضاء المتصلين عبر الإنترنت في حالة عدم وجود مسار تفويض ثانوي لإحدى جهات الإصدار، أو لم يكن مسموحًا به استنادًا إلى قواعد البرنامج أو الخدمة، ولا تستجيب جهة الإصدار عبر الإنترنت أو تستجيب متأخرًا لطلب التفويض / 0100-1100 رسالة، مما يتسبب في انقضاء المهلة المحددة، فإن منصة التفويض تستجيب للقابل باستجابة رفض.

- ه. لا يوجد مسار ثانوي للأعضاء المتصلين عبر الإنترنت - لا توجد استجابة من جهة الإصدار
1. ترسل جهة القبول رسالة طلب التفويض / 0100-1100 إلى منصة التفويض، وتقوم منصة التفويض بإعادة توجيه رسالة طلب التفويض / 0100 - 1100 إلى جهة الإصدار.
 2. لا تتلقى منصة التفويض استجابة جهة الإصدار لطلب التفويض / 0110 خلال وقت الاستجابة المسموح به لجهة الإصدار.
 3. ترسل منصة التفويض استجابة طلب التفويض / 0110 إلى جهة القبول حيث DE 39 (رمز الاستجابة) = 91 (نظام تفويض جهة الإصدار أو جهة الإصدار لا تعمل).
 4. ترسل منصة التفويض رسالة إلغاء نصيحة / 0420 تحتوي على القيم التالية إلى جهة الإصدار لأنه لم يتم تلقي أي استجابة من جهة الإصدار:
 - DE 39 = 82 (الوقت المستقطع عند جهة الإصدار)
 - DE 60 2، الحقل الفرعي 1 = 402 (نصيحة الشبكة: خطأ انتهاء مهلة IPS)
 5. عندما تتلقى جهة الإصدار رسالة "نصيحة الإلغاء / 0420"، يجب أن يقوم بإنشاء رسالة "استجابة نصيحة الإلغاء" / 0430 للإقرار باستلام رسالة "إشعار الإلغاء" / 0420.

- و. لا يوجد مسار ثانوي للأعضاء المتصلين عبر الإنترنت - استجابة جهة الإصدار المتأخرة
1. ترسل جهة القبول رسالة طلب التفويض / 0100-1100 إلى منصة التفويض، وتقوم منصة التفويض بإعادة توجيه رسالة طلب التفويض / 0100 - 1100 إلى جهة الإصدار.
 2. لا تتلقى منصة التفويض رسالة "استجابة طلب التفويض / 0110" خلال الحدود الزمنية من جهة الإصدار.
 3. تقوم منصة التفويض بإنشاء رسالة استجابة لطلب التفويض / 0110 حيث DE 39 (رمز الاستجابة) = 91 (نظام تفويض جهة الإصدار أو جهة الإصدار لا تعمل). وإعادة توجيهه إلى جهة القبول.
 4. ترسل منصة التفويض رسالة إلغاء نصيحة / 0420 تحتوي على القيم التالية إلى جهة الإصدار لأنه لم يتم تلقي أي استجابة من جهة الإصدار:
 - DE 39 = 82 (الوقت المستقطع عند جهة الإصدار)
 - DE 60 2، الحقل الفرعي 1 = 402 (نصيحة الشبكة: خطأ انتهاء مهلة IPS)
 5. عندما تتلقى جهة الإصدار رسالة "نصيحة الإلغاء / 0420"، يجب أن يقوم بإنشاء رسالة "استجابة نصيحة الإلغاء" / 0430 للإقرار باستلام رسالة "إشعار الإلغاء" / 0420.
 6. تتلقى منصة التفويض استجابة متأخرة لطلب التفويض / 0110 - 1110 من جهة الإصدار.
 7. ترسل منصة التفويض رسالة إقرار سلبي لاستجابة التفويض / 0190 إلى جهة الإصدار، تشير إلى عدم وجود سجل لرسالة طلب التفويض / 0100-1100 المقابلة.

ملاحظة: الرد ليس ضروريًا من جهة الإصدار بعد أن ترسل منصة التفويض رسالة إقرار سلبي لاستجابة التفويض / 0190.

5.1.4.3 Routing Timer Values—Issuer Response and Acquirer Minimum Wait Times

(Category C)

Routing timer values that apply to Acquirer-generated Authorization Request/0100 – 1100, Authorization Advice/0120, and Reversal Request/0400 messages are listed in the table below.

The Acquirer must ensure that its host does not apply authorization response wait time parameters that time out before the minimum authorization response wait time has elapsed. The Issuer must ensure that its host responds to the message within the minimum response time, or the Transaction will time out and be forwarded to an alternative authorization host specified by the Issuer.

(See appendix number 35)

5.2 The Clearing System

This section describes Interchange System functionality relating to the clearing of Transactions.

Clearing is the process by which Transaction data is exchanged between Members (also called presentment). The Clearing System is a centralized clearing facility owned and operated by the National Scheme Operator for the daily processing and routing of financial Transactions between the National Scheme Operator and its Members. The Clearing System accepts the data, edits it, assesses the appropriate fees, and routes it to the appropriate receiver. Clearing messages do not actually exchange or transfer funds.

- The Clearing System manages the clearing processing of Transactions. Its functions include:
- Editing Transactions for adherence to network processing standards.
- assessing interchange fees, and calculating settlement values for each Transaction.
- Routing clearing Transactions (messages) to the appropriate Member or vendor.
- Providing acknowledgement messages to advise the originator of the Transaction that the Clearing System received the Transaction.
- Providing notification messages to advise the receiver of the Transaction that the Clearing System has processed clearing Transactions for that receiver.
- Providing error messages and reports to advise the originator of an invalid Transaction that the Clearing System rejected the Transaction.
- Creating reconciliation reports.
- Providing summarized settlement request information to the Settlement System.
- Providing clearing information to other Interchange System components such as the billing system, and the data storage system.
- Providing optional on-behalf services.

5.2.1 Participation in the Clearing System

The Member responsible for a Transaction as an Issuer or as an Acquirer is permitted to participate in the clearing and settlement of the Transaction.

From the data provided in clearing, the Clearing System derives the amounts for settlement. Settlement provides Acquirers with the funds to reimburse their card acceptors and collects funds from Issuers.

Members also use clearing data for some of their back-office processes, including posting to Cardholder accounts. Members that issue Cards and Members contracting with card acceptors to accept cards must perform clearing to exchange Transaction data.

3.4.1.5 قيم مؤقتة التوجيه - استجابة جهة الاصدار، والحد الأدنى لمهلة انتظار جهة القبول

(الفئة ج)

يتم سرد قيم مؤقتة التوجيه التي تنطبق على رسائل طلب التفويض التي أنشأتها جهة القبول/ 0100-1100 وإشعار التفويض/ 0120 ورسائل طلب الإلغاء/ 0400 في الجدول أدناه.

يجب أن تتحقق جهة القبول من أن مضيفه لا يطبق معلمات مهلة انتظار أو مهلة استجابة التفويض التي تنتهي مدته قبل انقضاء الحد الأدنى لمهلة انتظار استجابة التفويض.

يجب أن تتحقق جهة الاصدار من أن مضيفه يستجيب للرسالة في خلال الحد الأدنى من مهلة الاستجابة، أو ستنتهي مهلة انتظار المعاملة وإعادة توجيهها إلى مضيف تفويض بديل محدد من قبل جهة الاصدار.

(انظر الملحق رقم 35)

2.5. نظام المقاصة

يصف هذا القسم وظائف نظام التبادل المتعلقة بتصفية المعاملات.

المقاصة هي العملية التي يتم من خلالها تبادل بيانات المعاملة بين الأعضاء (وتسمى أيضًا التقديم). ونظام المقاصة هو وسيلة مقاصة مركزية يملكها ويديرها مشغل شبكة الدفع المحلية للمعالجة اليومية، وتوجيه المعاملات المالية بين مشغل شبكة الدفع المحلية وأعضائه. ويقبل نظام المقاصة البيانات ويقوم بتحريرها، ويقيم الرسوم المناسبة، ويوجهها إلى المستلم المناسب. رسائل المقاصة لا تقوم في الواقع بتبادل الأموال أو تحويلها.

يدير نظام المقاصة معالجة مقاصة المعاملات، وتشمل وظائفه:

- تحرير المعاملات للالتزام بمعايير معالجة الشبكة.
- تقييم رسوم التبادل وحساب قيم التسوية لكل معاملة.
- توجيه معاملات (رسائل) المقاصة إلى العضو أو البائع المناسب.
- تقديم رسائل إقرار، لإبلاغ منشئ المعاملة بأن نظام المقاصة قد استلم المعاملة.
- تقديم رسائل إعلام، لإعلام متلقي المعاملة بأن نظام المقاصة قد عالج معاملات المقاصة لهذا المستلم.
- تقديم رسائل خطأ وتقارير، لإبلاغ منشئ المعاملة غير الصالحة بأن نظام المقاصة رفض المعاملة.
- إنشاء تقارير التسوية.
- تقديم معلومات موجزة عن طلب التسوية إلى نظام التسوية.
- توفير معلومات المقاصة لمكونات نظام التبادل الأخرى مثل نظام الفوترة ونظام تخزين البيانات.
- تقديم خدمات نيابة اختيارية.

1.2.5. المشاركة في نظام المقاصة

يُسمح للعضو المسؤول عن المعاملة بصفته جهة إصدار أو جهة استحواذ بالمشاركة في مقاصة وتسوية المعاملة.

من البيانات المقدمة في المقاصة، يقوم نظام المقاصة بتحديد المبالغ الذي يجب تسويتها، وتزود التسوية جهات القبول بالأموال لتعويض القابليين للبطاقات وتجمع الأموال من جهات الإصدار.

يستخدم الأعضاء أيضًا بيانات المقاصة لبعض عمليات المكتب الخلفي، بما في ذلك الترحيل إلى حسابات حامل البطاقة. ويجب على جهات الاصدار، والأعضاء الذين يتعاقدون مع القابليين للبطاقات لقبول البطاقات، إجراء المقاصة لتبادل بيانات المعاملة.

5.2.2 Clearing Messages

The clearing process begins when the Acquirer presents Transaction data to the Issuer for the first time, for posting to the Cardholder's account. After the first presentment of the Transaction, the Issuer may determine that the Transaction is invalid. The Issuer has the right to charge back the Transaction when chargeback procedures specifically allow the Issuer to return the Transaction to the Acquirer for possible remedy.

For each Transaction between Issuer and Acquirer, the following cycles allow presentment, retrieval, and chargeback processing:

- First presentment consists of one step—from the Acquirer to the Issuer.
- The retrieval process consists of two steps—retrieval request and fulfillment.
- The chargeback cycle consists of two steps: chargeback and second presentment.

If necessary, an arbitration case may be filed following second presentment, by either party. The Clearing System maintains a chargeback history file, which stores selected information from all incoming chargeback Transactions that the Clearing System accepts. The purpose of the chargeback history file is to track chargeback cycles and documentation that Members send. The Clearing System edits chargeback messages against the chargeback history file to validate cycle sequence, time frames, and documentation requirements.

Clearing messages contain the following data:

- Message Type Identifier (MTI): Identifies the purpose of the message, such as Financial, Administrative, or Fee Billing. The MTI identifies the general ISO message type. Valid MTIs include (Presentment), (Chargeback), (Administrative), and (Fee Collection).
- Two bit-maps: A series of binary digits (bits) that indicate the presence or absence of data elements.
- Data elements: Message elements, defined within the ISO 8583-1993 specification that may contain data.
- Private data subelements: Message elements defined by the National Scheme Operator to support data that is not defined within the ISO 8583-1993 specification.

(See appendix number 36)

The Data Element (DE) 24 (Function Code) in each message indicates the Transaction's primary type or function, and the DE 25 (Message Reason Code) indicates the primary reason for the Transaction.

First Presentment Messages

An Acquirer will initiate a First Presentment to advise the Issuer or its Service Provider that a financial Transaction was completed on its behalf. The First Presentment message must contain in the Message Type Identifier (MTI) and 200 in DE 24 to identify it as a First Presentment.

Refer to Rule 9.4.22.1 for Transaction presentment time frames.

Financial Detail Addendum Messages

A Financial Detail Addendum provides additional program, service, or industry data to supplement the First Presentment. This message must contain in the MTI and 696 in DE 24 to identify it as a Financial Detail Addendum.

2.2.5. رسائل المقاصة

تبدأ عملية المقاصة عندما تقدم جهة القبول بيانات المعاملة إلى جهة الإصدار لأول مرة، لنشرها في حساب حامل البطاقة. وبعد التقديم الأول للمعاملة، قد تقرر جهة الإصدار أن المعاملة غير صالحة. ويجوز لها في هذه الحالة استرداد قيمة المعاملة عندما تسمح إجراءات رد المبالغ المدفوعة على وجه التحديد لجهة الإصدار بإعادة المعاملة إلى جهة القبول للحصول على تعويض محتمل. لكل معاملة بين جهة الإصدار وجهة القبول، تسمح الدورات التالية بالتقديم والاسترجاع ومعالجة رد المبالغ المدفوعة:

- يتكون التقديم الأول من خطوة واحدة - من جهة القبول إلى جهة الإصدار.
 - تتكون عملية الاسترجاع من خطوتين - طلب الاسترجاع والاستيفاء.
 - تتكون دورة رد المبالغ المدفوعة من خطوتين: رد المبالغ المدفوعة والتقديم الثاني. وإذا لزم الأمر، يجوز رفع دعوى التحكيم بعد التقديم الثاني، من قبل أي من الطرفين.
- يحتفظ نظام المقاصة بملف محفوظات رد المبالغ المدفوعة، والذي يخزن المعلومات المحددة من جميع معاملات رد المبالغ المدفوعة الواردة التي يقبلها نظام المقاصة. والغرض من ملف محفوظات رد المبالغ المدفوعة هو تتبع دورات رد المبالغ المدفوعة والمستندات التي يرسلها الأعضاء. ويقوم نظام المقاصة بتحرير رسائل رد المبالغ المدفوعة مقابل ملف محفوظات رد المبالغ المدفوعة للتحقق من تسلسل الدورة والمدد الزمنية ومتطلبات التوثيق.

تحتوي الرسائل المقاصة على البيانات التالية:

- معرف نوع الرسالة : (MTI) يحدد الغرض من الرسالة، مثل الفواتير المالية أو الإدارية أو الرسوم. يحدد MTI نوع رسالة ISO العامة. تشمل MTIs الصالحة (التقديم) و (رد المبالغ المدفوعة) و (الإدارية) و (تحصيل الرسوم).
- خريطة بت: سلسلة من الأرقام الثنائية (بتات) التي تشير إلى وجود أو عدم وجود عناصر البيانات.
- عناصر البيانات: عناصر الرسالة المحددة في مواصفة ISO 8583-1993 التي قد تحتوي على بيانات.
- عناصر البيانات الفرعية الخاصة: عناصر الرسالة المحددة بواسطة مشغل شبكة الدفع المحلية عامل لدعم البيانات غير المحددة ضمن مواصفات ISO 8583-1993. (انظر الملحق رقم 36)

يشير عنصر البيانات (DE) 24 (رمز الوظيفة) في كل رسالة إلى النوع الأساسي أو الوظيفة الأساسية للمعاملة، ويشير DE 25 (رمز سبب الرسالة) إلى السبب الأساسي للمعاملة.

رسائل التقديم الأولى

ستبدأ جهة القبول التقديم الأول لإبلاغ جهة الإصدار أو مقدم الخدمة الخاص به بأن المعاملة المالية قد اكتملت نيابة عنه. ويجب أن تحتوي رسالة التقديم الأول على معرف نوع الرسالة (MTI) و 200 في DE 24 لتعريفها على أنها تقديم أول.

الرجوع إلى القاعدة 9.4.22.1 للأطر الزمنية لتقديم المعاملات.

رسائل ملحق التفاصيل المالية

يوفر ملحق التفاصيل المالية بيانات إضافية عن البرنامج أو الخدمة أو الصناعة لتكملة التقديم الأول. ويجب أن تحتوي هذه الرسالة في MTI و 696 في DE 24 لتعريفها كملحق تفاصيل مالية.

First Chargeback Messages

An Issuer initiates First Chargeback messages to return partially or completely a previous First Presentment. Depending on program and service rules, an Issuer may charge back a First Presentment that the Acquirer submitted. These messages must contain in the MTI and one of the following values in DE 24 (Function Code):

- 450 to indicate that the message is a First Chargeback (Full) for the full First Presentment amount
- 453 to indicate that the message is a First Chargeback (Partial) for part of the First Presentment amount

The specific reason for the First Chargeback is in DE 25 (Message Reason Code).

First Chargeback Time Frame

Certain timeliness requirements apply to the first chargeback. The time frames for first chargebacks are set out in Book 3 chapter 3.

Second Presentment Messages

An Acquirer initiates Second Presentment messages to remedy a previous First Chargeback. These messages must contain in the MTI

The specific reason for the Second Presentment is in DE 25 (Message Reason Code).

Second Presentment Time Frame

The time frame for a second presentment is 45 calendar days, which is measured as the time between the Clearing System processing date on which the Member received the chargeback and the date on which the Clearing System processed the Transaction as a second presentment.

Retrieval Request Messages

On occasion, the Issuer may find it necessary to request a copy of the Transaction receipt to satisfy a Cardholder's inquiry or resolve an internal investigation, and the Issuer will send a Retrieval Request to an Acquirer. The message must contain in the Message Type Identifier (MTI) and 603 in Data Element (DE) 24 (Function Code) to identify it as a Retrieval Request. An Acquirer is under obligation to fulfill this request by providing a copy or substitute draft of the TID, or by providing a response indicating the reason for its failure to honor the request.

Issuers may not submit retrieval requests for ATM Transactions.

Retrieval Request Acknowledgement Messages

An Acquirer sends a Retrieval Request Acknowledgement to an Issuer indicating that the Acquirer has fulfilled the Retrieval Request. The message must contain in the Message Type Identifier (MTI) and 605 in DE 24 (Function Code) to identify it as a Retrieval Request Acknowledgement.

Fee Collection Messages

Fee Collection messages are used for the collection or disbursement of fees that require funds settlement between various clearing system participants. Fee Collection messages may include fees generated between pairs of Members, and fees generated between the National Scheme Operator and Members. Following are some examples of Fee Collection messages:

الرسائل الأولى لرد المبالغ المدفوعة

تبدأ جهة الاصدار رسائل رد المبالغ المدفوعة الأولى لإرجاع التقديم الأول السابق جزئيًا أو كليًا. اعتمادًا على قواعد البرنامج والخدمة، قد تقوم جهة الاصدار بإعادة تحميل التقديم الأول الذي قدمته جهة القبول. يجب أن تحتوي هذه الرسائل في MTI وأحد القيم التالية في DE 24 (رمز الوظيفة):

- 450 للإشارة إلى أن الرسالة عبارة عن عملية رد المبالغ المدفوعة أولًا (كاملة) لكامل مبلغ التقديم الأول.
- 453 للإشارة إلى أن الرسالة عبارة عن عملية رد المبالغ المدفوعة أولًا (جزئية) لجزء من مبلغ التقديم الأول.

السبب المحدد لأول عملية رد مبالغ مدفوعة في DE 25 (رمز سبب الرسالة).

أول إطار زمني لرد المبالغ المدفوعة

تنطبق متطلبات توقيت معينة على عملية رد المبالغ المدفوعة الأولى. تم تحديد الأطر الزمنية لعمليات رد المبالغ المدفوعة لأول مرة في الفصل 3 من الكتاب الثالث.

رسائل التقديم الثانية

تبدأ إحدى جهات القبول رسائل التقديم الثاني لمعالجة عملية رد المبالغ المدفوعة الأولى السابقة.

يجب أن تحتوي هذه الرسائل في MTI

السبب المحدد للتقديم الثاني هو DE 25 (رمز سبب الرسالة).

الإطار الزمني الثاني للتقديم

الإطار الزمني للتقديم الثاني هو 45 يومًا تقويميًا، ويتم قياسه على أنه الوقت بين تاريخ معالجة نظام المقاصة الذي تلقى فيه العضو رد المبالغ المدفوعة والتاريخ الذي قام فيه نظام المقاصة بمعالجة المعاملة كتقديم ثانٍ.

رسائل طلب الاسترجاع

في بعض الأحيان، قد تجد جهة الاصدار أنه من الضروري طلب نسخة من إيصال المعاملة للرد على استفسار حامل البطاقة أو تسوية تحقيق داخلي، وتقوم جهة الاصدار بإرسال طلب استرداد إلى جهة القبول. ويجب أن تحتوي الرسالة على معرف نوع الرسالة (MTI) و 603 في عنصر البيانات (DE) 24 (رمز الوظيفة) لتعريفها كطلب استرداد.

تلتزم جهة القبول بتلبية هذا الطلب من خلال تقديم نسخة أو مسودة بديلة من TID ، أو من خلال تقديم رد يوضح سبب فشله في عدم تلبية الطلب.

لا يجوز لجهات الاصدار تقديم طلبات استرداد لمعاملات أجهزة الصراف الآلي.

رسائل إقرار طلب الاسترداد

ترسل جهة القبول إقرارًا باسترداد طلب الاسترداد إلى جهة الاصدار، يشير إلى أن جهة القبول قد استوفت طلب الاسترداد. ويجب أن تحتوي الرسالة على معرف نوع الرسالة (MTI) و 605 في DE 24 (رمز الوظيفة) لتعريفها على أنها إقرار باستلام طلب الاسترداد.

رسائل تحصيل الرسوم

تُستخدم رسائل تحصيل الرسوم، لتحصيل أو صرف الرسوم التي تتطلب تسوية الأموال بين مختلف المشاركين في نظام المقاصة. وقد تتضمن رسائل تحصيل الرسوم، الرسوم الناتجة بين أزواج من الأعضاء، والرسوم الناتجة بين مشغل شبكة الدفع المحلية والأعضاء. فيما يلي بعض الأمثلة على رسائل تحصيل الرسوم:

- Collection or disbursement from Member to Member of fees that brand, program, and service rules permit
- Collection or disbursement from the National Scheme Operator to Member of fees related to processing services that the clearing system provides
- Collection or disbursement from the National Scheme Operator to the Member of such fees as administrative fees, membership fees, and penalties, according to brand, program, and service
- Collection or disbursement from Member to Member of summary settlement positions between Members that participate in bilateral clearing arrangements with clearing system summary settlement

5.2.3 Clearing System Functionality

The sending Member can submit Transaction data for clearing to the Clearing System seven days a week, 24 hours a day.

The Clearing System processes the data once a day at 12:00AM of the processing day (All times shown are expressed as local time of Libya).

With the implementation of six clearing cycle cutoffs in the Clearing System, processing Members have the option to receive clearing files four, five, or six times per day.

Members may create and send clearing files as frequently as they want. Sending clearing files earlier allows Members to have more Transactions processed in earlier clearing cycle cutoffs, thus ensuring the next available settlement of their accepted Transactions.

Each Member must receive data from a minimum of one cycle per day. The Clearing System has established the initial default delivery cycles for all processing Members.

5.2.3.1 Methods of Transmitting Data to the Clearing System

Members transmit clearing data to the Clearing System through certain media and under certain conditions, using any of several available file transfer methods. For each transmission method, the Clearing System performs edits to ensure that the system does not process test files in the production environment. Therefore, if a Member inadvertently sends a test file to the production environment, the Clearing System does not process it as production data.

All files generated by the Clearing System will specify whether the Clearing System created them in production or in test mode, so that the Member can perform checks to verify that the Member is not processing a test file in the production environment.

5.2.3.2 Reversing Clearing Files

A reversal message informs the receiver to disregard the original message. The settlement values for a reversal message and its original together produce a net settlement value of zero. Members can reverse one or more individual messages or an entire clearing file.

- تحصيل أو صرف الرسوم من "العضو" إلى "العضو" التي تسمح بها قواعد العلامة التجارية والبرنامج والخدمة.
- تحصيل الرسوم المتعلقة بخدمات المعالجة التي يوفرها نظام المقاصة أو الصرف من مشغل شبكة الدفع المحلية إلى العضو.
- تحصيل أو صرف من مشغل شبكة الدفع المحلية إلى العضو رسوم مثل الرسوم الإدارية ورسوم العضوية والعقوبات، وفقاً للعلامة التجارية والبرنامج والخدم.
- تحصيل أو صرف من عضو إلى عضو آخر لإجراءات التسوية الموجزة بين الأعضاء الذين يشاركون في ترتيبات المقاصة الثنائية مع تسوية موجزة لنظام المقاصة.

3.2.5 وظائف نظام المقاصة

يمكن للعضو المرسل إرسال بيانات المعاملة للتصفية إلى نظام المقاصة سبعة أيام في الأسبوع، 24 ساعة في اليوم.

يعالج نظام المقاصة البيانات مرة واحدة يوميًا في الساعة 12:00 ظهرًا من يوم المعالجة (يتم التعبير عن جميع الأوقات المعروضة بالتوقيت المحلي لدولة ليبيا).

مع تنفيذ ستة عمليات قطع لدورة المقاصة في نظام المقاصة، يكون لدى أعضاء المعالجة خيار استلام ملفات المقاصة أربع أو خمس أو ست مرات في اليوم.

يمكن للأعضاء إنشاء وإرسال ملفات المقاصة بقدر ما يريدون. يسمح إرسال ملفات المقاصة في وقت سابق للأعضاء بإجراء المزيد من المعاملات التي تتم معالجتها في فترات زمنية سابقة لدورة المقاصة ، وبالتالي ضمان التسوية التالية المتاحة لمعاملاتهم المقبولة.

يجب أن يتلقى كل عضو بيانات من دورة واحدة على الأقل في اليوم. أنشأ نظام المقاصة دورات التسليم الافتراضية الأولية لجميع أعضاء المعالجة.

1.3.2.5 طرق إرسال البيانات إلى نظام المقاصة

يقوم الأعضاء بنقل بيانات المقاصة إلى نظام المقاصة من خلال وسائط معينة وفي ظل ظروف معينة، باستخدام أي من طرق نقل الملفات العديدة المتاحة. لكل طريقة إرسال، ويقوم نظام المقاصة بإجراء عمليات التحرير للتحقق من أن النظام لا يعالج ملفات الاختبار في بيئة الإنتاج. لذلك، إذا أرسل أحد الأعضاء عن غير قصد ملف اختبار إلى بيئة الإنتاج، فلن يقوم نظام المقاصة بمعالجته كبيانات إنتاج.

ستحدد جميع الملفات التي تم إنشاؤها بواسطة نظام المقاصة ما إذا كان نظام المقاصة قد أنشأها في الإنتاج أو في وضع الاختبار، بحيث يمكن للعضو إجراء فحوصات للتحقق من أن العضو لا يقوم بمعالجة ملف اختبار في بيئة الإنتاج.

2.3.2.5 إلغاء ملفات المقاصة

تُعلم رسالة الإلغاء المتلقي بتجاهل الرسالة الأصلية. وتنتج قيم التسوية لرسالة الإلغاء وأصلها معًا قيمة تسوية صافية قدرها صفر. يمكن للأعضاء إلغاء واحدة أو أكثر من الرسائل الفردية أو ملف المقاصة بأكمله.

How to Send Reversal Messages

Members will follow the procedure below to reverse an individual message.

Procedure

1. The Member realizes that it needs to reverse an individual message.
2. The Member extracts the message to be reversed.
3. The Member indicates in the message that it is a reversal and the corresponding clearing message .
4. The Member adds the reversal message to one of its outgoing clearing files.
5. If the Member's original message needs to be resent because it contained incorrect data, the Member corrects the data in the original message and resubmits it.

The Clearing System will individually process each reversal message submitted in a file that also includes other message types. There is no requirement to isolate reversal messages or to send them in separate files.

5.2.3.3 Duplicate Clearing Files

A duplicate file occurs when the Clearing System processes an individual Transaction more than once. The Clearing System has certain edits and built-in controls that help it to detect duplicate files. The National Scheme Operator recommends that Members establish controls to prevent and detect these and other errors to help prevent duplicate files and postings.

Reasons for Duplicate Clearing System Files or Postings

Duplicate postings may occur for various reasons.

- An operator changes the file ID number on a previously processed file and resends it.
- Previously processed Merchant deposits are processed again.
- The Merchant deposits the same Transaction more than once.

If a duplicate posting does occur, either the sending Member or the receiving Member may identify it. If the receiving Member discovers a duplicate posting, it must notify the sending Member. The sending Member must inform the Clearing System and then take action to correct the duplicate postings by submitting reversals.

When the sending Member notifies the National Scheme Operator about a duplicate posting, the Member must provide the following information about both the original and the duplicated postings:

- File ID numbers
- Net amounts

5.3 The Settlement System

The exchange of successfully processed detailed financial Transaction data through the Clearing System represents an obligation to exchange funds. Settlement is the process by which the Settlement System facilitates the exchange of funds on behalf of its Members.

The Settlement System performs the following two settlement functions:

- Sending settlement advisements
- Transferring funds (when applicable)

The Settlement System uses clearing data to calculate the net position of each Member involved in the clearing process. Funds are then exchanged each day between Members for the net monetary value of the cleared Transactions. The net value may include the following:

كيفية إرسال رسائل الإلغاء

يتبع الأعضاء الإجراء التالي لإلغاء رسالة فردية.

الإجراء

1. يدرك العضو أنه يحتاج إلى إلغاء رسالة فردية.
 2. يستخرج العضو الرسالة المراد إلغاؤها.
 3. يشير العضو في الرسالة إلى أنه إلغاء ورسالة المقاصة المقابلة.
 4. يضيف العضو رسالة الإلغاء إلى أحد ملفات المقاصة الصادرة الخاصة به.
 5. إذا كانت الرسالة الأصلية للعضو بحاجة إلى إعادة إرسالها لأنها تحتوي على بيانات غير صحيحة، فسيصحح العضو البيانات الموجودة في الرسالة الأصلية ويعيد إرسالها.
- سيقوم نظام المقاصة بمعالجة كل رسالة إلغاء يتم إرسالها في ملف يتضمن أيضًا أنواع الرسائل الأخرى بشكل فردي. ولا توجد متطلبات لعزل رسائل الإلغاء أو إرسالها في ملفات منفصلة.

3.3.2.5 ملفات المقاصة المكررة

يحدث ملف مكرر للمقاصة، عندما يعالج نظام المقاصة معاملة فردية أكثر من مرة. ويحتوي نظام المقاصة على بعض عمليات التحرير وعناصر التحكم المضمنة التي تساعد على اكتشاف الملفات المكررة. ويوجب مشغل شبكة الدفع المحلية على الأعضاء بأن يضعوا ضوابط لمنع، واكتشاف هذه الأخطاء وغيرها للمساعدة في منع تكرار الملفات والترحيلات.

أسباب تكرار ملفات نظام المسح أو الترحيلات

قد تحدث منشورات مكررة لأسباب مختلفة

- يغير عامل التشغيل رقم معرف الملف في ملف تمت معالجته مسبقًا، ويعيد إرساله.
- تتم معالجة ودائع التاجر التي تمت معالجتها مسبقًا مرة أخرى.
- يقوم التاجر بإيداع نفس المعاملة أكثر من مرة.

وفي حالة حدوث ملفات مكررة، فإنه يجوز للعضو المرسل أو العضو المستلم التعرف عليها. إذا اكتشف العضو المستلم ملفاً مكرراً، فيجب عليه إخطار العضو المرسل. يجب على العضو المرسل إبلاغ نظام المقاصة ثم اتخاذ إجراء لتصحيح الترحيلات المكررة عن طريق إرسال الإلغاء.

عندما يقوم العضو المرسل بإخطار مشغل شبكة الدفع المحلية بشأن ملف مكرر، يجب على العضو تقديم المعلومات التالية حول كل من المنشورات الأصلية والمكررة:

- أرقام معرف الملف.
- المبالغ الصافية.

3.5 نظام التسوية

يمثل تبادل بيانات المعاملات المالية المفصلة التي تمت معالجتها بنجاح من خلال نظام المقاصة التزامًا بتبادل الأموال.

التسوية هي العملية التي من خلالها يسهل نظام التسوية تبادل الأموال نيابة عن أعضائه.

يؤدي نظام التسوية وظيفتي التسوية التاليتين:

- إرسال إرشادات التسوية.
- تحويل الأموال (عند الاقتضاء).

يستخدم نظام التسوية بيانات المقاصة لحساب المركز الصافي لكل عضو مشارك في عملية المقاصة. ويتم بعد ذلك تبادل الأموال كل يوم بين الأعضاء مقابل صافي القيمة النقدية للصفتات المقاصة. قد تشمل القيمة الصافية ما يلي:

- Transaction amounts and all other Transaction and interchange charges processed through the clearing system(s)
- Cash disbursement and ATM cash disbursement service fees (off us based)
- Billing items submitted by the National Scheme Operator to the Clearing System, the Settlement System, or both.

Settlement with most Members occurs from Sunday through Thursday, excluding business holidays. Settlement can occur only after clearing has already occurred.

5.3.1 Participation in the Settlement System

(Category A)

Members, transfer Service Providers, or both must meet conditions to participate in settlement. The transfer Service Provider, as account owner, is the entity responsible for the transfer of funds on behalf of the Member.

5.3.2 General Settlement Obligations

(Category A)

A Principal Member must be prepared to perform all of the following obligations on an ongoing basis:

- Ensure that the settlement Service Provider has received funds on the value date for the amount due as indicated on the Transfer Agent Detail Advisement;
- Is able to receive funds when the Member has a net credit position; and
- Be prepared to settle in accordance with the Settlement System holiday schedule.

Initial and continued participation in the Settlement System by a Member is further expressly conditioned upon such Member's compliance with the following obligations:

- To notify the Settlement System promptly and, in no event not more than 24 hours should the Member become aware that any information provided in the Net Settlement Information Form (NSIF) is not accurate or complete or is no longer accurate;
- To ensure that necessary and appropriate personnel of the Member and, if applicable, its transfer Service Provider, including personnel responsible for the Member's participation in settlement, are aware of and faithfully and fully perform all of the Member's obligations arising from or relating to its participation in settlement; and
- To timely pay fees and other assessments arising from or relating to participation in settlement. The National Scheme Operator uses a standard monthly billing schedule to assess fees to Members for facilitating settlement services. Core settlement services include the following:
 - The maintenance of Member settlement parameters;
 - Preparation and delivery of settlement advisements; and
 - Facilitating the process of settlement;

- معالجة مبالغ المعاملات وجميع رسوم المعاملات والتبادل الأخرى من خلال نظام (أنظمة) المقاصة.

- الصرف النقدي ورسوم خدمة الصرف النقدي من أجهزة الصراف الآلي (off us based)
- بنود الفواتير التي يرسلها مشغل شبكة الدفع المحلية إلى نظام المقاصة أو نظام التسوية أو كليهما.

تتم التسوية مع أغلب الأعضاء من الأحد إلى الخميس، باستثناء أيام العطلات الرسمية. ويمكن أن تحدث التسوية فقط بعد إجراء المقاصة بالفعل.

1.3.5 المشاركة في نظام التسوية

(الفئة أ)

يجب على الأعضاء أو مقدمي الخدمات المنقولين أو كليهما استيفاء الشروط للمشاركة في التسوية. مقدم خدمة التحويل، بصفته مالك الحساب، هو الكيان المسؤول عن تحويل الأموال نيابة عن العضو.

2.3.5 التزامات التسوية العامة

(الفئة أ)

يجب أن يكون العضو الرئيسي مستعدًا لأداء جميع الالتزامات التالية على أساس صفة مستمرة:

- التحقق من أن مقدم خدمة التسوية قد تلقى أموالاً في تاريخ استحقاق المبلغ المستحق كما هو مبين في إشعار تفاصيل وكيل التحويل.
- أن يكون قادرًا على تلقي الأموال عندما يكون للعضو وضع ائتماني صافي.
- أن يكون مستعدًا للتسوية وفقًا لجدول عطلة نظام التسوية.

المشاركة الأولية والمستمرة في نظام التسوية من قبل العضو مشروطة أيضًا صراحةً بامتثال هذا العضو للالتزامات التالية:

- لإخطار نظام التسوية على الفور، ولا تزيد مدة الإخطار بأي حال من الأحوال عن 24 ساعة في حالة إدراك العضو أن أي معلومات مقدمة في نموذج معلومات التسوية الصافية (NSIF) ليست دقيقة أو كاملة أو لم تعد دقيقة.
- للتحقق من أن الموظفين الضروريين والمناسبين للعضو، وإذا كان ذلك ممكنًا، مقدم خدمة النقل، بما في ذلك الموظفون المسؤولون عن مشاركة العضو في التسوية، على دراية بجميع التزامات العضو الناشئة عن أو المتعلقة بالمشاركة في التسوية وتنفيذها بأمانة وبشكل كامل. و
- لدفع الرسوم في الوقت المناسب والتقييمات الأخرى الناشئة عن أو المتعلقة بالمشاركة في التسوية.

يستخدم مشغل شبكة الدفع المحلية جدول فوترة شهريًا قياسيًا لتقييم الرسوم للأعضاء لتسهيل خدمات التسوية. تشمل خدمات التسوية الأساسية ما يلي:

- الحفاظ على معايير تسوية الأعضاء.
- إعداد وتسليم نواتج التسوية.
- تسهيل عملية التسوية.

5.3.2.1 Interbank Payment Methods

(Category C)

Principal Members must make interbank payments with the National Scheme Operator's settlement Service Provider using one of the following methods:

- The Principal Member owns a nostro account with the settlement Service Provider. Typically, these are low-risk payments because the Principal's account and the settlement account are maintained at the same bank and payments are considered on-us Transactions executed through book transfer.
- The Principal Member is a direct participant of the local Real Time Gross Settlement (RTGS) system. Typically, these are low-risk payments because the Principal and the settlement Service Provider are direct participants of the RTGS system.
- The Principal Member owns a nostro account with a correspondent bank (the "Transfer Agent"). The correspondent bank should own a nostro account at the settlement Service Provider or be able to effect settlement with the settlement Service Provider through the local RTGS system. These payments are more likely to have points of failure because the number of participants required to take actions during the payment process have increased. Payments are typically executed through book transfers, the RTGS system, or a combination thereof.

Principal Members should evaluate each option, considering the Transfer Agent's account requirements and settlement methods when in a net debit or credit position, timeliness, and the cost of payments to determine which option best meets its needs.

5.3.2.2 Settlement on Value Date Required

(Category A)

Principal Members in a net debit position and that participate in direct request payment processing are responsible for settlement to the settlement account on the value date. Non-receipt of a direct debit request is not a valid reason or just cause to fail settlement with the National Scheme Operator.

Principal Members must verify with the Transfer Agent's bank that on the value date, the Member's nostro account has been debited and the settlement account has been credited.

5.3.2.3 Reconciliation

(Category C)

It is the responsibility of each Member to reconcile the totals and Transactions provided by the Interchange System to its own internal records on a daily basis.

5.3.2.5 Settlement Finality and Discharge

(Category A)

The Settlement Finality and Discharge tables depict settlement obligations as they relate to supported payment methods.

Settlement Finality (See appendix number 37)

Discharge (See appendix number 38)

5.3.3 Settlement Best Practices

Members should consider the following best practices to avoid settlement failures and noncompliance fees when in a net debit position:

1.2.3.5 طرق الدفع بين المصارف

(الفئة ج)

يجب على الأعضاء الرئيسيين إجراء المدفوعات بين المصارف مع مقدم خدمة التسوية لمشغل شبكة الدفع المحلية باستخدام إحدى الطرق التالية:

- أن يمتلك العضو الرئيسي حساب نوسترو مع مقدم خدمة التسوية. عادةً ما تكون هذه مدفوعات منخفضة المخاطر، لأن حساب الموكل وحساب التسوية يتم الاحتفاظ بهما في نفس المصرف، وتعتبر المدفوعات معاملات تتم من خلال التحويل الكتابي.
- يعتبر العضو الرئيسي مشاركًا مباشرًا في نظام التسوية الإجمالية في الوقت الفعلي (RTGS) المحلي. عادةً ما تكون هذه مدفوعات منخفضة المخاطر لأن المدير ومقدم خدمة التسوية هم مشاركين مباشرين في نظام RTGS.
- يمتلك العضو الرئيسي حساب نوسترو مع مصرف مراسل ("وكيل التحويل"). يجب أن يمتلك المصرف المراسل حساب نوسترو (وهو حساب يحتفظ به البنك بعملة أجنبية في بنك آخر) عند مقدم خدمة التسوية أو أن يكون قادرًا على إجراء التسوية مع مقدم خدمة التسوية من خلال نظام RTGS المحلي. ومن المرجح أن يكون لهذه المدفوعات نقاط فشل لأن عدد المشاركين المطلوبين لاتخاذ إجراءات أثناء عملية الدفع قد زاد. ويتم تنفيذ المدفوعات عادةً من خلال تحويلات الدفاتر أو نظام RTGS أو مزيج منهما.

يجب على الأعضاء الرئيسيون تقييم كل خيار، مع الأخذ في الاعتبار متطلبات حساب وكيل التحويل وطرق التسوية عندما تكون في وضع مدين أو ائتماني، وحسن التوقيت، وتكلفة المدفوعات لتحديد الخيار الأفضل الذي يلبي احتياجاته.

2.2.3.5 التسوية المطلوبة في تاريخ الاستحقاق

(الفئة أ)

الأعضاء الرئيسيون في مركز الخصم الصافي، والذين يشاركون في معالجة الدفع المباشر للطلب مسؤولون عن التسوية لحساب التسوية في تاريخ القيمة. إن عدم استلام طلب الخصم المباشر ليس سببًا صالحًا أو مجرد سبب لفشل التسوية مع مشغل شبكة الدفع المحلية. يجب على الأعضاء الرئيسيون التحقق من مصرف وكيل التحويل من أنه في تاريخ القيمة، قد تم الخصم من حساب نوسترو الخاص بالعضو وتم قيد حساب التسوية.

3.2.3.5 المصالحة

(الفئة ج)

تقع على عاتق كل عضو مسؤولية التوفيق بين المجاميع والمعاملات التي يوفرها نظام التبادل مع السجلات الداخلية الخاصة به على أساس يومي.

4.2.3.5 إنهاء التسوية والإبراء

(الفئة أ)

يوضح الجدولين "إنهاء التسوية" و "إبراء الذمة" التزامات التسوية من حيث صلتها بطرق الدفع المدعومة. التسوية النهائية (انظر الملحق رقم 37) إبراء الذمة (انظر الملحق رقم 38)

3.3.5 أفضل ممارسات التسوية

يجب على الأعضاء مراعاة أفضل الممارسات التالية، لتجنب فشل التسوية، ودفع رسوم عدم الامتثال عندما يكونون في المركز القانوني للمدين الصافي:

- Receive a Transfer Agent Advisement Detail and execute the amount due on the value date as indicated on the advisement. Payments must be executed for the exact amount due on each Transfer Agent Advisement Detail, before the cut time and on the specified value date.
- Reference the Member ID number on payment details.
- Reference Member account details.
- Do not combine payments for many Member IDs or value dates into one payment.
- Ensure that the payment instruction includes the correct settlement Service Provider name for the amount due on the value date.
- Ensure all payments are marked as urgent.
- Ensure that the Transfer Agent's correspondent bank fees are not deducted from the amount due to the National Scheme Operator.
- Include the Transfer Agent ID and name within the payment message when sending payments due to the National Scheme Operator. The Transfer Agent ID and name included in the payment message must match the advisement to ensure payments are posted timely.

5.3.4 Interchange and Service Fees

A Transaction settled between Members gives rise to the payment of the appropriate interchange fee or service fee, as applicable.

The National Scheme Operator will inform Members of all fees it establishes and may periodically publish fee tables.

5.3.5 Settlement Funds Transfer Obligations

(Category A)

A Member in a net debit settlement position must transfer funds to the National Scheme Operator's settlement Service Provider on the appropriate value date.

If a Member in a net credit settlement position is not ready and able to receive settlement funds transfers from the settlement Service Provider, the National Scheme Operator can hold these funds until the Member requests that they be forwarded.

When the Member is able to receive the funds, the Member must request in writing that the National Scheme Operator forward the funds. This request should include the principal's ID, a transfer Service Provider bank account, an original signature from the principal, and the payee name, address, amount, and advisement date. When a change of account is requested, this must be submitted through the National Scheme file Interface. The Member is not entitled to any compensation in this situation.

5.3.5.1 Business Recovery Plan

A Member is expected to have a business recovery plan in place such that the Member will be able to transfer funds in a timely manner in the event of a natural disaster or other force majeure at the Member's primary location(s). The National Scheme Operator has the option to terminate the Member's License if the Member is unable to transfer funds to the settlement Service Provider.

- تلقي إخطار وكيل التحويل بالتفصيل، وتنفيذ المبلغ المستحق في تاريخ الاستحقاق كما هو موضح في الإرشاد. ويجب تنفيذ المدفوعات بالمبلغ المحدد (المستحق) في كل تفصيل من تفاصيل إخطار وكيل التحويل، قبل وقت القطع، وفي تاريخ القيمة المحدد.
- الرجوع إلى رقم معرف العضو في تفاصيل الدفع.
- مرجع تفاصيل حساب الأعضاء.
- لا تدمج المدفوعات للعديد من معرفات الأعضاء، أو تواريخ القيمة في دفعة واحدة.
- التحقق من أن تعليمات الدفع تتضمن اسم مقدم خدمة التسوية الصحيح للمبلغ المستحق في تاريخ الاستحقاق.
- التحقق من وضع علامة على جميع المدفوعات على أنها عاجلة.
- التحقق من عدم خصم رسوم المصرف المراسل لوكيل التحويل من المبلغ المستحق لمشغل شبكة الدفع المحلية.
- القيام بتضمين معرف وكيل التحويل واسمه في رسالة الدفع عند إرسال المدفوعات المستحقة لمشغل شبكة الدفع المحلية. ويجب أن يتطابق معرف وكيل التحويل والاسم المضمن في رسالة الدفع مع التنبيه لضمان ترحيل المدفوعات في الوقت المناسب.

4.3.5 رسوم التبادل والخدمة

تؤدي المعاملة التي تتم تسويتها بين الأعضاء إلى دفع رسوم التبادل، أو رسوم الخدمة المناسبة، حسب الاقتضاء.

ويقوم مشغل شبكة الدفع المحلية بإبلاغ الأعضاء بجميع الرسوم التي يحددها، ويمكنه نشر جداول الرسوم بشكل دوري.

5.3.5 التزامات تحويل أموال التسوية

(الفئة أ)

يجب على العضو في وضع تسوية الخصم الصافي تحويل الأموال إلى مقدم خدمة التسوية لمشغل شبكة الدفع المحلية في تاريخ القيمة المناسب.

إذا كان العضو في وضع تسوية الائتمان الصافي وغير جاهز وقادر على تلقي تحويلات أموال التسوية من مقدم خدمة التسوية، يمكن لمشغل شبكة الدفع المحلية الاحتفاظ بهذه الأموال حتى يطلب العضو إعادة توجيهها.

عندما يكون العضو قادرًا على استلام الأموال، يجب عليه أن يطلب كتابيًا من مشغل شبكة الدفع المحلية أن يقوم بإرسال الأموال. ويجب أن يتضمن هذا الطلب معرف المدير، والحساب المصرفي لمقدم خدمة التحويل، والتوقيع الأصلي من المدير، واسم المدفوع لأمره، والعنوان، والمبلغ، وتاريخ الاستشارة. وعند طلب تغيير الحساب، يجب تقديم ذلك من خلال واجهة ملف الشبكة المحلية. ولا يحق للعضو الحصول على أي تعويض في هذه الحالة.

1.5.3.5 خطة استعادة الأعمال

من المتوقع أن يكون لدى العضو خطة لاستعادة الأعمال، بحيث يتمكن من تحويل الأموال في الوقت المناسب في حالة وقوع كارثة طبيعية أو ظروف القاهرة أخرى في الموقع (المواقع) الرئيسية للعضو. ومشغل شبكة الدفع المحلية لديه الخيار لإنهاء ترخيص العضو إذا كان العضو غير قادر على تحويل الأموال إلى مقدمي خدمة التسوية.

5.3.5.2 Transfer Agent Obligations

The Member responsible for paying the National Scheme Operator is called the “Transfer Agent”. In the event of a settlement failure, the Transfer Agent may be required to pay interest compensation and a non-compliance fee to the National Scheme Operator, regardless of the reason for the settlement failure or any use by the transfer Service Provider of a third party such as a “Pay Thru” bank.

5.3.5.3 Disputes and Claims Procedures

(Category C)

If a Member disputes the amount of a net settlement credit or debit of which it has been advised and seeks compensation (as described in section 9.3.15), the Member must, upon discovery and in writing within one business day, request the National Scheme Operator to perform an investigation of the matter.

In any event, the Member must timely transfer funds as reflected in the advisement to avoid settlement penalties unless notified otherwise by the National Scheme Operator. Upon request of the National Scheme Operator, the Member must provide relevant clearing records or other documentation as necessary to evidence the amount involved.

5.3.6 Indemnification and Limitation of Liability of National Scheme Operator

Each Member shall indemnify and hold the National Scheme Operator and its settlement Service Provider harmless from and against any and all claims, losses, damages, liabilities, costs, and expenses, including reasonable attorneys’ fees incurred by the National Scheme Operator or its settlement Service Provider by way of suit, claim settlement, or otherwise, alleged or to arise out of, arising out of, or in connection with services provided by the National Scheme Operator or its settlement Service Provider in connection with settlement. The settlement Service Provider shall be deemed to be a third-party beneficiary of the preceding sentence with independent rights of enforcement.

Neither CBL nor its’ National Scheme Operator are subject to incur any financial or other responsibility, or other liability to any Member or other person for any loss, cost, or other damage arising out of the net settlement process described in this section except due to an error by the National Scheme Operator that results in a transfer by the National Scheme Operator to a Member of an insufficient amount of funds or in a transfer from a Member of an excess amount of funds.

If the National Scheme Operator, in its sole discretion, accepts responsibility, the total maximum responsibility of the National Scheme Operator for the error(s) or delay(s), as the case may be, will be the compensation defined in Rule 5.3.14.3, Compensation.

5.3.14.3, Compensation.

Unless being set differently by CBL, Payment of principal (or a portion thereof) and compensation by the National Scheme Operator shall be a Member’s sole and exclusive remedy with respect to the National Scheme Operator for any and all damage incurred by it, directly or indirectly, as a result of its participation in the National Scheme Operator net settlement program. In this respect, only a principal and not the transfer Service Provider bank, if different, may recover compensation from the National Scheme Operator.

NOTE: In no event shall the National Scheme Operator be responsible for any special, indirect, consequential, punitive, or other damages of any type.

2.5.3.5 التزامات وكيل النقل

العضو المسؤول عن الدفع لمشغل شبكة الدفع المحلية يسمى “وكيل التحويل”. وفي حالة فشل التسوية، قد يُطلب من وكيل التحويل دفع تعويض يتمثل في قيمة الفائدة ورسوم عدم الامتثال لمشغل شبكة الدفع المحلية، وبغض النظر عن سبب فشل التسوية أو أي استخدام من قبل مقدم خدمة النقل لطرف ثالث مثل مصرف “الدفع من خلال”.

3.5.3.5 إجراءات المنازعات والمطالبات

(الفئة ج)

إذا اعترض أحد الأعضاء على مبلغ صافي ائتمان التسوية أو على الخصم الذي تم إبلاغه به وطلب تعويضًا (كما هو موضح في القسم 9.3.15)، فيجب على العضو، عند اكتشافه لذلك، أن يطلب كتابيًا وخلال يوم عمل واحد من مشغل شبكة الدفع المحلية إجراء تحقيق في الأمر.

وعلى أي حال، يجب على العضو تحويل الأموال في الوقت المناسب على النحو المبين في التنبيه لتجنب غرامات التسوية ما لم يخطر بخلاف ذلك من قبل مشغل شبكة الدفع المحلية. بناءً على طلب لمشغل شبكة الدفع المحلية، يجب على العضو تقديم سجلات المقاصة ذات الصلة أو غيرها من الوثائق حسب الضرورة لإثبات المبلغ المعني.

6.3.5 تعويض وحدود مسؤولية مشغل شبكة الدفع المحلية

يتعين على كل عضو تعويض مشغل شبكة الدفع المحلية، ومقدم خدمة التسوية الخاص به والتدخل لحمايته من المطالبات والخسائر والأضرار والمسؤوليات والتكاليف والمصروفات، بما في ذلك أتعاب المحاماة المعقولة التي تكبدها مشغل شبكة الدفع المحلية أو خدمة التسوية الخاصة به. إذا كانت الدعوى أو المطالبة تتعلق بالخدمات المقدمة من قبل مشغل شبكة الدفع المحلية أو مقدم خدمة التسوية الخاص به فيما يتعلق بالتسوية. ويعتبر مقدم خدمة التسوية طرفًا ثالثًا مستفيدًا من الجملة السابقة مع حقوق إنفاذ مستقلة.

لا يخضع مصرف ليبيا المركزي ولا مشغل شبكة الدفع المحلية الخاص بها لتحمل أي مسؤولية مالية أو غيرها من المسؤوليات، تجاه أي عضو أو شخص آخر عن أي خسارة أو تكلفة أو أي ضرر آخر ينشأ عن عملية التسوية الصافية الموضحة في هذا القسم؛ باستثناء ما يرجع إلى الخطأ من قبل مشغل شبكة الدفع المحلية الذي أدى إلى تحويل من قبل مشغل شبكة الدفع المحلية لعضو لديه مبلغ غير كاف من الأموال أو في تحويل من عضو لمبلغ فائض من الأموال.

إذا قبل مشغل شبكة الدفع المحلية، وفقاً لسلطته التقديرية، المسؤولية، فسيكون التعويض المحدد في القاعدة 5.3.14.3.

5.3.14.3, التعويض.

ما لم يتم تعيينها بشكل مختلف من قبل مصرف ليبيا المركزي، فإن دفع المبلغ الأصلي (أو جزء منه) والتعويض من قبل مشغل شبكة الدفع المحلية يكون هو التعويض الوحيد والحصري للعضو فيما يتعلق بمشغل شبكة الدفع المحلية عن جميع الأضرار التي تكبدها، بشكل مباشر أو غير مباشر. نتيجة مشاركتها في برنامج التسوية الصافية لمشغل شبكة الدفع المحلية. في هذا الصدد، ويجوز فقط للمدير، وليس للمصرف مقدم خدمة التحويل، إذا كان مختلفًا، استرداد التعويض من مشغل شبكة الدفع المحلية.

ملاحظة: لن يكون مشغل شبكة الدفع المحلية بأي حال من الأحوال مسؤولاً عن أي أضرار خاصة أو غير مباشرة أو تبعية أو عقابية أو أي أضرار أخرى من أي نوع.

NOTE: The National Scheme Operator disclaims all warranties with respect to the Settlement System, both expressed and implied, including, but not limited to, any implied warranty of merchantability or fitness for a particular purpose.

5.3.7 Failure of a Principal Member to Discharge a Settlement Obligation

(Category A)

Subject to the limitation set forth in this Rule, if a Principal Member fails to discharge a Settlement Obligation arising from or in connection with any Processed Transaction, the National Scheme Operator will satisfy such Settlement Obligation to the extent such Settlement Obligation is not otherwise satisfied.

To the extent the National Scheme Operator satisfies a Member's Settlement Obligation, such satisfaction constitutes an automatic transfer, sale, and absolute assignment to the National Scheme Operator, and not an assignment for security purposes, of all right, title, and interest in the receivable. Such satisfaction of the Member's Settlement Obligation also entitles the National Scheme Operator to all records and documents related to the receivable, including the name and address of each Cardholder or other person obligated to satisfy any part of the receivable. The Member must promptly deliver all such records and documents to the National Scheme Operator or to the National Scheme Operator's designee. Any proceeds received by or on behalf of the Member from any receivable must be held in trust by the Member and paid to the National Scheme Operator as soon as practicable.

The National Scheme Operator may take any action the National Scheme Operator deems necessary or appropriate to protect its interest in the receivable and to protect the integrity of the affairs of the National Scheme Operator, such as, by way of example and not limitation, by:

1. Refusing or rejecting Transaction authorization requests relating to use of the Member's Cards.
2. Without prior notice to the Member, holding any monies due, directly or indirectly and for any purpose, to the Member from the National Scheme Operator and any Settlement Obligations due to the Member and apply those monies to the amounts the Member owes to the National Scheme Operator and to other Members arising from Activity.
3. Listing some or all of a Member's Account numbers on the stoplist or in other or similar publications.
4. Effecting chargebacks on behalf of the Member.
5. Overseeing the disposition of unused Card stock and any other media bearing security-sensitive information, including Account information.

The National Scheme Operator assumes no liability, responsibility, or obligation to satisfy, in full or in part:

- A. A Settlement Obligation arising from or in connection with a Transaction in which the Principal, considered together with one or more of its Affiliates, acts as both the Issuer and the Acquirer.
- B. A Settlement Obligation arising from or in connection with a Transaction in which the Issuer and Acquirer are related parties or are under common Control by one or more parents, holding companies, or other entities.
- C. A Settlement Obligation arising from or in connection with any of the Principal's Sponsored Affiliates.

ملاحظة: يتنصل لمشغل شبكة الدفع المحلية من جميع الضمانات المتعلقة بنظام التسوية، سواء الصريحة أو الضمنية، بما في ذلك، على سبيل المثال لا الحصر، أي ضمان ضمني خاص بالتسويق أو الملاءمة لغرض معين.

7.3.5 فشل العضو الرئيسي في إبراء الذمة من التزام التسوية (الفئة أ)

مع مراعاة القيد المنصوص عليه في هذه القاعدة، إذا فشل العضو الرئيسي في الوفاء بالتزامات التسوية الناشئة عن أي معاملة تمت معالجتها، فسوف يفي لمشغل شبكة الدفع المحلية بالالتزام التسوية هذا، إلى الحد الذي لا يتم فيه استيفاء التزام التسوية هذا.

إلى الحد الذي يفي فيه لمشغل شبكة الدفع المحلية بالالتزام التسوية الخاص بالعضو، فإن هذا الرضا يشكل نقلًا تلقائيًا وبيعًا وتنازلًا مطلقًا لمشغل شبكة الدفع المحلية، وليس تخصيصًا لأغراض أمنية، لجميع الحقوق والملكية والمصلحة في المستحق. كما يمنح هذا الإيفاء بالالتزام التسوية الخاص بالعضو مشغل شبكة الدفع المحلية الحق في جميع السجلات والمستندات المتعلقة بالمستحق، بما في ذلك اسم وعنوان كل حامل بطاقة أو أي شخص آخر ملزم بإيفاء أي جزء من المستحق. ويجب على العضو تسليم جميع هذه السجلات والمستندات على الفور إلى مشغل شبكة الدفع المحلية أو إلى من ينوب عن مشغل شبكة الدفع المحلية. وأي عائدات يتلقاها العضو أو نيابة عنه من أي ذمم مدينة له يجب أن يحتفظ بها العضو في أمانة ودفعها لمشغل شبكة الدفع المحلية في أقرب وقت ممكن عمليًا.

يجوز لمشغل شبكة الدفع المحلية اتخاذ أي إجراء يراه ضروريًا أو مناسبًا لحماية مصلحته في المستحق ولحماية سلامة شؤون مشغل شبكة الدفع المحلية على سبيل المثال وليس الحصر، من خلال:

1. رفض طلبات تفويض المعاملات المتعلقة باستخدام بطاقات العضو.
2. دون توجيه إشعار مسبق للعضو، الاحتفاظ بأي أموال مستحقة، بشكل مباشر أو غير مباشر ولأي غرض، للعضو من مشغل شبكة الدفع المحلية وأي التزامات تسوية مستحقة للعضو وتطبيق هذه الأموال على المبالغ التي يدين بها العضو لمشغل شبكة الدفع المحلية والأعضاء الآخرين الناشئين عن النشاط.
3. إدراج بعض أو كل أرقام حساب العضو في قائمة التوقف أو في منشورات أخرى أو مشابهة.
4. تنفيذ عمليات رد المبالغ المدفوعة نيابة عن العضو.
5. الإشراف على التصرف في مخزون البطاقات غير المستخدم وأي وسائط أخرى تحمل معلومات أمنية حساسة، بما في ذلك معلومات الحساب.

لا يتحمل مشغل شبكة الدفع المحلية أي مسؤولية أو التزام بالوفاء كليًا أو جزئيًا بما يلي:

- أ. التزام تسوية ينشأ أو يتعلق بمعاملة يعمل فيها الموكل مع واحدة أو أكثر من الشركات التابعة له، بصفته كل من جهة اصدار أو جهة استحواذ.
- ب. التزام تسوية ينشأ عن أو فيما يتعلق بمعاملة تكون فيها جهة الاصدار أو جهة القبول طرفين مرتبطين أو يخضعان لسيطرة مشتركة من قبل واحد أو أكثر من الوالدين أو الشركات القابضة أو الكيانات الأخرى.
- ت. التزام تسوية ينشأ أو يتعلق بأي من الشركات التابعة المكفولة للموكل.

D. A Settlement Obligation arising from or in connection with a Transaction that was not settled by means of the Settlement System, in whole or in part, where the non-settlement was expressly directed, mandated, or otherwise compelled by a government or governmental regulatory agency, regardless of whether such direction or mandate was publicly announced. For clarity, this provision shall not apply where the non-settlement occurred at the direction of a government or government-designated receiver or trustee made in the ordinary course of a receivership/insolvency proceeding.

5.3.8 System Liquidity

(Category A)

If the National Scheme Operator requires funds to maintain system liquidity and to meet the obligations that a Member or Members have failed to discharge (for purposes of this section, “Non-discharged Member Obligations”), the National Scheme Operator may collect funds directly from the settlement accounts of Members upon reasonable notice to the Members.

In such event, the funds will be collected by the National Scheme Operator by:

- Decreasing the gross daily settlement amounts of outgoing volumes of Members by up to five percent (5 percent) of the amount settled on one or more days; and
- Increasing the gross daily settlement amounts of incoming volumes of Members by up to five percent (5 percent) of the amount settled on one or more days.

This collection may continue as long as deemed necessary or appropriate to satisfy Non-discharged Member Obligations and to ensure system liquidity or until the National Scheme Operator deems such collection no longer necessary or appropriate.

Collected funds are treated as advance payments on the sums that may be required from the Members in the allocation among Members of loss related to Non-discharged Member Obligations. If the funds collected from a Member exceed the amount ultimately allocated to it in connection with Non-discharged Member Obligations, the excess amount will be returned to the Member with interest. If the funds collected from a Member do not exceed the amount allocated to it, the Member will pay any shortage to the National Scheme Operator with interest. Any interest payment by or to the National Scheme Operator will be based on a rate that the National Scheme Operator designates, during the time between the incidence of the Member funding and the final allocation.

5.3.9 Liability for Owned or Controlled Entities

(Category A)

Each Member (referred to for purposes of this Rule as a “Responsible Member”) shall irrevocably and unconditionally guarantee, as a primary obligor and not merely as a surety, to the National Scheme Operator and all other Members, the prompt payment and performance of the obligations (the “Guaranteed Obligations”) of each of the Responsible Member’s affiliated entities arising under the Standards and from each such affiliated entity’s Activities and use of any of the Marks.

For purposes of this Rule, a Responsible Member’s affiliated entity is defined as follows:

1. A Member that is Owned or Controlled by the Responsible Member or is owned or controlled by the Responsible Member and another Member or Members; or
2. A Member that, with the Responsible Member, is under common Ownership by, or Control of, another entity; or

ث. التزام تسوية ناشئ أو يتعلق بمعاملة لم تتم تسويتها عن طريق نظام التسوية، كليًا أو جزئيًا، حيث تم توجيه عدم التسوية صراحة أو تفويضه أو إلزامه من قبل حكومة أو هيئة تنظيمية حكومية الوكالة، بغض النظر عما إذا كان هذا التوجيه أو التفويض قد تم الإعلان عنه علنًا. للتوضيح، لا ينطبق هذا الحكم في حالة حدوث عدم التسوية بناءً على توجيه من الحكومة أو المستلم المعين من قبل الحكومة أو الوصي الذي تم إجراؤه في السياق العادي لإجراء الحراسة / الإعسار.

8.3.5 سيولة النظام

(الفئة أ)

إذا طلب مشغل شبكة الدفع المحلية أموالًا للحفاظ على سيولة النظام والوفاء بالالتزامات التي فشل العضو أو الأعضاء في الوفاء بها (لأغراض هذا القسم ، “التزامات الأعضاء غير المسرودة“)، يجوز لمشغل شبكة الدفع المحلية جمع الأموال مباشرة من حسابات التسوية للأعضاء بموجب إخطار معقول للأعضاء.

في مثل هذه الحالة، سيتم جمع الأموال من قبل مشغل شبكة الدفع المحلية من خلال:

- تقليل إجمالي مبالغ التسوية اليومية للأحجام الصادرة من الأعضاء بنسبة تصل إلى خمسة بالمائة (5 بالمائة) من المبلغ الذي تمت تسويته في يوم واحد أو أكثر.
- زيادة إجمالي مبالغ التسوية اليومية للأحجام الواردة من الأعضاء بنسبة تصل إلى خمسة بالمائة (5 بالمائة) من المبلغ الذي تمت تسويته في يوم واحد أو أكثر.

قد يستمر هذا التحصيل طالما كان ضروريًا أو مناسبًا للوفاء بالتزامات الأعضاء غير المسرودة ولضمان سيولة النظام أو حتى يرى مشغل شبكة الدفع المحلية أن هذا التحصيل لم يعد ضروريًا أو مناسبًا. تعامل الأموال المحصلة على أنها مدفوعات مسبقة على المبالغ التي قد تكون مطلوبة من الأعضاء في التخصيص بين الأعضاء للخسارة المتعلقة بالتزامات الأعضاء غير المسرودة. وإذا تجاوزت الأموال المحصلة من أحد الأعضاء المبلغ المخصص له في النهاية فيما يتعلق بالتزامات العضو غير المعفي منها، فسيتم إعادة المبلغ الزائد إلى العضو مع الفائدة. إذا كانت الأموال المحصلة من أحد الأعضاء لا تتجاوز المبلغ المخصص له، فسوف يقوم العضو بدفع أي نقص لمشغل شبكة الدفع المحلية مع الفائدة. ستعتمد أي مدفوعات فائدة من أو إلى مشغل شبكة الدفع المحلية على السعر الذي يحدده مشغل شبكة الدفع المحلية، خلال الفترة بين حدوث تمويل العضو والتخصيص النهائي.

9.3.5 المسؤولية عن الكيانات المملوكة أو الخاضعة للسيطرة

(الفئة أ)

يجب على كل عضو (يشار إليه لأغراض هذه القاعدة باسم “العضو المسؤول”) أن يضمن بشكل نهائي وغير مشروط، بصفته ملتزمًا أساسيًا وليس مجرد ضمان لمشغل شبكة الدفع المحلية، وعلى جميع الأعضاء الآخرين، الدفع الفوري وأداء الالتزامات (“الالتزامات المضمونة”) لكل من الكيانات التابعة للعضو المسؤول الناشئة بموجب المعايير وعن أنشطة كل كيان تابع واستخدام أي من العلامات.

لأغراض تطبيق هذه القاعدة، يتم تعريف الكيان التابع للعضو المسؤول على النحو التالي:

1. عضو يملكه أو يتحكم فيه العضو المسؤول أو يملكه أو يتحكم فيه العضو المسؤول وعضو آخر أو أعضاء؛ أو
2. العضو الذي يخضع، مع العضو المسؤول، للملكية المشتركة لكيان آخر أو يتحكم فيه؛ أو

3. A Member that Owns or Controls the Responsible Member or shares Ownership or Control of the Responsible Member with another Member or Members.

The obligations of each Responsible Member under this Rule shall be continuing, absolute, and unconditional and shall not be discharged or impaired or otherwise affected by any act or omission (including any renewal, extension, amendment, waiver or unenforceability of any of the Guaranteed Obligations) that may vary the risk of such Responsible Member or otherwise operate as a discharge of the obligations of such Responsible Member as a matter of law or equity, and all defenses of the Responsible Member with respect thereto are waived to the fullest extent permitted by applicable law.

The Responsible Member's liability to the National Scheme Operator and all other Members is a primary obligation, while the National Scheme Operator's liability, if any, to another Member is secondary, in that it only arises if a Responsible Member is unable to pay its Guaranteed Obligations in full. Any assessments imposed on a Member for liability under this Rule may be collected by the National Scheme Operator, at its option, from the Member's settlement account or by any other means available. A Responsible Member may not be exempted from this Rule except upon written notice by the General Counsel of the National Scheme Operator.

5.3.10 Risk of Loss

(Category A)

Each Member bears all risk of loss and the National Scheme Operator bears no risk of loss with respect to all amounts owed by the Member related to the settlement except to the extent any such amount is received by the National Scheme Operator, free and clear.

Each Member remains fully responsible for fulfillment of, and must take all actions necessary to fulfill, all of its obligations under the Standards, regardless of whether the Member designates a Service Provider or other third party to perform all or any part of such obligations on the Member's behalf. The fact that a Member has paid any portion of any amount owed to any such third-party designee does not discharge any of the Member's obligations to the National Scheme Operator.

The National Scheme Operator may draw on the Member's funds to fulfill any one or more of the Member's obligations under the Standards, regardless of whether those funds are held or controlled by the Member or by any third party designee, to the same extent that the National Scheme Operator is entitled to draw on funds from any settlement account or funds of the Member in accordance with the Standards, and regardless of whether those funds are commingled with any other funds. If the National Scheme Operator draws on the Member's funds in accordance with the Standards, the National Scheme Operator is not required to reimburse the Member or any third party (whether a third party designee of the Member or another Member) for funds drawn which are owned by any of them or otherwise subject to any of their rights. The Member and any third party (whether a third-party designee of the Member or another Member) bear all risk and liability related to the funds drawn and must jointly and severally indemnify and hold the National Scheme Operator harmless from all liability and claims arising from any such draw of funds.

Each Member bears all risk of loss, and the National Scheme Operator bears no risk of loss with respect to all amounts owed by the National Scheme Operator to the Member under the Standards once the National Scheme Operator has discharged its settlement obligations, regardless of whether the payment is received by the Member or a third-party designee of the Member.

3. العضو الذي يملك أو يتحكم في العضو المسؤول أو يشارك في ملكية أو سيطرة العضو المسؤول مع عضو آخر أو أعضاء.

يجب أن تكون التزامات كل عضو مسؤول بموجب هذه القاعدة مستمرة ومطلقة وغير مشروطة، ولا يجوز الإبراء أو الاعفاء منها أو إضعافها أو تأثرها بأي فعل (بما في ذلك أي تجديد أو تمديد أو تعديل أو تنازل أو عدم قابلية تنفيذ أي من الالتزامات المضمنة) قد يغير من مخاطر هذا العضو المسؤول أو يعمل بطريقة أخرى كإبراء من التزامات هذا العضو المسؤول كمسألة قانونية أو حقوق ملكية، ويتم التنازل عن جميع دفاعات العضو المسؤول فيما يتعلق بذلك إلى أقصى حد يسمح به القانون المعمول به.

تعد مسؤولية العضو المسؤول تجاه مشغل شبكة الدفع المحلية، وجميع الأعضاء الآخرين التزامًا أساسيًا، في حين أن مسؤولية مشغل شبكة الدفع المحلية، إن وجدت، تجاه عضو آخر تعد مسؤولية ثانوية، من حيث أنها تنشأ فقط إذا كان العضو المسؤول غير قادر على سداد التزاماته المضمنة كلياً. قد يتم جمع أي تقييمات مفروضة على العضو فيما يتعلق بالمسؤولية بموجب هذه القاعدة بواسطة مشغل شبكة الدفع المحلية، وحسب اختياره، من حساب تسوية العضو أو بأي وسيلة أخرى متاحة. ولا يجوز إعفاء العضو المسؤول من هذه القاعدة إلا بناءً على إشعار مكتوب من قبل المستشار العام لمشغل شبكة الدفع المحلية.

10.3.5 مخاطر الخسارة

(الفئة أ)

يتحمل كل عضو جميع مخاطر الخسارة، ولا يتحمل مشغل شبكة الدفع المحلية أي مخاطر خسارة فيما يتعلق بجميع المبالغ المستحقة على العضو والمتعلقة بالتسوية باستثناء الحد الذي يتم فيه استلام أي مبلغ من هذا القبيل بواسطة مشغل شبكة الدفع المحلية، مجاناً وبشكل واضح.

يبقى كل عضو مسؤولاً مسؤولية كاملة عن الوفاء بجميع التزاماته بموجب المعايير، ويجب أن يتخذ جميع الإجراءات اللازمة للوفاء بها، وبغض النظر عما إذا كان العضو يعين مقدم خدمة أو طرفاً ثالثاً آخر لأداء كل أو جزء من هذه الالتزامات على نيابة عن العضو. وإثبات أن العضو قد دفع أي جزء من أي مبلغ مستحق لأي طرف ثالث معين لا يفي بأي من التزامات العضو تجاه مشغل شبكة الدفع المحلية.

يجوز لمشغل شبكة الدفع المحلية سحب من أموال العضو للوفاء بواحد أو أكثر من التزامات العضو بموجب المعايير، وبغض النظر عما إذا كانت هذه الأموال مملوكة أو في حيازة العضو أو أي طرف ثالث معين، إلى نفس الحد يحق لمشغل شبكة الدفع المحلية سحب الأموال من أي حساب تسوية أو أموال للعضو وفقاً للمعايير، وبغض النظر عما إذا كانت هذه الأموال ممزوجة بأي أموال أخرى. وإذا قام مشغل شبكة الدفع المحلية بسحب أموال العضو وفقاً للمعايير، فلا يلتزم مشغل شبكة الدفع المحلية بتعويض العضو أو أي طرف ثالث (سواء كان طرفاً ثالثاً معيناً للعضو أو عضواً آخر) عن الأموال المسحوبة المملوكة من قبل أي منهم أو خاضعاً لأي من حقوقهم. ويتحمل العضو وأي طرف ثالث (سواء كان طرفاً ثالثاً معيناً للعضو أو عضواً آخر) جميع المخاطر والمسؤوليات المتعلقة بالأموال المسحوبة، ويجب أن يقوم بالتضامن والتكافل بتعويض مشغل شبكة الدفع المحلية، وإبعاده عن جميع المسؤوليات والمطالبات الناشئة عن أي سحب أموال على هذا النحو.

يتحمل كل عضو جميع مخاطر الخسارة، ولا يتحمل مشغل شبكة الدفع المحلية أي مخاطر الخسارة فيما يتعلق بجميع المبالغ المستحقة على مشغل شبكة الدفع المحلية للعضو بموجب المعايير بمجرد وفاء مشغل شبكة الدفع المحلية بالتزامات التسوية، بغض النظر عما إذا كان يتم استلام الدفعة من قبل العضو أو من ينوب عن طرف ثالث للعضو.

Each Member must notify the National Scheme Operator promptly in writing if any third-party designee commingles funds received for or from the Member in connection with the Member's Transactions with any other funds. Each Member must notify the National Scheme Operator promptly in writing of the details of any failure of the Member or any third-party designee of the Member to meet any of their obligations with respect to payment of funds owed under the Standards.

If a Member's third party designee advances funds on behalf of the Member to pay the National Scheme Operator or any other party entitled to receive those funds in accordance with the Standards, then such payment is deemed to be a payment by the Member, and the Member, and the third party designee of the Member, jointly and severally bear all risks of loss and must jointly and severally indemnify and hold the National Scheme Operator harmless from any and all liability and claims arising from any such payment.

In addition to the other Member obligations set forth in this section, a Member must:

1. Obtain the prior written agreement of any third-party designee of the Member that may be given access to any funds owed by or to the Member pursuant to the Standards; and
2. Be responsible for any such third-party designee's compliance with all applicable Standards, including those set forth in this Rule.

5.3.11 Adjustment of Settlement Positions—Loss Allocation Among Members

(Category A)

Any loss that the National Scheme Operator incurs, or for which the National Scheme Operator may otherwise be responsible due to the failure of a Member, whether or not intentional, to perform any of its Participation obligations, may be allocated among the Members by the National Scheme Operator in such manner and at such times as the National Scheme Operator determines to be appropriate. Such allocation may be funded by application of available mitigants and options to cover the loss, including but not limited to the following:

- Netting the issuing and acquiring obligations of the defaulting Member;
- Applying to the defaulting Member any Standards relating to Member payments of fees, assessments, and other payment obligations (as may be amended from time to time);
- Applying any collateral of the defaulting Member that is for the benefit of the National Scheme Operator;
- Applying any applicable recovery mechanisms such as regulatory protections (for example, governmental resolution regimes or depository insurance) or commercial arrangements with or by the defaulting Member (i.e., trusts or escrows of settlement funds, insurance policies against failure);
- Applying Rule 9.3.11, Liability for Owned or Controlled Entities (as may be amended from time to time) to the defaulting Member;

Should the actions above not fully cover a loss, the National Scheme Operator may commit a portion of its capital toward the loss. The amount of any capital contribution by the National Scheme Operator will be determined by the National Scheme Operator, at its sole discretion, based on the circumstances at the time of the loss.

After application of any capital contribution by the National Scheme Operator any residual losses may be allocated among Members by the National Scheme Operator in such manner as the National Scheme Operator deems to be appropriate, with the objective of minimizing the risk to the overall payment system.

يجب على كل عضو إخطار مشغل شبكة الدفع المحلية على الفور وبطريقة مكتوبة إذا قام أي طرف ثالث معين، بدمج الأموال المستلمة من العضو أو منه فيما يتعلق بمعاملات العضو مع أي أموال أخرى. ويجب على كل عضو إخطار مشغل شبكة الدفع المحلية على الفور وبطريقة مكتوبة بتفاصيل أي إخفاق من جانب العضو أو أي طرف ثالث ينوب عن العضو في الوفاء بأي من التزاماته فيما يتعلق بدفع الأموال المستحقة بموجب المعايير.

إذا قام الطرف الثالث الذي ينوب عن العضو بتقديم أموال نيابة عن العضو لدفع أموال لمشغل شبكة الدفع المحلية أو أي طرف آخر يحق له تلقي هذه الأموال وفقاً للمعايير، فإن هذا الدفع يعتبر قد تم دفعة من قبل العضو، ويتحمل العضو والطرف الثالث المعين من قبل العضو المسؤولية التضامنية عن جميع مخاطر الخسارة ويجب أن يقوم بالتضامن والتكافل عند تعويض مشغل شبكة الدفع المحلية وإبعاده عن أي وجميع المسؤوليات والمطالبات الناشئة عن أي مدفوعات من هذا القبيل.

بالإضافة إلى التزامات العضو الأخرى المنصوص عليها في هذا القسم، يجب على العضو:

1. الحصول على موافقة مكتوبة مسبقاً من أي طرف ثالث معين للعضو يمكن منحه حق الوصول إلى أي أموال مستحقة على العضو أو له وفقاً للمعايير.
2. أن يكون مسؤولاً عن امتثال أي طرف ثالث معين من هذا القبيل لجميع المعايير المعمول بها، بما في ذلك تلك المنصوص عليها في هذه القاعدة.

11.3.5 تعديل أوضاع التسوية - تخصيص الخسارة بين الأعضاء

(الفئة أ)

أي خسارة يتكبدها مشغل شبكة الدفع المحلية، أو قد كان مسؤولاً عنها بخلاف ذلك بسبب فشل العضو، سواء أكان ذلك عن قصد أم عن تقصير في أداء أي من التزامات المشاركة الخاصة به، فإنه يجوز توزيعها بين الأعضاء بواسطة مشغل شبكة الدفع المحلية بالطريقة، وفي الأوقات التي يقرر مشغل شبكة الدفع المحلية أنها مناسبة.

يمكن تمويل هذا التخصيص من خلال تطبيق وسائل التخفيف المتاحة والخيارات لتغطية الخسارة، بما في ذلك على سبيل المثال لا الحصر ما يلي:

- معاوضة إصدار واستحواد التزامات العضو المتعثر.
- تطبيق أي معايير على العضو المتخلف عن السداد تتعلق بمدفوعات الأعضاء للرسوم، والاشتراكات، والالتزامات الدفع الأخرى (التي قد يتم تعديلها من وقت لآخر).
- تطبيق أي ضمانات للعضو المتخلف تكون لصالح مشغل شبكة الدفع المحلية.
- تطبيق أي آليات استرداد قابلة للتطبيق مثل الحماية التنظيمية (على سبيل المثال، أنظمة القرارات الحكومية أو تأمين الإيداع) أو الترتيبات التجارية مع أو من قبل العضو المتخلف (أي الصناديق الاستثمارية أو الضمانات الخاصة بأموال التسوية، وبواليص التأمين ضد الفشل).
- تطبيق القاعدة 11.3.9 ، المسؤولية عن الكيانات المملوكة أو الخاضعة للسيطرة (كما قد يتم تعديلها من وقت لآخر) على العضو المتخلف.

إذا لم تغطي الإجراءات المذكورة أعلاه الخسارة بالكامل، فقد يلتزم مشغل شبكة الدفع المحلية بجزء من رأس ماله تجاه الخسارة. سيتم تحديد مبلغ أي مساهمة رأسمالية من قبل مشغل شبكة الدفع المحلية وفقاً لسلطته التقديرية، وبناءً على الظروف في وقت الخسارة

بعد تطبيق أي مساهمة رأسمالية من قبل مشغل شبكة الدفع المحلية، قد يتم تخصيص أي خسائر متبقية بين الأعضاء من قبل مشغل شبكة الدفع المحلية بالطريقة التي يراها مناسبة، وذلك بهدف تقليل المخاطر على نظام الدفع العام.

Any allocations of losses to Members under this Rule will be collected by appropriately adjusting Member settlement positions. Decisions on which Members will receive an allocation, and the size of the allocation to be included in the settlement positions of individual Members will be based on considerations including, but not limited to:

- The guaranteed issuing volume of each Member on Cards or Access Devices, and/or in total; and
- The guaranteed acquiring volume of each Member.

5.3.11 Settlement Noncompliance—Cost Reimbursement, Noncompliance Assessments, and Compensation

(Category A)

5.3.11.1 Cost Reimbursement to the National Scheme Operator

The National Scheme Operator reserves the right to collect any costs related from a Member's failure to comply with the Standards, on behalf of and at the direction of the National Scheme Operator's settlement Service Provider.

Each Member shall, at the demand of the National Scheme Operator or its settlement Service Provider, refund to the National Scheme Operator any and all costs including, but not limited to interest, fees, taxes, compensation, assessments, or other costs paid by the National Scheme Operator to its settlement Service Provider or other person, entity, or local governing authority on account of such Member's failure to comply with the Standards.

In addition to these costs, the National Scheme Operator may also charge administrative or noncompliance fees, interest, or other administrative charges for the collection of such fees related to a Member's failure to comply with the Standards. The National Scheme Operator reserves the right to charge the Member a two percent surcharge assessed on any amount the National Scheme Operator collects on behalf of its settlement Service Provider or other person, entity, or local governing authority on account of such Member's failure to comply with the Standards.

5.3.11.2 Settlement Noncompliance Assessments

The National Scheme Operator reserves the right to levy settlement noncompliance assessments against any Member that:

- fails to transfer funds by the specified value date to the National Scheme Operator settlement Service Provider, or
- negatively impacts the settlement position of another Member or Members as a result of Transaction submissions into the Clearing System for erroneous amounts

Settlement noncompliance assessments are calculated based on the LYD settlement equivalent amount, and are applied on the first day, and each subsequent day thereafter, that a Member fails to transfer funds in a timely manner and in agreement with proper settlement procedures. Members with multiple Member IDs will be assessed separately for each individual Member ID that has failed settlement.

In addition, the National Scheme Operator may impose interest compensation against a Member for settlement underpayments resulting in unjust enrichment of the Member, as appropriate.

سيتم تحصيل أي مخصصات للخسائر للأعضاء بموجب هذه القاعدة عن طريق تعديل أوضاع تسوية الأعضاء بشكل مناسب. والقرارات التي بموجبها سيتلقى الأعضاء تخصيصًا، وسيستند حجم التخصيص الذي سيتم تضمينه في مواقف التسوية الخاصة بالأعضاء الفرديين إلى اعتبارات تشمل، على سبيل المثال لا الحصر:

- حجم الإصدار المضمون لكل عضو على البطاقات أو أجهزة الوصول، و بشكل إجمالي.
- حجم القبول المضمون لكل عضو.

11.3.5 عدم الامتثال للتسوية — سداد التكاليف، تقييمات عدم الامتثال والتعويضات

(الفئة أ)

1.11.3.5 سداد التكاليف لمشغل شبكة الدفع المحلية

يحتفظ مشغل شبكة الدفع المحلية بالحق في تحصيل أي تكاليف مرتبطة بفشل العضو في الامتثال للمعايير، نيابة عن مقدم خدمة تسوية مشغل شبكة الدفع المحلية وبتوجيه منه.

يجب على كل عضو، بناءً على طلب مشغل شبكة الدفع المحلية أو مقدم خدمة التسوية الخاص به، أن يعيد إلى مشغل شبكة الدفع المحلية جميع التكاليف بما في ذلك، على سبيل المثال، الفوائد أو الرسوم أو الضرائب أو التعويضات أو التقييمات أو التكاليف الأخرى التي يدفعها مشغل شبكة الدفع المحلية لمقدم خدمة التسوية أو أي شخص أو كيان أو سلطة حاكمة محلية أخرى بسبب فشل هذا العضو في الامتثال للمعايير.

بالإضافة إلى هذه التكاليف، يجوز لمشغل شبكة الدفع المحلية أيضًا فرض رسوم إدارية أو رسوم عدم الامتثال أو الفائدة أو الرسوم الإدارية الأخرى لتحصيل هذه الرسوم المتعلقة بفشل العضو في الامتثال للمعايير. ويحتفظ مشغل شبكة الدفع المحلية بالحق في تحميل العضو رسومًا إضافية بنسبة 2% مقسمة على أي مبلغ يجمعه مشغل شبكة الدفع المحلية نيابة عن مقدم خدمة التسوية أو أي شخص أو كيان أو سلطة حاكمة محلية أخرى بسبب فشل هذا العضو في الامتثال لها للمعايير.

2.11.3.5 تقييمات عدم الامتثال للتسوية

يحتفظ مشغل شبكة الدفع المحلية بالحق في فرض تقييمات عدم الامتثال للتسوية ضد أي عضو:

- فشل في تحويل الأموال بحلول تاريخ القيمة المحدد إلى مقدم خدمة تسوية مشغل شبكة الدفع المحلية.
- يؤثر سلبيًا على موقف التسوية لعضو آخر أو أعضاء نتيجة لتقديم المعاملات في نظام المقاصة للمبالغ الخاطئة.

يتم احتساب تقييمات عدم الامتثال للتسوية بناءً على مبلغ تسوية بالدينار الليبي، ويتم تطبيقها في اليوم الأول، وفي كل يوم لاحق بعد ذلك يفشل فيه العضو في تحويل الأموال في الوقت المناسب وبما يتفق مع إجراءات التسوية المناسبة.

سيتم تقييم الأعضاء الذين لديهم عدة معرفات أعضاء بشكل منفصل لكل معرف عضو فردي فشل في التسوية.

بالإضافة إلى ذلك، يجوز لمشغل شبكة الدفع المحلية فرض تعويض فائدة ضد أحد الأعضاء لتسوية المدفوعات الناقصة التي أدت إلى إثراء غير عادل للعضو، حسب الاقتضاء.

Settlement Noncompliance Assessment Calculations

The following table contains the assessment schedule for Members that fail to settle on the appropriate value date:

(See appendix number 39)

The National Scheme Operator will assess a multi-penalty fee when a Member fails settlement more than two (2) times in a 30-day period. For each failure after the second failure for the same Member ID, the assessment will be LYD XXXXX for each occurrence. This includes when a Member fails the cutoff deadline three or more times in a 30-day period.

The National Scheme Operator assesses an LYD XXXX processing fee for funds transfer exceptions. Examples include, but are not limited to, overpayment refunds and funds collection re-presentments.

5.3.11.3 Compensation

Members or the National Scheme Operator may be reimbursed regarding the use of funds during settlement. Compensation means:

- Reimbursement to a Member from the National Scheme Operator if the Member has lost the use of funds.

The National Scheme Operator computes compensation owed to a Member using the appropriate daily effective Settlement Agent Earnings Credit Rate in place during the failure period.

- Reimbursement to the National Scheme Operator from a Member if the Member had use of funds to which it was not entitled.

The National Scheme Operator will calculate the amount of interest compensation due by assessing two percent more than the overdraft rate charged to the National Scheme Operator by its settlement Service Provider.

Compensation Calculations

Compensation paid to the Membership will be computed as follows.

(See appendix number 40)

Compensation to the National Scheme Operator will be collected for the period from the date the transfer was due through the date that the respective funds are transferred correctly to the National Scheme Operator net settlement account, as follows.

(See appendix number 41)

NOTE: “Number of Days” includes the date a Member or the National Scheme Operator fails to make payment of funds owed and includes the date the Member or the National Scheme Operator pays funds owed, including weekends and holidays.

5.4 Transaction Requirements and Processing Procedures

5.4.1 Authorization Service

5.4.1.1 Acquirer Authorization Requirements

An Acquirer and each of its Merchants must support POS Transactions (and a full reversal when performed to cancel a POS Transaction that the Acquirer cannot complete due to a technical problem.

An Acquirer may also support, and its Merchants may optionally offer, the following Transaction and message types, in compliance with applicable Standards:

حسابات تقييم عدم الامتثال للتسوية

يحتوي البيان التالي على جدول التقييم للأعضاء الذين فشلوا في التسوية في تاريخ القيمة المناسب: (انظر الملحق رقم 39)

يقوم مشغل شبكة الدفع المحلية بتقييم رسوم متعددة العقوبات عندما يفشل العضو في التسوية أكثر من مرتين (2) في فترة 30 يومًا. لكل فشل بعد الفشل الثاني لنفس معرف العضو، سيكون التقييم XXXXX دينار ليبي لكل تكرار. وهذا يشمل عندما يفشل العضو في الموعد النهائي للقطع ثلاث مرات أو أكثر في فترة 30 يومًا.

يقوم مشغل شبكة الدفع المحلية بتقييم رسوم المعالجة XXXX دينار ليبي لاستثناءات تحويل الأموال. على سبيل المثال لا الحصر، المبالغ المستردة والزائدة وإعادة التقديم لتحصيل الأموال.

3.11.3.5. التعويض

يجوز تعويض الأعضاء أو مشغل شبكة الدفع المحلية فيما يتعلق باستخدام الأموال أثناء التسوية. التعويض يعني:

- السداد لعضو من مشغل شبكة الدفع المحلية إذا فقد العضو استخدام الأموال.
- ويحسب مشغل شبكة الدفع المحلية التعويض المستحق للعضو باستخدام معدل ائتمان أرباح وكيل التسوية الفعال المناسب الساري خلال فترة الفشل.
- السداد لمشغل شبكة الدفع المحلية من أحد الأعضاء إذا كان العضو قد استخدم الأموال التي لا يحق له الحصول عليها.

سيحسب مشغل شبكة الدفع المحلية مبلغ تعويض الفائدة المستحق عن طريق تقييم 2 في المائة أكثر من معدل السحب على المكشوف الذي يفرضه مقدم خدمة التسوية على مشغل شبكة الدفع المحلية.

حسابات التعويض

سيتم احتساب التعويضات المدفوعة للعضوية على النحو التالي.

(انظر الملحق رقم 40)

سيتم تحصيل التعويض لمشغل شبكة الدفع المحلية عن الفترة من تاريخ استحقاق التحويل حتى تاريخ تحويل الأموال المعنية بشكل صحيح إلى حساب التسوية الصافي لمشغل شبكة الدفع المحلية، على النحو التالي.

(انظر الملحق رقم 41)

ملاحظة: “عدد الأيام” يشمل التاريخ الذي يفشل فيه العضو أو مشغل شبكة الدفع المحلية في سداد الأموال المستحقة ويتضمن التاريخ الذي يدفع فيه العضو أو مشغل شبكة الدفع المحلية الأموال المستحقة، بما في ذلك عطلات نهاية الأسبوع والعطلات.

4.5. متطلبات المعاملات وإجراءات المعالجة

1.4.5. خدمة التفويض

1.1.4.5. متطلبات تفويض جهة القبول

يجب على جهة القبول، وكل من التجار التابعين له دعم معاملات نقاط البيع (والإلغاء الكامل عند إجرائه لإلغاء معاملة نقطة البيع التي لا تستطيع جهة القبول إكمالها بسبب مشكلة فنية. قد تدعم جهة القبول أيضًا، ويجوز لتجاره بطريقة اختيارية أن يقدموا أنواع المعاملات والرسائل التالية، بما يتوافق مع المعايير المعمول بها:

- Purchase with cash back Transactions
- Deferred authorization
- Full reversal, including cancellation, and partial reversal
- balance inquiry
- refund Transactions

5.4.1.2 Acquirer Host System Requirements

An Acquirer must ensure that its POS Terminal host systems and those of its Service Providers: (As a mandate for today all POS terminals are driven by National Scheme operator)

1. Are capable of processing Contact Chip Transactions and Contactless Transactions ;
2. Support the transmission of Contact Chip Transaction and Contactless Transaction messages in accordance with the Standards;
3. Support online PIN and signature as CVM options for Chip Transactions, regardless of whether each Hybrid POS Terminal connected to the Acquirer host system supports these options;
4. Support all mandatory and applicable conditional data subelements within DE 55 (Integrated Circuit Card [ICC] System-Related Data); and
5. Have been approved by the National Scheme Operator, with respect to each Interchange System network interface, as enabled for Contact Chip Transaction and Contactless Transaction processing.

5.4.1.3 Issuer Authorization Requirements

The Issuer of a Card Program that provides cash access at ATMs:

1. Must support POS Transaction authorizations and preauthorizations.
 2. Must offer cash withdrawal, purchase of Merchandise and cash advances to Cardholders.
 3. May offer, at its option, balance inquiry and transfers to and from a Cardholder’s accounts.
- In the event that an Issuer chooses not to offer a particular Transaction message type to its Cardholders, the Issuer must provide a value of 57 indicating “Transaction not permitted to Issuer/Cardholder” in DE 39 (Response Code) of the online authorization message.
- An Issuer must decline authorization of a Transaction when technical fallback from chip to magnetic stripe occurred.

ATM Cash Withdrawal Amounts

The Issuer determines the maximum cash withdrawal limits applicable to its Cardholders; however, the Issuer must permit its Cardholders to withdraw at least the equivalent of LYD XXX daily if the available credit exists, and there is no other reason to deny the Transactions. To accommodate ATM Access Fees, the Issuer must authorize Transactions up to the equivalent of LYD XXX or XX %, whichever is greater, more than the daily Transaction amount limit communicated to the Cardholder.

5.4.1.4 Issuer Host System Requirements

An Issuer’s host system interfaces must support the online processing of:

- POS Transactions
- Refund Transactions
- Reversal and correction requests
- Cash withdrawals and the purchase of Merchandise at ATMs and Bank Branch Terminals

- الشراء مع المعاملات النقدية.
- الإذن المؤجل.
- إلغاء كامل، بما في ذلك الإلغاء، والإلغاء الجزئي.
- الاستفسار عن الرصيد.
- معاملات الاسترداد.

2.1.4.5 متطلبات نظام مضيف جهة القبول

يجب على جهة القبول التحقق من أن أنظمة مضيف محطات نقاط البيع وأنظمة مقدمي الخدمة الخاصة به: (كتفويض اليوم، يتم تشغيل جميع محطات نقاط البيع بواسطة مشغل شبكة الدفع المحلية)

1. قادرة على معالجة معاملات شريحة الاتصال والمعاملات التي تتم عن بعد.
2. دعم نقل معاملات شريحة الاتصال ورسائل المعاملات عن بعد وفقًا للمعايير.
3. دعم رقم التعريف الشخصي والتوقيع الإلكتروني كخيارات CVM لمعاملات الشريحة، بغض النظر عما إذا كانت كل محطة نقاط بيع متصلة بنظام مضيف جهة الإصدار تدعم هذه الخيارات.
4. دعم جميع العناصر الفرعية للبيانات الشرطية الإلزامية والقابلة للتطبيق داخل DE 55 (بطاقة الدوائر المتكاملة [ICC] البيانات المتعلقة بالنظام)، و
5. تمت الموافقة عليها من قبل مشغل شبكة الدفع المحلية، فيما يتعلق بكل واجهة شبكة لنظام التبادل، كما تم تمكينه لمعاملات شريحة الاتصال ومعالجة المعاملات التي تتم عن بعد.

3.1.4.5 متطلبات تفويض جهة الإصدار

- جهة إصدار برنامج البطاقة الذي يوفر الوصول النقدي في أجهزة الصراف الآلي:
1. يجب أن تدعم عمليات التفويضات والتفويضات المسبقة لمعاملة نقاط البيع.
 2. يجب تقديم السحب النقدي وشراء البضائع والسلف النقدية لحاملي البطاقات.
 3. قد يعرض، حسب اختياره، الاستعلام عن الرصيد والتحويلات من وإلى حسابات حامل البطاقة.
- وفي حالة اختيار جهة الإصدار عدم تقديم رسالة لنوع معين من المعاملات إلى حاملي البطاقات، يجب أن تقدم قيمة 57 التي تشير إلى أن “المعاملة غير مصرح بها لجهة الإصدار/ حامل البطاقة” في DE 39 (رمز الاستجابة) لرسالة التفويض عبر الإنترنت.
- يجب أن ترفض جهة الإصدار تفويض المعاملة عند حدوث تراجع فني من الشريحة إلى الشريط المغناطيسي.

قيمة مبالغ السحب النقدي من أجهزة الصراف الآلي

تحدد جهة الإصدار الحدود العليا للسحب النقدي المطبقة على حاملي البطاقات؛ ومع ذلك، يجب أن تسمح جهة الإصدار لحاملي بطاقتها بسحب ما لا يقل عن XXX دينار ليبي يوميًا إذا كان الرصيد متاح موجودًا، ولا يوجد سبب آخر لرفض المعاملات.

ولاستيعاب رسوم الوصول إلى أجهزة الصراف الآلي، يجب أن تفوض جهة الإصدار المعاملات بما يعادل XXX دينار ليبي أو XX %، أيهما أعلى، أكثر من حد مبلغ المعاملة اليومي المرسل إلى حامل البطاقة.

4.1.4.5 متطلبات نظام مضيف جهة الإصدار

يجب أن تدعم واجهات النظام المضيف لجهة الإصدار المعالجة عبر الإنترنت لما يلي:

- معاملات نقاط البيع.
- معاملات الاسترداد.
- طلبات الإلغاء والتصحيح.
- السحب النقدي وشراء البضائع من أجهزة الصراف الآلي ومحطات فروع المصارف.

5.4.2 Connecting to the Interchange System

(Category A)

A Member must maintain the necessary equipment and procedures to process Transactions and to connect to the Interchange System, using a telecommunications circuit established by the Interchange System that is equipped with backup service. Before processing Transactions and on an ongoing basis thereafter, the Member must perform testing and obtain any necessary certifications of its equipment, procedures, and Interchange System connections as may be required by the National Scheme Operator to ensure compatibility with its technical specifications then in effect.

Each Principal Member must establish and maintain, at its own expense, a data processing facility that is capable of receiving, storing, processing, and communicating any Transaction sent to or received from the Interchange System, and may connect at least one data processing facility directly to the Interchange System. Such facility may be established and maintained by the Member's parent, its wholly-owned subsidiary, or an entity that is wholly owned, directly or indirectly, by the Member's parent, or with the prior written agreement of the National Scheme Operator, by the Member's designated third party Service Provider.

5.4.2.1 Terminal Connectivity to the Interchange System

Except as otherwise provided in the Standards, each Member that acquires any ATM Transactions must always make available for connection to the Interchange System all of the eligible ATMs established by that Member (including its parents, subsidiaries, affiliates, and Sponsored entities) in Libya.

5.4.3 Authorization Routing

(Category A)

5.4.3.1 National Scheme Operator BINs

On an ongoing basis, an Acquirer must recognize and use all active National Scheme Operator bank identification numbers (BINs) for purposes of obtaining Transaction authorizations, and obtain such authorizations on behalf of each of its Merchants and ATM operators as the Standards require. The Acquirer must use Account range files provided by the National Scheme Operator for this purpose. Such files must be used by the Acquirer, its Merchants, and any entities that handle Account range files on behalf of the Acquirer or the Acquirer's Merchant within six calendar days from the date that each updated file is made available by the National Scheme Operator.

After downloading an updated Account range file from the National Scheme Operator, an Acquirer must return an acknowledgment to the National Scheme Operator confirming that:

- The Acquirer has updated its systems accordingly; and
- Each of the Acquirer's Merchants and entities that handle Account range files on behalf of the Acquirer or the Acquirer's Merchant have updated their systems accordingly as well.

Alternatively, the Acquirer must submit all authorization requests containing an Account number with a BIN in the National Scheme Operator BIN range to the Interchange System for routing to the Issuer.

This provision does not apply with respect to a Domestic Transaction for which the Issuer and Acquirer is the same Member (an "on-us" Transaction).

2.4.5 التوصليل بنظام التبادل

(الفئة أ)

يجب على العضو صيانة المعدات، وتحديث الإجراءات اللازمة لمعالجة المعاملات والاتصال بنظام التبادل، باستخدام دائرة اتصالات أنشأها نظام التبادل المجهز بخدمة النسخ الاحتياطي. وقبل معالجة المعاملات وبطريقة مستمرة، يجب على العضو إجراء الاختبارات، والحصول على أي شهادات ضرورية لمعداته وإجراءاته وتوصيلات نظام التبادل كما قد يطلبه مشغل شبكة الدفع المحلية لضمان التوافق مع المواصفات الفنية السارية في ذلك الوقت.

يتحمل كل عضو رئيسي وعلى نفقه الخاصة، تكاليف إنشاء وصيانة، مرفق معالجة بيانات قادر على تلقي وتخزين ومعالجة وإبلاغ أي معاملة يتم إرسالها أو استلامها من نظام التبادل، ويمكنه توصيل مرفق معالجة بيانات واحد على الأقل مباشرة إلى نظام التبادل. وقد يتم إنشاء هذه التسهيلات والاحتفاظ بها من قبل الشركة الأم للعضو، أو الشركة الفرعية المملوكة لها بالكامل، أو كيان مملوك بالكامل، بشكل مباشر أو غير مباشر، من قبل الشركة الأم للعضو، أو بموافقة مكتوبة مسبقة من مشغل شبكة الدفع المحلية، من قبل العضو. مقدم خدمة الطرف الثالث المعين.

1.2.4.5 التوصليل الطرفي بنظام التبادل

باستثناء ما هو منصوص عليه، خلّافاً لذلك في المعايير، يجب على كل عضو يحصل على معاملات أجهزة الصراف الآلي أن يتيح دائماً الاتصال بنظام التبادل جميع أجهزة الصراف الآلي المؤهلة التي أنشأها ذلك العضو (بما في ذلك الشركات الرئيسية وفروعها والشركات التابعة والكيانات الراعية) في ليبيا.

3.4.5 توجيه التفويض

(الفئة أ)

1.3.4.5 أرقام التعريف المصرفية لمشغل شبكة الدفع المحلية

يجب على جهة القبول بطريقة مستمرة، التعرف على جميع أرقام التعريف المصرفية لمشغل شبكة الدفع المحلية النشطة (BINs) واستخدامها لأغراض الحصول على تفويضات المعاملات، والحصول على هذه التفويضات نيابة عن كل من التجار ومشغلي أجهزة الصراف الآلي كما تتطلب المعايير. يجب على جهة القبول أن تستخدم ملفات نطاق الحساب التي يوفرها مشغل شبكة الدفع المحلية لهذا الغرض. ويجب استخدام هذه الملفات من قبل جهة القبول، وتجاره وأي كيانات تتعامل مع ملفات نطاق الحساب نيابة عن جهة القبول أو التاجر القابل خلال ستة أيام تقويمية من تاريخ إتاحة كل ملف محدث بواسطة مشغل شبكة الدفع المحلية. وبعد تنزيل ملف نطاق حساب محدث من مشغل شبكة الدفع المحلية، يجب على جهة القبول إعادة إقرار إلى مشغل شبكة الدفع المحلية يؤكد ما يلي:

- قامت جهة الاصدار بتحديث أنظمتها وفقاً لذلك.
- قام كل من تجار وكيانات جهة القبول الذين يتعاملون مع ملفات نطاق الحساب نيابة عنها، أو عن التاجر القابل بتحديث أنظمتهم وفقاً لذلك أيضاً.

بدلاً من ذلك، يجب على جهة القبول إرسال جميع طلبات التفويض التي تحتوي على رقم حساب برقم تعريف شخصي (BIN) في نطاق رقم التعريف المصرفي لمشغل شبكة الدفع المحلية إلى نظام التبادل للتوجيه إلى جهة الاصدار.

لا ينطبق هذا الحكم فيما يتعلق بالمعاملة المحلية التي تكون فيها جهة الاصدار أو القبول هما نفس العضو (معاملة "داخلية").

5.4.3.2 Chip-based Transactions

Any chip-based Transaction generated by an Application Identifier (AID) owned or licensed to the National Scheme Operator must be routed through the Interchange System, or as otherwise approved by the National Scheme Operator.

This provision does not apply with respect to a Domestic Transaction for which the Issuer and Acquirer is the same Member (an “on-us” Transaction).

5.4.3.3 Routing Instructions and System Maintenance

Each Member or its Sponsor must:

1. Submit to the National Scheme Operator completed authorization routing instruction documentation no later than five business days prior to the requested effective date of live processing via the Interchange System.
2. Notify the National Scheme Operator of any routing updates at least five business days before the effective date of the change. Expedited maintenance may be performed within two business days of such notice.
3. Notify the National Scheme Operator of any scheduled downtime at least 24 hours in advance.

5.4.4 Stand-In Processing Service

(Category A)

An Issuer is liable for all Transactions authorized (with or without PIN validation) using the Stand-In Processing Service. The Issuer may establish Stand-In Processing Service PIN validation at its option.

For all of its [product] Card Programs, an Issuer must use the Stand-In Processing Service. Stand-In Parameters for [product] Card Programs must be set at or above the National Scheme Operator’s default limits.

In the event that fraudulent activity is detected with respect to a National Scheme Operator BIN or BIN range, the National Scheme Operator, in its sole discretion and judgment, may take such action as the National Scheme Operator deems necessary or appropriate to safeguard the goodwill and reputation of the National Scheme Operator’s Marks. Such action may include, by way of example and not limitation, declining some or all Transaction authorization requests received by the Stand-in Processing Service relating to the use of Cards issued under such National Scheme Operator BIN or BIN range.

An Issuer may employ a blocking service which declines all Transaction authorization requests during Stand-In processing for inactive BINs or in situations where Stand-In processing does not apply for regulatory reasons.

5.4.5 Obtaining an Authorization

5.4.5.1 Card-Not-Present Transaction Declines

(Category A)

If a Merchant initiates an authorization request for a Card-not-present Transaction and the Acquirer receives any one of the following declined responses in DE 39 (Response Code) of the Issuer’s authorization request response message, the Merchant must not initiate any additional authorization requests for the same Transaction with the same PAN and expiration date at any time:

2.3.4.5. المعاملات القائمة على الشرائح

يجب أن يتم توجيه أي معاملة قائمة على الشريحة تم إنشاؤها بواسطة معرف التطبيق (AID) المملوك أو المرخص لمشغل شبكة الدفع المحلية من خلال نظام التبادل، أو على النحو المعتمد من قبل مشغل شبكة الدفع المحلية.

لا ينطبق هذا الحكم فيما يتعلق بالمعاملة المحلية التي تكون فيها جهة الاصدار أو القبول هما نفس العضو (معاملة “داخلية”).

3.3.4.5. تعليمات التوجيه وصيانة النظام

يجب على كل عضو أو راعيه:

1. القيام بتقديم كل المستندات المتعلقة بتعليمات توجيه التفويض إلى مشغل شبكة الدفع المحلية في موعد لا يتجاوز خمسة أيام عمل قبل التاريخ الفعلي المطلوب للمعالجة المباشرة عبر نظام التبادل.
2. القيام بإشعار مشغل شبكة الدفع المحلية بأي تحديثات للتوجيه قبل خمسة أيام عمل على الأقل من تاريخ نفاذ التغيير. ويمكن إجراء الصيانة المستعجلة خلال يومي عمل من هذا الإشعار.
3. إشعار مشغل شبكة الدفع المحلية بأي وقت تعطل فيه مجدول قبل 24 ساعة على الأقل.

4.4.5. خدمة المعالجة الاحتياطية

(الفئة أ)

جهة الاصدار هي المسؤولة عن جميع المعاملات المصرح بها (مع أو بدون التحقق من صحة رقم التعريف الشخصي) باستخدام خدمة المعالجة الاحتياطية. ويجوز للجهة الاصدار إنشاء التحقق من صحة رقم التعريف الشخصي لخدمة المعالجة الاحتياطية حسب اختيارها.

بالنسبة لجميع برامج بطاقات [المنتج]، يجب على جهة الاصدار استخدام خدمة المعالجة الاحتياطية. ويجب تعيين معلومات الاستعداد لبرامج بطاقة [المنتج] عند أو أعلى من الحدود الافتراضية لمشغل شبكة الدفع المحلية.

في حالة اكتشاف نشاط احتيالي فيما يتعلق بنطاق BIN أو BIN لمشغل شبكة الدفع المحلية، فإنه يجوز لمشغل شبكة الدفع المحلية، طبقاً لسلطته التقديرية، اتخاذ مثل هذا الإجراء الذي يراه ضرورياً أو مناسباً لحماية شهرة و سمعة علامات مشغل شبكة الدفع المحلية. وقد يشمل هذا الإجراء، على سبيل المثال، رفض بعض أو كل طلبات تفويض المعاملة التي تتلقاها خدمة المعالجة الاحتياطية والمتعلقة باستخدام البطاقات الصادرة بموجب نطاق BIN أو BIN لمشغل شبكة الدفع المحلية. يجوز لجهة الاصدار استخدام خدمة حظر ترفض جميع طلبات تفويض المعاملة أثناء المعالجة الاحتياطية لأرقام التعريف المصرفية غير النشطة أو في الحالات التي لا تنطبق فيها المعالجة الاحتياطية لأسباب تنظيمية.

5.4.5 الحصول على تفويض

1.5.4.5. رفض معاملة البطاقة غير الموجودة

(الفئة أ)

إذا بدأ التاجر طلب تفويض لمعاملة بطاقة غير الموجودة وتلقت جهة القبول أيًا من الردود المرفوضة التالية في DE 39 (رمز الاستجابة) لرسالة رد طلب التفويض من جهة الاصدار، يجب على التاجر عدم بدء طلبات تفويض إضافية لنفس المعاملة بنفس رقم الحساب الأساسي (PAN) وتاريخ انتهاء الصلاحية في أي وقت:

- 04 Capture card
- 14 Invalid card number
- 15 Invalid Issuer
- 41 Lost card
- 43 Stolen card
- 54 Expired card

5.4.5.2 Use of Card Validation Number (CVV) 2

(Category B)

A Merchant must not prompt or otherwise require a Cardholder to enter CVV 2 information when a Chip Card or Contactless Payment Device is used to complete a Chip Transaction at a POS Terminal or MPOS Terminal.

In a Card-not-present environment, a Merchant may request Card validation code (CVV) 2 verification from the Issuer, as a means to check the validity of a Card.

CVV 2 data must not be stored by the Merchant, its Acquirer, or any Service Provider.

5.4.6 Authorization Responses

Every authorization request receives an authorization response that directs the Acquirer or the Merchant on how to proceed with the Transaction.

The response received is typically a code that identifies the action that the Merchant should take.

This code informs the Acquirer of the action to be taken (approve, decline, refer to card Issuer, capture card, or valid).

Regardless of the format in which the authorization response is received, the response always prompts one of the following actions on the part of the Merchant:

- Approve
- Decline
- Refer to card Issuer
- Capture card
- Valid (not declined)—used for non-financial Transaction types only

5.4.6.1 Approve Response

The approve response means the Transaction is authorized.

For magnetic stripe, chip, and key-entered Transactions, the Issuer provides a six-digit authorization code to the Acquirer when it approves a Transaction for the purchase of goods or services or a cash disbursement. The Merchant still must perform its normal review process before completing the Transaction.

5.4.6.2 Decline Response

The decline response means the Merchant may not complete the Transaction. The Merchant may return the Card but may not accept the Card in payment for that Transaction amount.

- 04 بطاقة الالتقاط.
- 14 رقم البطاقة غير صالح.
- 15 جهة إصدار غير صالحة.
- 41 بطاقة مفقودة.
- 43 بطاقة مسروقة.
- 54 بطاقة منتهية الصلاحية.

2.5.4.5 استخدام رقم التحقق من صحة البطاقة (CVV2)

(الفئة ب)

يجب على التاجر ألا يطالب حامل البطاقة أو يطلب منه إدخال معلومات CVV 2 عند استخدام بطاقة شريحة أو جهاز دفع عن بعد لإكمال معاملة شريحة في جهاز نقاط البيع أو محطة نقاط بيع متنقلة. في حالة البطاقة غير الموجودة، قد يطلب التاجر التحقق من رمز التحقق من صحة البطاقة (CVV 2) من جهة الإصدار، كوسيلة للتحقق من صلاحية البطاقة.

يجب ألا يتم تخزين بيانات CVV 2 من قبل التاجر أو الجهة القابلة عليه أو مقدم خدمة.

6.4.5 استجابات التفويض

يتلقى كل طلب تفويض رد تفويض يوجه جهة القبول أو التاجر إلى كيفية متابعة المعاملة.

عادةً ما يكون الرد المستلم رمزًا يحدد الإجراء الذي يجب على التاجر اتخاذه.

يُعلم هذا الرمز جهة القبول بالإجراء الذي يتعين اتخاذه (الموافقة أو الرفض أو الرجوع إلى جهة إصدار البطاقة أو بطاقة الالتقاط أو الصلاحية).

بغض النظر عن التنسيق الذي يتم تلقي رد التفويض به، فإن الاستجابة تحت دائمًا على اتخاذ أحد الإجراءات التالية

من جانب التاجر:

- الموافقة.
- الرفض.
- الرجوع إلى جهة اصدار البطاقة.
- الحجز على البطاقة.
- صالح (غير مرفوض) - يُستخدم لأنواع المعاملات غير المالية فقط.

1.6.4.5 الموافقة على الاستجابة

تعني استجابة الموافقة أن المعاملة مصرح بها.

بالنسبة للمعاملات ذات الشريط المغناطيسي والشرائح والمفاتيح المدخلة، توفر جهة الاصدار رمز تفويض مكون من ستة أرقام إلى جهة القبول عندما يوافق على معاملة لشراء سلع أو خدمات أو صرف نقدي. لا يزال يتعين على التاجر إجراء عملية المراجعة العادية قبل إتمام المعاملة.

2.6.4.5 رفض الاستجابة

تعني استجابة الرفض أن التاجر قد لا يكمل المعاملة. ويجوز له إعادة البطاقة، ولكن لا يجوز له قبول البطاقة في السداد لمبلغ المعاملة.

5.4.6.3 Refer to Card Issuer Response

A “refer to card issuer” or “call referral” response means the Acquirer or Merchant must contact the Issuer for further instructions before the Merchant can complete the Transaction. The use of call referrals is not recommended. The voice authorization approval code that the Issuer provides to the Merchant is not recorded in an authorization log, and therefore cannot be used as proof of authorization in the event of a dispute.

An Acquirer is permitted to convey all call referral responses to decline responses before forwarding the response to the Merchant. An Acquirer that chooses to support call referral responses must:

- Establish a merchant call referral response rate of 60 percent.
- Monitor individual merchant performance.
- Encourage, where possible or appropriate, three-way communication to allow merchants, cardholders, and issuers to exchange information during a call referral response call.
- Develop and distribute educational materials for merchants.
- Apply all call referral standards to the rules governing Member Service Providers (MSPs).

An Acquirer is permitted to convert a call referral response to a decline response. An Acquirer choosing to support call referral responses has the following responsibilities:

- Establish a Merchant call referral response rate of no less than 60 percent.
- Monitor individual Merchant performance.
- Encourage, where possible or appropriate, three-way communication to allow Merchants, Cardholders, and Issuers to exchange information during a call referral response call.
- Develop and distribute educational materials for Merchants.

Issuers are recommended to send call referral responses only when necessary, and must not send call referrals for Transactions identified as occurring at unattended POS Terminals or in a Card-not-present environment.

The National Scheme Operator uses a tiered pricing structure to discourage excess call referral responses, where higher charges apply for lower Transaction amount call referrals, and lower charges apply for higher Transaction amount call referrals. For more information, refer to the Billing System manual.

The Stand-In Processing System never generates a refer to card issuer response in the following situations:

- When the Transaction is a mail order/telephone order (MO/TO) or electronic commerce Transaction
- When the Acquirer is responding to a refer to card issuer response, the Issuer is unavailable, and the Stand-In Processing System processes the call referral Transaction
- When the Transaction is an ATM Transaction
- When the Issuer’s call center is closed

5.4.6.4 Capture Card Response

If the Merchant receives a “capture card” or “pick-up-card” response to an authorization request, the Merchant must not complete the Transaction. In a face-to-face Transaction environment, the Merchant should attempt to retain the Card by reasonable and peaceful means. The Card retention requirement does not apply when an Access Device has been presented. Upon recovering a Card, the Merchant must notify its Acquirer and ask for further instructions.

3.6.4.5 الرجوع إلى استجابة جهة إصدار البطاقة

تعني عبارة “الرجوع إلى جهة إصدار البطاقة” أو “إحالة الاتصال” أنه يجب على جهة القبول أو التاجر الاتصال بجهة الإصدار للحصول على مزيد من الإرشادات قبل أن يتمكن التاجر من إكمال المعاملة. ولا ينصح باستخدام إحالات المكالمات. لا يتم تسجيل رمز الموافقة على التفويض الصوتي الذي توفره جهة الإصدار للتاجر في سجل التفويض، وبالتالي لا يمكن استخدامه كدليل على التفويض في حالة حدوث نزاع.

يُسمح لجهة القبول تحويل جميع استجابات إحالة المكالمات لردود مرفوضة قبل إعادة توجيه الرد إلى التاجر. يجب على جهة القبول الذي يختار دعم استجابات إحالة المكالمات:

- إنشاء معدل استجابة إحالة مكالمات التاجر بنسبة 60 بالمائة.
 - مراقبة أداء التاجر الفردي.
 - تشجيع الاتصال ثلاثي الاتجاهات، حيثما كان ذلك ممكنًا أو مناسبًا، للسماح للتجار وحاملي البطاقات وجهات الإصدار بتبادل المعلومات أثناء مكالمات رد إحالة المكالمات.
 - تطوير وتوزيع المواد التعليمية للتجار.
 - تطبيق جميع معايير إحالة المكالمات إلى القواعد التي تحكم مقدمي خدمة الأعضاء (MSPs).
- يُسمح لجهة القبول تحويل استجابة إحالة مكالمات إلى استجابة رفض.
- وتتحمل جهة القبول التي تختار دعم استجابات إحالة المكالمات، المسؤوليات التالية:
- إنشاء معدل استجابة إحالة مكالمات التاجر لا يقل عن 60 بالمائة.
 - مراقبة أداء التاجر الفردي.
 - تشجيع الاتصال ثلاثي الاتجاهات، حيثما كان ذلك ممكنًا أو مناسبًا، للسماح للتجار وحاملي البطاقات وجهات الإصدار بتبادل المعلومات أثناء مكالمات رد إحالة المكالمات.
 - تطوير وتوزيع المواد التعليمية للتجار.

يُنصح جهات الإصدار بإرسال استجابات إحالة المكالمات فقط عند الضرورة، ويجب ألا يرسلوا إحالات للمكالمات للمعاملات التي تم تحديدها على أنها تحدث في محطات نقاط البيع غير الخاضعة للرقابة أو في بيئة البطاقة غير الموجودة.

يستخدم مشغل شبكة الدفع المحلية نظام تسعير متدرج لتثبيط استجابات إحالة المكالمات الزائدة، حيث يتم تطبيق رسوم أعلى على إحالات مكالمات ذات مبلغ معاملة أقل، ويتم تطبيق رسوم أقل على إحالات مكالمات ذات مبلغ معاملة أعلى. للمزيد من المعلومات، راجع دليل نظام الفواتير. لا يقوم نظام المعالجة الاحتياطية مطلقًا بإنشاء إشارة إلى استجابة جهة إصدار البطاقة في المواقف التالية:

- عندما تكون المعاملة بالطلب عبر البريد/ الطلب عبر الهاتف (MO /TO) أو معاملة تجارة إلكترونية.
- عندما تستجيب جهة القبول لإشارة إلى استجابة جهة إصدار البطاقة، تكون جهة الإصدار غير متاحة، ويقوم نظام المعالجة الاحتياطية بمعالجة معاملة إحالة المكالمات.
- عندما تكون المعاملة معاملة جهاز صراف آلي.
- عند إغلاق مركز الاتصال الخاص بجهة الإصدار.

4.6.4.5 استجابة بطاقة الالتقاط

إذا تلقى التاجر استجابة “بطاقة الالتقاط” أو “بطاقة الاستلام” على طلب التفويض، فإنه يجب على التاجر أن ألا يكمل المعاملة. في بيئة المعاملات وجهًا لوجه، يجب على التاجر محاولة الاحتفاظ بالبطاقة بوسائل معقولة وسليمة. ولا ينطبق شرط الاحتفاظ بالبطاقة عند تقديم جهاز وصول. عند استرداد

The Acquirer must follow these procedures when returning a recovered Card to the Issuer after Card capture:

- If the Merchant has not already done so, the Acquirer must render the Card unusable by cutting it in half vertically through the magnetic stripe.
- The Acquirer must forward the recovered Card to the Issuer within five calendar days of receiving the Card along with the first copy (white) of the Interchange Card Recovery Form (ICA-6 Annex 1). The additional copies are file copies for the Acquirer's records. Unless otherwise noted in the "Other Information" section of the Company Contact Management application, a recovered Card must be returned to the Security Contact of the Issuer.

5.4.6.5 Valid Response

A "valid" or "not declined" response is provided when the authorization request is a balance inquiry, Account status inquiry, or other non-financial type of request. The valid response indicates to the Acquirer or Merchant that the request was completed successfully by the Issuer. Merchants use the information returned in the response message to provide information to the Cardholder or to determine if further authorization decisioning is required.

5.4.7 Pre-authorizations

(Category A)

An Acquirer is advised to identify a POS Transaction authorization request as a preauthorization if:

1. Authorization is requested for an estimated amount that is greater than zero; or
2. The Transaction might not be completed for reasons other than technical failure or lack of full Issuer approval; for example:
 - a. When the Cardholder will be offered the choice at a later time to complete the Transaction with another payment means (such as when checking out of a hotel or returning a rental car);
 - b. When the products ordered by the Cardholder might be later found to be out of stock; or
 - c. If the mobile phone number for which the Cardholder has requested a top-up is later found not to exist.

The risk of technical failures, such as telecommunications failure or Terminal failure, should not be taken into account when determining whether preauthorization coding is appropriate. Each POS Transaction authorization request message identified as a preauthorization has a message reason code 4808 chargeback protection period of 30 calendar days. The clearing message corresponding to a preauthorization (or multiple incremental preauthorizations for the same Transaction) must be presented within 15 calendar days of the authorization approval date.

NOTE: The message reason code 4808 chargeback protection for a properly identified preauthorization of an Acquirer-financed or Merchant-financed installment billing payment arrangement is not limited in time.

The Issuer must release any hold placed on the Cardholder's Account after the expiration of the message reason code 4808 chargeback protection period for the Transaction. The total authorized amount of a Transaction does not include any amount for which the message reason code 4808 chargeback protection period has expired. The approved amount of any

البطاقة، يجب على التاجر إخطار الجهة القابلة عليها وطلب المزيد من الإرشادات.

يجب على جهة القبول اتباع هذه الإجراءات عند إعادة البطاقة المستردة إلى جهة الإصدار بعد الحصول على البطاقة:

- إذا لم يقم التاجر بذلك بالفعل ، يجب على جهة القبول جعل البطاقة غير صالحة للاستعمال عن طريق قصها إلى نصفين عموديًا من خلال الشريط المغناطيسي.
- يجب على جهة القبول إرسال البطاقة المستردة إلى جهة الإصدار خلال خمسة أيام تقويمية من استلام البطاقة مع النسخة الأولى (البيضاء) من نموذج استرداد بطاقة التبادل ICA-6 ، (الملحق 1) النسخ الإضافية هي نسخ ملفات لسجلات لجهة القابلة. ما لم يُذكر خلاف ذلك في قسم "معلومات أخرى" من تطبيق إدارة جهات اتصال الشركة، يجب إعادة البطاقة المستردة إلى جهة اتصال الأمان الخاصة بجهة الإصدار.

5.6.4.5 استجابة صالحة

يتم تقديم استجابة "صالحة" أو "غير مرفوضة" عندما يكون طلب التفويض عبارة عن استعلام عن الرصيد أو استعلام عن حالة الحساب أو أي نوع آخر من الطلبات غير المالية. وتشير الاستجابة الصحيحة للقابل أو التاجر إلى أن الطلب قد اكتمل بنجاح من قبل جهة الإصدار. ويستخدم التاجر المعلومات التي يتم إرجاعها في رسالة الرد لتوفير المعلومات لحامل البطاقة أو لتحديد ما إذا كان هناك حاجة إلى مزيد من قرارات التفويض.

7.4.5 التفويضات المسبقة

(الفئة أ)

يُنصح جهات القبول بتحديد طلب تفويض معاملة نقطة البيع كتصديق مسبق إذا:

1. طلب التفويض بمبلغ تقديري أكبر من الصفر.
2. قد لا يتم إكمال المعاملة لأسباب أخرى غير العطل الفني أو عدم الحصول على الموافقة الكاملة من جهة الإصدار؛ على سبيل المثال:
 - أ. عندما يُعرض على حامل البطاقة الخيار في وقت لاحق لإكمال المعاملة بوسائل دفع أخرى (مثل عند تسجيل الخروج من فندق أو إعادة سيارة مستأجرة).
 - ب. عندما يتم اكتشاف أن المنتجات التي طلبها حامل البطاقة قد نفذت في وقت لاحق.
 - ت. إذا تم اكتشاف عدم وجود رقم الهاتف المحمول الذي طلب حامل البطاقة إعادة شحنه لاحقًا.

لا ينبغي أخذ مخاطر الأعطال الفنية، مثل فشل الاتصالات أو فشل الجهاز، في الاعتبار عند تحديد ما إذا كان ترميز التفويض المسبق مناسبًا.

تحتوي كل رسالة طلب تفويض معاملة نقطة البيع التي تم تحديدها على أنها تفويض مسبق على رمز سبب الرسالة 4808، وفترة حماية رد المبالغ المدفوعة 30 يومًا تقويميًا. ويجب تقديم رسالة المقاصة المقابلة للتفويض المسبق (أو التفويضات المسبقة المتزايدة المتعددة لنفس المعاملة) خلال 15 يومًا تقويميًا من تاريخ اعتماد التفويض.

ملاحظة: رمز سبب الرسالة 4808 حماية رد المبالغ المدفوعة من أجل التفويض المسبق المحدد بشكل صحيح لترتيب سداد الفواتير الممول من قبل جهة القبول أو الممول من التاجر غير محدود بالوقت. يجب على جهة الإصدار تحرير أي تعليق تم وضعه في حساب حامل البطاقة بعد انتهاء صلاحية رمز سبب الرسالة 4808 فترة حماية رد المبالغ المدفوعة للمعاملة. ولا يشمل إجمالي المبلغ المصرح

authorization with an expired message reason code 4808 chargeback protection period is deemed to be zero.

To extend the duration of the message reason code 4808 chargeback protection period afforded by an approved preauthorization of a Transaction, a Merchant may later submit an additional preauthorization request for the same Transaction. A preauthorization to extend the chargeback protection period but not increase the total authorized amount should be sent for a zero amount.

5.4.8 Final Authorizations

(Category A)

An Acquirer is advised to identify a POS Transaction authorization request as a final authorization if:

1. Authorization is requested for the final Transaction amount; and
2. The Transaction is not expected to be cancelled after the authorization request is approved in full by the Issuer (excluding non-completion for technical reasons such as telecommunications failure or POS Terminal failure).

Each POS Transaction authorization request message identified as a final authorization has a message reason code 4808 chargeback protection period of seven (7) calendar days. When an authorization request is identified as a final authorization:

1. The Transaction must be presented for clearing within seven calendar days of the authorization approval date; and
2. The Transaction amount in the clearing message must equal the authorized amount.

5.4.9 Multiple Incremental Authorizations

(Category A)

The following requirements apply to POS Transactions that are Processed Transactions when multiple authorizations are processed for a single Transaction:

1. The Acquirer must use a unique identifier from the initial approved authorization of a Transaction in any additional authorizations requested in connection with the same Transaction. This unique identifier must also be included in the Transaction clearing record.
2. Upon receipt of the Transaction clearing record, the Issuer must use the unique identifier to match the original and any additional approved authorizations to the Transaction.
3. Upon matching all authorizations to the clearing record, the Issuer must release any hold placed on the Cardholder's account in connection with the original and any additional approved authorizations that is in excess of the Transaction amount.

5.4.10 Full Approvals

(Category A)

A full approval occurs when the entire authorization request amount is approved. A cash withdrawal Transaction must be approved or declined for the amount requested. A purchase with cash back Transaction must be either approved or declined for the total amount requested (purchase plus cash) or approved for the purchase amount only.

به للمعاملة أي مبلغ انتهت صلاحية رمز سبب الرسالة 4808 له فترة حماية رد المبالغ المدفوعة. ويعتبر المبلغ المعتمد لأي تفويض برمز سبب رسالة منتهي الصلاحية 4808 فترة حماية لرد المبالغ المدفوعة صفرًا.

لتمديد مدة حماية رمز سبب الرسالة 4808 التي يوفرها التفويض المسبق المعتمد لمعاملة ما، قد يقدم التاجر لاحقًا طلب تفويض إضافي لنفس المعاملة. ويجب إرسال التفويض المسبق لتمديد فترة حماية رد المبالغ المدفوعة دون زيادة إجمالي المبلغ المصرح به بمبلغ صفر.

8.4.5. التفويضات النهائية

(الفئة أ)

يُنصح جهات القبول بتحديد طلب تفويض معاملة نقطة البيع كتحويل نهائي إذا:

1. طلب التفويض لمبلغ المعاملة النهائية.
2. من غير المتوقع إلغاء المعاملة بعد الحصول على الموافقة الكاملة على طلب التفويض من قبل جهة الاصدار (باستثناء عدم الإكمال لأسباب فنية مثل فشل الاتصالات أو فشل محطة نقاط البيع).

تحتوي كل رسالة طلب تفويض معاملة نقطة البيع التي تم تحديدها على أنها تفويض نهائي على رمز سبب الرسالة 4808 وفترة حماية رد المبالغ المدفوعة لمدة سبعة (7) أيام تقويمية. عندما يتم تحديد طلب التفويض على أنه تفويض نهائي:

1. يجب تقديم المعاملة للمقاصة خلال سبعة أيام تقويمية من تاريخ الموافقة على التفويض.
2. يجب أن يساوي مبلغ المعاملة في رسالة المقاصة المبلغ المصرح به.

9.4.5. التفويضات الإضافية المتعددة

(الفئة أ)

تنطبق المتطلبات التالية على معاملات نقاط البيع التي تتم معالجتها عند معالجة تفويضات متعددة لمعاملة واحدة:

1. يجب على جهة القبول استخدام معرف مميز من التفويض المبدئي المعتمد للمعاملة في أي تفويضات إضافية مطلوبة فيما يتعلق بنفس المعاملة. ويجب أيضًا، تضمين هذا المعرف المميز في سجل مقاصة المعاملات.
2. عند استلام سجل مقاصة المعاملة، يجب على جهة الاصدار استخدام المعرف المميز لمطابقة الأصل وأي تفويضات معتمدة إضافية للمعاملة.
3. عند مطابقة جميع التفويضات بسجل المقاصة، يجب على جهة الإصدار تحرير أي حجز تم وضعه في حساب حامل البطاقة فيما يتعلق بالأصل وأي تفويضات معتمدة إضافية تزيد عن مبلغ المعاملة.

10.4.5. الموافقات الكاملة

(الفئة أ)

تحدث الموافقة الكاملة عند الموافقة على مبلغ طلب التفويض بالكامل. ويجب الموافقة على معاملة السحب النقدي أو رفضها للمبلغ المطلوب. ويجب أن تتم الموافقة على عملية الشراء باسترداد نقدي أو رفضها لإجمالي المبلغ المطلوب (الشراء بالإضافة إلى النقد) أو الموافقة على مبلغ الشراء فقط.

5.4.11 Full and Partial Reversals

(Category A)

5.4.11.1 Acquirer Requirements

POS Transactions

An Acquirer must support reversals (automatic or otherwise) for the full amount of any POS or refund Transaction authorization request whenever the Acquirer host system is unable to communicate an authorization response to the POS Terminal.

A reversal or adjustment of a refund Transaction must only be submitted to correct a documented clerical error and upon agreement of the Issuer. In such an event, the error must be reversed or adjusted no later than one calendar day after submission of the Financial Transaction/0200 or First Presentment message for the refund Transaction. Reversible clerical errors include, by way of example and not limitation, the erroneous capture of Transaction data, a duplicate Transaction, or an error caused by the transposition of data. An Acquirer must ensure that each Reversal Request/0400 or Acquirer Reversal Advice/0420 message submitted that originates from a Merchant corresponds to an original authorization request message.

The Acquirer must ensure that a Me”chan’ submits a Reversal Request/0400 message to the Issuer within 24 hours of:

- The cancellation of a previously authorized Transaction (for example, the sale was voided or the Merchant accepted another form of payment); or
- The finalization of a Transaction with a lower amount than previously approved.

The reversal may be a full or partial reversal, as appropriate. In the case of finalization of a Transaction with a lower amount, a partial reversal is not required if the First Presentment message is submitted within 24 hours of finalization of the Transaction.

Notwithstanding the above reversal requirement, the Acquirer must ensure that if a Merchant cancels a Transaction or finalizes a Transaction for a lower amount than previously approved, no reversal is submitted if such event occurs:

- More than 30 calendar days after the authorization date for a preauthorization; or
- More than seven calendar days after the authorization date for any other authorization message.

ATM Transactions

An Acquirer must not automatically generate a full or partial reversal of an authorized ATM Transaction when the ATM indicates that the Transaction was not completed because the Cardholder failed to collect some or all of the cash dispensed.

5.4.11.2 Issuer Requirements

An Issuer receiving a Reversal Request/0400 message or an Acquirer Reversal Advice/0420 message must release any hold placed on funds in the Account in the amount specified within 60 minutes of matching the reversal message to the original authorization request message.

5.4.11.3 Reversal to Convert an Approval to a Decline

An Acquirer or Merchant may convert an approval authorization request response (herein, an “Issuer-approved authorization”) into a decline for a Card-not-present Transaction believed, in good faith, by the Acquirer or Merchant to be fraudulent solely in accordance with the following procedure:

1. The Acquirer or Merchant must determine whether to proceed with a Transaction believed,

11.4.5. العمليات العكسية الكاملة والجزئية

(الفئة أ)

1.11.4.5. متطلبات جهة القبول

معاملات نقاط البيع

يجب أن تدعم جهة القبول عمليات الإلغاء (التلقائية أو غير ذلك) للمبلغ الكامل لأي نقطة بيع أو طلب تفويض معاملة استرداد عندما يتعذر على نظام مضيف القابل إرسال رد تفويض إلى محطة نقاط البيع.

يجب تقديم إلغاء أو تعديل معاملة استرداد فقط لتصحيح خطأ كتابي موثق وبناءً على موافقة جهة الإصدار. في مثل هذه الحالة، يجب إلغاء الخطأ أو تعديله في موعد لا يتجاوز يوم تقويمي واحد بعد تقديم المعاملة المالية/ 0200 أو رسالة التقديم الأولى لمعاملة الاسترداد. تشمل الأخطاء الكتابية القابلة للإلغاء، على سبيل المثال، الالتقاط الخاطئ لبيانات المعاملة، أو المعاملة المكررة، أو الخطأ الناجم عن نقل البيانات.

يجب على جهة القبول التأكد من أن كل رسالة طلب إلغاء/ 0400 أو إشعار إلغاء الجهة القابلة / 0420 المقدمة والتي تنشأ من التاجر تتوافق مع رسالة طلب التفويض الأصلية.

يجب أن تتحقق جهة القبول من أن التاجر يرسل رسالة طلب إلغاء/ 0400 إلى جهة الإصدار خلال 24 ساعة من:

- إلغاء معاملة مصرح بها مسبقًا (على سبيل المثال، تم إلغاء البيع أو قبول التاجر لطريقة دفع أخرى).
- إتمام معاملة بمبلغ أقل مما تمت الموافقة عليه سابقًا.

قد يكون الإلغاء إلغاءً كليًا أو جزئيًا، حسب الاقتضاء. وفي حالة إنهاء معاملة بمبلغ أقل، فإنه لا يلزم الإلغاء الجزئي إذا تم إرسال رسالة العرض الأول خلال 24 ساعة من إنهاء المعاملة.

بصرف النظر عن متطلبات الإلغاء المذكورة أعلاه ، يجب على جهة القبول التحقق من أنه إذا ألغى التاجر معاملة أو أنهى معاملة بمبلغ أقل من المبلغ المعتمد مسبقًا، فلن يتم تقديم أي إلغاء في حالة حدوث مثل هذا الحدث:

- أكثر من 30 يومًا بعد تاريخ التفويض للتفويض المسبقة.
- أكثر من سبعة أيام بعد تاريخ التفويض لأي رسالة تفويض أخرى.

معاملات أجهزة الصراف الآلي

يجب ألا تُنشئ جهة القبول بطريقة تلقائية إبطالًا كليًا أو جزئيًا لمعاملة الصراف الآلي المصرح بها عندما يشير جهاز الصراف الآلي إلى أن المعاملة لم تكتمل؛ لأن حامل البطاقة فشل في تحصيل بعض أو كل الأموال النقدية التي تم صرفها.

2.11.4.5. متطلبات جهة الإصدار

يجب على جهة الإصدار الذي يتلقى رسالة طلب عكس/ 0400 أو رسالة إشعار جهة القبول عكس/ 0420 تحرير أي حجز تم وضعه على الأموال في الحساب بالمبلغ المحدد خلال 60 دقيقة من مطابقة رسالة الإلغاء مع رسالة طلب التفويض الأصلية.

3.11.4.5. تحويل الموافقة إلى رفض عبر العمليات العكسية

يجوز لجهة القبول أو التاجر تحويل استجابة طلب اعتماد الموافقة (هنا، ”تفويض معتمد من جهة الإصدار“) إلى رفض لمعاملة بطاقة غير الموجودة يعتقد، بحسن نية، من قبل جهة القبول أو التاجر

- in good faith, to be fraudulent within 72 hours of sending the original authorization request message.
2. Upon deciding not to proceed with the Transaction and still within 72 hours of the original authorization request, the Acquirer or Merchant must:
 - a. Generate a reversal message for the full Transaction amount that includes a reason code indicating that the Transaction was declined by the Acquirer or the Merchant due to perceived fraud,
 - b. Disclose to the Cardholder that the Transaction cannot be completed at that time, and provide the Cardholder with valid customer service contact information (phone number or email address) to respond to Cardholder calls or email messages related to the cancelled order.

The contact information should be that of the Acquirer or Merchant that made the decision not to proceed with the Transaction. Sharing the specific reasons for the decline is not recommended or required.

The likelihood that a Transaction is fraudulent typically is determined through fraud screening and fraud scoring services that involve the storage, transmission or processing of Card or Transaction data in compliance with the Payment Card Industry Data Security Standard (PCI DSS). The Acquirer must register any third party provider of such services with the National Scheme Operator as a Third Party Processor (TPP). The systematic decline by an Acquirer or Merchant of CNP Transactions arising from particular Cards, Issuers, or geographic locations is prohibited.

5.4.12 ATM Transactions

(Category A)

An ATM Transaction is identified with MCC 6011 (Automated Cash Disbursements).

The NUMO network supports the following ATM Transaction types:

- Withdrawal
- Deposit
- PIN Unblock – for Chip Cards only
- PIN Change – for magnetic stripe and Chip Cards

ATM Transactions are processed on the Single Message System and require PIN entry and online authorization by the Issuer.

5.4.13 Transaction Records

(Category A)

Each Transaction record must reflect a valid and accurate Transaction date as follows.

(See appendix number 42)

5.4.13.1 Presentment Time Frame

- A refund Transaction must be presented within five calendar days of the date on which the Merchant completed the refund and provided a refund Transaction receipt to the Cardholder.

The Acquirer has a maximum of 30 calendar days after the Transaction date to present a Transaction when the Acquirer must delay presentment:

- Because of the Merchant's permissible delay in submitting the Transaction; or
- A national bank holiday of at least four consecutive days occurred, which prevented the Acquirer from presenting a Transaction within the applicable seven-calendar-day time frame.

An Issuer must still accept Transactions submitted beyond the applicable time frame if the

أنها احتيالية فقط وفقًا بالإجراء التالي:

1. يجب على جهة القبول أو التاجر تحديد ما إذا كان سيتم المضي قدمًا في معاملة يعتقد بحسن نية أنها احتيالية خلال 72 ساعة من إرسال رسالة طلب التفويض الأصلية.
 2. عند اتخاذ قرار بعدم متابعة المعاملة وخلال 72 ساعة من طلب التفويض الأصلي، يجب على جهة القبول أو التاجر:
 - أ. القيام بإنشاء رسالة إلغاء للمبلغ الكامل للمعاملة التي تتضمن رمز السبب يشير إلى أن المعاملة قد تم رفضها من قبل جهة القبول أو التاجر بسبب الاحتيال المشتبه فيه.
 - ب. الإفصاح لحامل البطاقة أنه لا يمكن إتمام المعاملة في ذلك الوقت، وتزويد حامل البطاقة بمعلومات الاتصال بخدمة العملاء الصالحة (رقم الهاتف أو عنوان البريد الإلكتروني) للرد على مكالمات حامل البطاقة أو رسائل البريد الإلكتروني المتعلقة بالطلب الملغى.
- يجب أن تكون معلومات الاتصال خاصة بالقابل أو التاجر الذي اتخذ قرار عدم متابعة المعاملة. فإن مشاركة الأسباب المحددة للرفض غير مطلوب.

يتم تحديد احتمالية أن تكون المعاملة احتيالية عادةً من خلال خدمات فحص الاحتيال وتسجيل نقاط الاحتيال التي تتضمن تخزين أو نقل أو معالجة بيانات البطاقة أو المعاملة وفقًا لمعيار أمان بيانات صناعة بطاقات الدفع (PCI DSS). يجب على جهة القبول تسجيل أي مقدم تابع لطرف ثالث لهذه الخدمات مع مشغل شبكة الدفع المحلية باعتباره معالجًا تابعًا لطرف ثالث (TPP). ويُحظر الرفض المنتظم من قبل جهة القبول أو التاجر لمعاملات CNP الناشئة عن بطاقات أو جهات إصدار أو مواقع جغرافية معينة.

12.4.5. معاملات أجهزة الصراف الآلي

يتم تحديد معاملة جهاز الصراف الآلي مع MCC 6011 (المدفوعات النقدية الآلية).

تدعم شبكة نمو أنواع معاملات جهاز الصراف الآلي التالية:

- سحب.
 - إيداع.
 - إلغاء حظر رقم التعريف الشخصي - لبطاقات الشريحة فقط.
 - تغيير رقم التعريف الشخصي - للشريط المغناطيسي وبطاقات الشريحة.
- تتم معالجة معاملات أجهزة الصراف الآلي على نظام الرسائل الفردية وتتطلب إدخال رقم التعريف الشخصي والتفويض عبر الإنترنت من قبل جهة الإصدار.

13.4.5. سجلات المعاملات

يجب أن يعكس كل سجل معاملة تاريخ معاملة صالحًا ودقيقًا على النحو التالي.

(انظر الملحق رقم 42)

1.13.4.5. الإطار الزمني للتقديم

- يجب تقديم معاملة استرداد خلال خمسة أيام تقويمية من التاريخ الذي أكمل فيه التاجر عملية الاسترداد وقدم إيصال معاملة استرداد لحامل البطاقة.
- لدى جهة القبول 30 يومًا كحد أقصى بعد تاريخ المعاملة لتقديم المعاملة عندما يتعين على جهة القبول تأخير التقديم:
- بسبب التأخير المسموح به من قبل التاجر في تقديم المعاملة، أو
- حدثت عطلة مصرفية وطنية لمدة أربعة أيام متتالية على الأقل، مما منع الجهة القابلة من تقديم معاملة خلال الإطار الزمني المعمول به وهو سبعة أيام.

Cardholder account is in good standing or the Transaction can be otherwise honored and posted.

If the message has no Transaction date when processed through the Clearing System, the date 15 days before the processing date will be presumed (for rules administration) to be the Transaction date, subject to subsequent establishment of the actual date by support documentation.

5.4.14 Transaction Queries and Disputes

(Category C)

A Member must have the facilities and ensure the support of processes to handle Transaction queries, disputes, documentation requests, and chargebacks.

5.4.14.1 Compliance with Dispute Procedures

The National Scheme Operator administers dispute procedures that enable a Member to seek redress against another Member for failure to comply with the Standards applicable to a Transaction. Any filing by or on behalf of a Member related to an arbitration procedure (including any chargeback or re-presentment cycle) or pre-compliance or compliance procedure must be made in good faith and only after careful review of both the Standards and available information pertinent to the dispute5.4.24.3 Chargebacks for Reissued Cards Upon reissuing a Card with the same primary account number (PAN) and a new expiration date, the Issuer must include the expiration date in all Transaction chargeback records.

5.4.15 Correction of Errors

(Category A)

If a Member has been unjustly enriched because of an error, the Member must reimburse the amount with which it has been enriched to the Member or Members that have suffered the corresponding loss.

Annex 1: Captured Card Form

Bank Name: _____

Log – Reference: _____/ _____

Capture Date -Time : _____

Captured ATM Code: _____

Terminal ID: _____ -

Captured ATM Location: _____

Captured Card Number:

Issuing Bank Name : _____

Journal Reference : _____

Capture Reason Code :

Action Taken

Date and Time: _____

Authorized Person: _____

ويتعين على جهة الاصدار قبول المعاملات المقدمة بعد الإطار الزمني المعمول به إذا كان حساب حامل البطاقة في وضع جيد، أو يمكن تقدير المعاملة ونشرها بطريقة أخرى.

إذا لم يكن للرسالة تاريخ معاملة عند معالجتها من خلال نظام المقاصة، فسيتم افتراض أن التاريخ قبل 15 يومًا من تاريخ المعالجة (لإدارة القواعد) هو تاريخ المعاملة، مع مراعاة التأسيس اللاحق للتاريخ الفعلي من خلال وثائق الدعم.

14.4.5. استفسارات ونزاعات المعاملات

(الفئة ج)

يجب أن يمتلك العضو التسهيلات، ويضمن دعم العمليات للتعامل مع استفسارات المعاملات والنزاعات وطلبات التوثيق وعمليات رد المبالغ المدفوعة.

1.14.4.5 الامتثال لإجراءات النزاع

يدير مشغل شبكة الدفع المحلية إجراءات النزاع التي تمكن العضو من طلب التعويض ضد عضو آخر لعدم امتثاله للمعايير المطبقة على المعاملة. ويجب أن يتم أي إيداع من قبل عضو أو نيابة عنه فيما يتعلق بإجراءات التحكيم (بما في ذلك أي دورة رد المبالغ المدفوعة أو إعادة التقديم) أو الامتثال المسبق أو إجراء الامتثال بحسن نية وفقط بعد مراجعة دقيقة لكل من المعايير والمعلومات المتاحة ذات الصلة.3.24.4.5. عمليات رد المبالغ المدفوعة للبطاقات المعاد إصدارها، عند إعادة إصدار بطاقة بنفس رقم الحساب الأساسي (PAN) وتاريخ انتهاء صلاحية جديد، يجب على جهة الاصدار تضمين تاريخ انتهاء الصلاحية في جميع سجلات استرداد المدفوعات الخاصة بالمعاملات.

15.4.5. تصحيح الأخطاء

(الفئة أ)

إذا تم إثراء العضو بشكل غير قانوني بسبب حدوث خطأ، فإنه يجب على العضو سداد المبلغ الذي تم إثراءه به إلى العضو أو الأعضاء الذين افترضوا من الخسارة المقابلة.

المرفق 1: نموذج البطاقة الملتقطة

اسم المصرف: _____

السجل – المرجع: _____ / _____

تاريخ-الوقت الالتقاط: _____

رمز جهاز الصراف الآلي الملتقط: _____ معرف الجهاز: _____

موقع جهاز الصراف الآلي الملتقط: _____

رقم البطاقة الملتقطة: _____

رقم المصرف المصدر: _____

مرجع المجلة: _____

رمز سبب الالتقاط: _____

الإجراءات المتخذة

التاريخ و الوقت: _____

الشخص المفوض: _____

Regulatory Rules of The Libyan National Payment Scheme

Chapter 6 – Fraud & Risk Management

This Chapter contains information relating to the protection of Cardholder and Transaction data, scheme risk management, fraud control procedures and reporting requirements, and Member obligations relating to these functions.

6.1 Payment System Integrity Standards

Each Member is responsible to the National Scheme Operator and all other Members for any data security, fraud, and other scheme risks related to its participation in the Interchange System. To limit such risks, the Member must comply with the Scheme's risk and fraud management Standards, including but not limited to those set forth in this chapter.

Due to the potential impact of Member noncompliance on payment system integrity, all Rules in this chapter 6 are within compliance zone Category A (Referenced in Chapter 1).

6.1.1 Connecting to the Network—Physical and Logical Security Requirements

Each Member and any agent thereof must be able to demonstrate to the satisfaction of the National Scheme Operator the existence and use of meaningful physical and logical security controls for any communications processor or other device used to connect the Member's processing systems to the National Scheme Operator's network (herein, "a Network Device") and all associated components, including all hardware, software, systems, and documentation (herein collectively referred to as "Service Delivery Point Equipment") located on-site at the Member or its' agent facility. Front-end communications processors include Member interface processors, network interface units (NIUs), and debit interface units.

The controls must meet the minimum requirements described in this section, and preferably will include the recommended additional parameters.

6.1.1.1 Minimum Security Requirements

At a minimum, the Member or its agent must put in place the following controls at each facility housing Service Delivery Point Equipment:

1. Each network segment connecting a Network Device to the Member's processing systems must be controlled tightly, as appropriate or necessary to prevent unauthorized access to or from other public or private network segments.
2. The connectivity provided by each such network segment must be dedicated wholly and restricted solely to the support of communications between the National Scheme Operator and the Member's processing systems.
3. The Member or its agent must replace each vendor-supplied or default password present on the Member's processing systems, each Network Device, and any device providing connectivity between them with a "strong password." A strong password contains at least eight characters, uses a combination of letters, numbers, symbols, punctuation, or all, and does not include a name or common word(s).

القواعد التنظيمية لشبكة الدفع المحلية الليبية

الفصل 6 – مكافحة عمليات الاحتيال وإدارة المخاطر

يحتوي هذا الفصل على المعلومات التي تتعلق بحماية حامل البطاقة وبيانات المعاملات، إدارة مخاطر النظام، إجراءات مكافحة الاحتيال، طرق الإبلاغ والتزامات الأعضاء المتعلقة بتطبيق هذه القواعد.

1.6 معايير سلامة نظام الدفع

كل عضو مسؤول أمام مشغل شبكة الدفع المحلية، وجميع الأعضاء الآخرين عن المخاطر التي تتعلق بأمن البيانات وعمليات الاحتيال، ومخاطر النظام الأخرى المتعلقة بمشاركته في نظام التبادل للحد من هذه المخاطر، ويجب على العضو الامتثال لمعايير إدارة المخاطر وعمليات الاحتيال الخاصة بالنظام، بما في ذلك على سبيل المثال، تلك المنصوص عليها في هذا الفصل.

نظرًا للتأثير المحتمل لعدم امتثال الأعضاء، على سلامة شبكة الدفع المحلية، فإن جميع القواعد الواردة في هذا الفصل 6 تعتبر من قواعد الامتثال للفئة أ (المشار إليها في الفصل 1).

1.1.6 الاتصال بالشبكة - متطلبات الأمان المادية والمعنوية

يجب أن يكون كل عضو وأي وكيل قادرًا على تطبيق وتوفير ما يطلبه مشغل شبكة الدفع المحلية من وجود واستخدام ضوابط أمنية مادية ومعنوية ذات قدرة لمعالجة الاتصالات أو الأجهزة الأخرى التي يستخدمها لربط أنظمة معالجة العضو بشبكة مشغل شبكة الدفع المحلية (هنا، "جهاز الشبكة") وجميع المكونات المرتبطة بها، بما في ذلك، جميع الأجهزة والبرامج والأنظمة والمستندات (يشار إليها مجتمعة باسم "معدات نقطة تقديم الخدمة") الموجودة في الموقع في منشأة العضو أو وكيله. وتتضمن معالجات الاتصالات الأمامية معالجات واجهة الأعضاء، ووحدات واجهة الشبكة ووحدات واجهة الخصم.

ويجب أن تلبى هذه الضوابط الحد الأدنى من المتطلبات الموضحة في هذا القسم، ويفضل أن تتضمن الضوابط الإضافية الموصى بها.

1.1.1.6 الحد الأدنى من متطلبات الأمان

طبقاً لقواعد الحد الأدنى، يجب على العضو أو وكيله وضع الضوابط التالية، في كل منشأة تحتوي على معدات نقطة تقديم الخدمة:

1. يجب التحكم بفاعلية في كل قطاع شبكة يربط جهاز الشبكة بأنظمة العضو المعالجة، حسب الاقتضاء أو الضرورة لمنع الوصول غير المصرح به، إلى أو من، قطاعات الشبكة العامة أو الخاصة الأخرى.
2. يجب أن يتم تخصيص الاتصال الذي يوفره كل قطاع شبكة بشكل كامل ومقتصر فقط على دعم الاتصالات بين مشغل شبكة الدفع المحلية وأنظمة العضو المعالجة.
3. يجب على العضو أو وكيله استبدال كل كلمة مرور افتراضية، أو يوفرها البائع موجودة على أنظمة العضو المعالجة، وكل جهاز للشبكة، وأي جهاز يوفر الاتصال فيما بينها بـ "كلمة مرور قوية". تحتوي كلمة المرور القوية على ثمانية أحرف على الأقل، وتتكون من الأحرف والأرقام والرموز وعلامات الترقيم أو الكل، ولا تتضمن اسمًا أو كلمة (كلمات) شائعة.

4. The Member or its agent must conduct regular periodic reviews of all systems and devices that store Account information to ensure that access is strictly limited to appropriate Member personnel on a “need to know” basis.
5. The Member or its agent must notify the National Scheme Operator within 30 business days of any change in the personnel designated to administer the Network Device.
6. The Member or its agent must maintain and document appropriate audit procedures for each Network Device. Audit reports must be maintained and accessible to the Member for at least one year, including a minimum of 90 days in an easily retrieved electronic format.
7. The Member must ensure that the software employed in any system or device used to provide connectivity to the Network is updated with all appropriate security patches, revisions, and other updates as soon after a release as is practicable.
8. The physical location of the Service Delivery Point Equipment must be accessible only by authorized personnel of the Member or its agent. Visitor access must be controlled by at least one of the following measures:
 - a. Require each visitor to provide government-issued photo identification before entering the physical location; and/or
 - b. Require each visitor to be escorted to the physical location by authorized personnel of the Member or its agent.
9. If the physical location of the Service Delivery Point Equipment provides common access to other devices or equipment, then the Network Device must be stored in a cabinet that is locked both in front and the rear at all times. Keys to the cabinet must be stored in a secured location.
10. The Member or its agent must have documented procedures for the removal of Service Delivery Point Equipment from the physical location.

6.1.1.2 Additional Recommended Security Requirements

Members and their agents are strongly encouraged to put in place the following additional controls at each facility housing a Network Device:

1. Placement of the Network Device in a physical location that is enclosed by floor-to-ceiling walls.
2. Continual monitoring of the Network Device by cameras or other type of electronic surveillance system. Video records should be maintained for a minimum of 90 days.

6.1.1.3 Ownership of Service Delivery Point Equipment

Each Member owns his Delivery Point Equipment, the National Scheme Operator is the only entity that has the right to set the configuration with accordance to Switch configuration and requirements.

The Member at all times must employ at that location the minimum-security requirements set forth in this Rule.

6.1.1.4 Component Authentication

All components actively participating in the Interchange System must authenticate each other by means of cryptographic procedures, either explicitly by a specific authentication protocol or implicitly by correct execution of a cryptographic service possessing secret information (for example, the shared key or the login ID).

A component actively participates in the Interchange System if, because of its position in the system, it can evaluate, modify, or process security-related information.

4. يجب على العضو أو وكيله إجراء مراجعات دورية منتظمة لجميع الأنظمة والأجهزة التي تخزن معلومات الحساب للتحقق من أن الوصول يقتصر بشكل صارم على أفراد الأعضاء المحددين على أساس “الحاجة إلى المعرفة”.
5. يجب على العضو أو وكيله، إخطار مشغل شبكة الدفع المحلية خلال 30 يوم عمل بأي تغيير في الموظفين المعيّنين لإدارة جهاز الشبكة.
6. يجب على العضو أو وكيله، الحفاظ على إجراءات التدقيق المناسبة وتوثيقها لكل جهاز شبكة. ويجب الاحتفاظ بتقارير التدقيق وإتاحتها للعضو لمدة عام واحد على الأقل، بما في ذلك 90 يومًا على الأقل بتنسيق إلكتروني يسهل استرداده.
7. يجب على العضو التحقق من أن البرنامج المستخدم في أي نظام أو جهاز يستخدم لتوفير الاتصال بالشبكة قد تم تحديثه بجميع تصحيحات الأمان والمراجعات، والتحديثات الأخرى في أقرب وقت بعد الإصدار كما هو ممكن عمليًا.
8. يجب ألا يكون الوصول إلى الموقع الفعلي لمعدات نقطة تقديم الخدمة متاحًا إلا للموظفين المعتمدين من قبل العضو أو وكيله. ويجب التحكم في وصول الزوار بأحد الإجراءات التالية:
 - أ. مطالبة كل زائر بتقديم بطاقة هوية تحمل صورة صادرة عن الجهات المختصة في الدولة قبل الدخول إلى الموقع الفعلي.
 - ب. اشتراط اصطحاب كل زائر إلى الموقع الفعلي من قبل موظفين معتمدين من العضو أو وكيله.
9. إذا كان الموقع الفعلي لمعدات نقطة تقديم الخدمة يوفر وصولًا مشتركًا إلى الأجهزة أو المعدات الأخرى، فيجب تخزين جهاز الشبكة في خزانة مقفلة من الأمام والخلف في جميع الأوقات. ويجب تخزين مفاتيح الخزنة في مكان آمن.
10. يجب أن يكون لدى العضو أو وكيله إجراءات موثقة لإزالة معدات نقطة تقديم الخدمة من الموقع الفعلي.

2.1.1.6 متطلبات الأمان الإضافية الموصى بها

يشجع الأعضاء ووكلائهم بتطبيق الضوابط الإضافية التالية في كل منشأة تحتوي على جهاز شبكة:

1. وضع جهاز الشبكة في مكان فعلي محاط بجدران محصنة من الأرض حتى السقف.
2. المراقبة المستمرة لجهاز الشبكة بواسطة الكاميرات، أو أي نوع آخر من أنظمة المراقبة الإلكترونية. ويجب الاحتفاظ بسجلات الفيديو لمدة 90 يومًا على الأقل.

3.1.1.6 ملكية معدات نقطة تقديم الخدمة

يملك كل عضو معدات نقطة التقديم الخاصة به، ويعد مشغل شبكة الدفع المحلية هو الجهة الوحيدة التي تختص بتعيين الإعدادات وفقًا لإعدادات المحول ومتطلباته. يلتزم كل العضو، وفي جميع الأوقات، أن يطبق في ذلك الموقع الحد الأدنى من متطلبات الأمان المنصوص عليها في هذه القاعدة.

4.1.1.6 المصادقة على المكونات

يجب أن تقوم جميع المكونات المشاركة بنشاط في نظام التبادل، بمصادقة بعضها البعض عن طريق إجراءات التشفير، إما صراحةً عن طريق بروتوكول مصادقة محدد أو ضمنيًا عن طريق التنفيذ الصحيح لخدمة التشفير التي تعالج معلومات سرية (على سبيل المثال ، المفتاح المشترك أو معرف تسجيل الدخول).

ويجب أن تشارك المكونات بشكل فعال في نظام التبادل، إذا كان بإمكانه، بسبب موقعه في النظام، تقييم المعلومات المتعلقة بالأمن أو تعديلها أو معالجتها.

6.1.2 Integrity of NUMO Brand and Network

A Member may not directly or indirectly engage in or facilitate any action that is illegal or that, in the judgement of the National Scheme Operator and whether or not addressed elsewhere in the Standards, damages or may damage the goodwill or reputation of the National Scheme Operator. Upon request of the National Scheme Operator, a Member will promptly cease engaging in or facilitating any such action.

In addition, a Member must not place or cause to be placed on any Card or any Terminal or other acceptance device any image, information, application or product that would in any way, directly or indirectly, have or potentially have the effect of diminishing or devaluing the reputation or utility of NUMO Marks, Cards, or any of the National Scheme Operator's products, programs, services, networks, or systems.

6.1.3 CBL Anti-Money Laundering and Sanctions Requirements

As a condition of being granted a License by the CBL, and on an ongoing basis thereafter, each License applicant and each Member (together, for purposes of this Rule, "Members") must demonstrate to the satisfaction of the CBL ongoing maintenance of comprehensive anti-money laundering ("AML") compliance programs (together, for purposes of this Rule, "Programs") that safeguard the National Scheme Operator and the Interchange System from risk associated with money laundering, terrorist financing, pursuant to applicable law, regulation, and Central Bank of Libya (CBL) requirements, including but are not limited to Law No. 2 of 2005 against Money Laundering ("the Anti-Money Laundering Law") and ("the Law on Terrorists Organizations and Terrorists Lists").

The Programs are subject to periodic examination at the discretion of the National Scheme Operator. Such an examination may be by the National Scheme Operator or a designee of the National Scheme Operator or other person deemed satisfactory by the National Scheme Operator. Any such examination is at the Member's expense.

The National Scheme Operator must "e pr'vided with a complete copy of the examination report and the Member shall not engage in any conduct or permit any person within the Member's control to engage in any conduct, agreement, or understanding that would impair the completeness, accuracy, or objectivity of any aspect of the examination or examination report.

6.1.3.1 CBL AML Requirements -Governed by CBL

Each Member conducting or proposing to conduct Payments Activity must have a written AML compliance Program with a policy, procedures, and controls in place to safeguard the National Scheme and the Interchange System from and against the use of the Interchange System for money laundering and/or terrorist financing. Each Member's AML compliance Program must be commensurate with its respective AML risk profile and fully implemented in accordance with this Rule and local regulatory requirements.

A Member's AML compliance Program must address, in a manner satisfactory to the Central Bank of Libya, all Activity and include, at a minimum, the following:

1. A process to ensure thorough client identification and due diligence
2. Sufficient controls, resources, and monitoring systems for the prompt detection and reporting of suspicious activity
3. Compliance with all regulatory record-keeping and reporting requirements
4. Risk assessment processes designed to identify and apply appropriate risk management controls

2.1.6. سلامة العلامة التجارية وشبكة نمو

لا يجوز للعضو أن يمارس بشكل مباشر أو غير مباشر أو تسهيل إجراء غير قانوني، أو يؤدي إلى الإضرار بشهرة أو سمعة مشغل شبكة الدفع المحلية. وبناءً على طلب مشغل شبكة الدفع المحلية، يجب على العضو التوقف فوراً عن المشاركة عن مثل هذه الأعمال.

بالإضافة إلى ذلك، يجب على العضو أن لا يضع، أو أن يتسبب في أن الوضع على البطاقة أو المحطة أو أي جهاز قبول آخر، أي صورة أو معلومات أو تطبيق أو منتج، قد يكون له بشكل مباشر أو غير مباشر، أو يحتمل أن يكون له تأثير التضليل أو التقليل من قيمة أو سمعة أو فائدة علامات أو بطاقات نمو أو أي من منتجات أو برامج أو خدمات أو شبكات أو أنظمة مشغل شبكة الدفع المحلية.

3.1.6. متطلبات مصرف ليبيا المركزي لمكافحة غسل الأموال والعقوبات

يشترط للحصول على الترخيص من قبل مصرف ليبيا المركزي، أن يقوم كل طالب ترخيص وكل عضو (معاً لأغراض تطبيق هذه القاعدة "الأعضاء") بالصيانة المستمرة الشاملة لبرامج الامتثال لمكافحة غسل الأموال (معاً لأغراض تطبيق هذه القاعدة "البرامج") التي تحمي مشغل شبكة الدفع المحلية ونظام التبادل من المخاطر المرتبطة بغسل الأموال وتمويل الإرهاب، وفقاً للقانون المعمول به واللوائح، ومتطلبات مصرف ليبيا المركزي، بما في ذلك على سبيل المثال، القانون رقم 2 لسنة 2005 بشأن مكافحة غسل الأموال ("قانون مكافحة غسل الأموال") و ("قانون مكافحة المنظمات الإرهابية وقوائم الإرهابيين").

ويجب أن تخضع البرامج للفحص الدوري وفقاً لتقدير مشغل شبكة الدفع المحلية. وقد يتم هذا الفحص بواسطة مشغل شبكة الدفع المحلية أو من ينوب عنه، أو خبير يفوضه مشغل شبكة الدفع المحلية للقيام بهذه المهمة. وتكون نفقات هذا الفحص على العضو.

ويجب تزويد مشغل شبكة الدفع المحلية بنسخة كاملة من تقرير الفحص، ولا يجوز للعضو ممارسة سلوك، أو السماح لشخص تحت سيطرته بالمشاركة في سلوك أو اتفاق من شأنه أن يضعف من اكتمال دقة أو موضوعية أي جانب من جوانب تقرير الفحص أو الفحص نفسه.

1.3.1.6. متطلبات مصرف ليبيا المركزي لمكافحة غسل الأموال - يحكمها مصرف ليبيا المركزي

يجب أن يكون لدى كل عضو يمارس، أو يقترح ممارسة نشاط مدفوعات، برنامج امتثال مكتوب لمكافحة غسل الأموال مع سياسة وإجراءات وضوابط مطبقة لحماية شبكة الدفع، ونظام التبادل من وضد استخدام نظام التبادل لغسيل الأموال وتمويل الإرهاب. ويجب أن يكون برنامج الامتثال لمكافحة غسل الأموال الخاص بكل عضو متناسباً مع ملف إدارة مخاطر مكافحة غسل الأموال الخاص به، وأن يتم تنفيذه بالكامل وفقاً لهذه القاعدة والمتطلبات التنظيمية الوطنية.

ووفقاً للسلطة التقديرية لمصرف ليبيا المركزي، يجب أن يتضمن برنامج الامتثال لمكافحة غسل الأموال الخاص بالعضو، جميع الأنشطة وأن يتناول، على الأقل، ما يلي:

1. عملية لضمان التحديد الدقيق للعميل والعناية الواجبة.
2. ضوابط وموارد وأنظمة مراقبة كافية للكشف الفوري عن النشاط المشبوه بالاحتيال، والإبلاغ عنه.
3. الامتثال لجميع متطلبات حفظ السجلات التنظيمية وإعداد التقارير.
4. عمليات تقييم المخاطر المصممة لتحديد وتطبيق ضوابط إدارة المخاطر المناسبة.

5. A training program for all personnel whose duties require knowledge of the AML compliance Program and requirements
6. An audit process to periodically test controls

6.1.3.2 Noncompliance with CBL AML requirements – Governed by CBL

A failure to comply with any of the obligations set forth in this Rule may result in:

- The denial of a License;
- License suspension;
- Noncompliance assessments; and/or
- Such other action as the National Scheme Operator may deem necessary or appropriate.

6.1.4 Satisfaction of Minimum Financial Requirements

Each Member at all times must satisfy the minimum financial requirements established by the CBL. The CBL, in its discretion, may establish different or additional financial requirements for (i) a category of financial institutions, organizations, or corporations or other entities that are eligible to become a Member, or (ii) an individual Member or prospective Member in the manner set forth in the Standards should the CBL determine that different or additional requirements are reasonably appropriate to evidence the financial integrity of a type of Member or an individual Member or prospective Member.

Such requirements may include both objective standards, such as the measurement of capital adequacy, and subjective standards, such as evaluating key management experience and ability, the area in which the Member engages in business, and the manner in which such business is conducted.

6.2 Scheme Risk Management Program

The Scheme Risk Management Program is dedicated to supporting good standing position of a Member and Service Provider growth. The program works with Members and Service Providers to ensure that they understand and operate within the Standards to minimize operational, financial, reputational, and compliance risks.

In addition, the Scheme Risk Management Program provides industry best practices to support business growth by enhancing the overall operational efficiency and profitability of the issuing and acquiring Portfolio while maintaining losses at an acceptable level.

6.2.1 Scheme Risk Management Review Levels

The Scheme Risk Management Program consists of three mandatory levels. The three mandatory levels are:

- Member Onboarding Reviews for prospective Principal Members and participant Members;
- The Payment Service Provider Risk Management Program.
- Member Scheme Reviews for existing Members.

Must be clear to all members:

(1) that all members are submitted to the ICRM framework requested by the CBL regulations (especially circular on licensing and governance)

(2) that the 1st line and 2nd lines of defense controls must include the 3 mandatory levels described here

5. برنامج تدريبي لجميع الموظفين الذين تتطلب واجباتهم معرفة برنامج ومتطلبات الامتثال لمكافحة غسل الأموال.
6. عملية تدقيق لاختبار الضوابط بشكل دوري.

2.3.1.6 عدم الامتثال لمتطلبات مصرف ليبيا المركزي لمكافحة غسل الأموال – يحكمها مصرف ليبيا المركزي

قد يؤدي عدم الامتثال لحد الالتزامات المنصوص عليها في هذه القاعدة إلى:

- رفض الترخيص.
- تعليق الترخيص.
- تقييمات عدم الامتثال.
- أي إجراء آخر قد يراه مشغل شبكة الدفع المحلية ضروريًا أو مناسبًا.

4.1.6 استيفاء الحد الأدنى من المتطلبات المالية

يجب على كل عضو، وفي جميع الأوقات أن يستوفي الحد الأدنى من المتطلبات المالية التي وضعها مصرف ليبيا المركزي. ويجوز لمصرف ليبيا المركزي وفقاً لسلطته التقديرية، وضع متطلبات مالية مختلفة أو إضافية لـ (1) فئة من المؤسسات المالية أو المنظمات أو الشركات أو الكيانات الأخرى المؤهلة لتصبح عضوًا . (2) عضو فردي أو عضو محتمل بالطريقة المنصوص عليها في المعايير ويجب أن يقرر مصرف ليبيا المركزي أن المتطلبات المختلفة أو الإضافية مناسبة بشكل معقول لإثبات السلامة المالية لنوع من الأعضاء أو عضو فردي أو عضو محتمل.

قد تشمل هذه المتطلبات كلاً من المعايير الموضوعية، مثل قياس كفاية رأس المال، والمعايير الذاتية، مثل تقييم الخبرة والقدرة الإدارية الرئيسية، والمجال الذي ينخرط فيه العضو في الأعمال التجارية، والطريقة التي يتم بها تنفيذ هذه الأعمال.

2.6 برنامج إدارة مخاطر النظام

برنامج إدارة مخاطر النظام مكرس لدعم الوضع الجيد للأعضاء، ونمو مقدم الخدمة. يعمل البرنامج مع الأعضاء ومقدمي الخدمات للتحقق من أنهم يفهمون ويعملون ضمن المعايير لتقليل مخاطر التشغيل والمالية والسمعة والامتثال.

بالإضافة إلى ذلك، يوفر برنامج إدارة مخاطر النظام أفضل الممارسات الصناعية لدعم نمو الأعمال من خلال تعزيز الكفاءة التشغيلية الإجمالية، وإصدار المحفظة، والحصول عليها، مع الحفاظ على الخسائر عند مستوى مقبول.

1.2.6 مستويات مراجعة إدارة مخاطر النظام

يتكون برنامج إدارة مخاطر النظام من ثلاثة مستويات إلزامية، على النحو التالي:

- مراجعات تأهيل الأعضاء، وتشمل الأعضاء الرئيسيين، والأعضاء المشاركين المحتملين.
- برنامج إدارة مخاطر مقدم خدمة الدفع.
- مراجعات نظام الأعضاء، للأعضاء الحاليين.

ملاحظة: يجب أن يكون واضحًا لجميع الأعضاء:

- (1) أن يتم تقديم جميع الأعضاء إلى إطار ICRM الذي تطلبه لوائح مصرف ليبيا المركزي (خاصة التعميم المتعلق بالترخيص والحوكمة).
- (2) أن الخط الأول والثاني من عناصر التحكم في الحماية يجب أن يشتمل على المستويات الثلاثة الإلزامية الموضحة هنا.

Actions for the three levels to be delegated from CBL to National Scheme Operator to execute and audit as such.

6.2.1.1 Member Onboarding Reviews

The Member Onboarding Review is mandatory for any entity applying to become a Principal Member or a participant Member, at the sole discretion of Scheme Risk Management Program staff.

The Member Onboarding Review takes place during the initial certification stage, and requires the entity to complete one or both of the following questionnaires:

- Scheme Risk Management Program Issuer Questionnaire
- Scheme Risk Management Program Acquirer Questionnaire.

If an entity that has applied to become a Member is not in compliance with the Standards, the National Scheme Operator may withhold approval of the application until the entity achieves compliance.

In addition, the National Scheme Operator reserves the right to require a Member Scheme Review if:

- Scheme Risk Management Program staff is dissatisfied with the response to a Member Onboarding questionnaire (in terms of speed, content, or both), or
- Scheme Risk Management Program staff determines that the Member represents a potential unacceptable risk, or potential threat to other Members.

NOTE: There may be an additional on-site review conducted by Scheme Risk Management Program staff and by the CBL within one year of assessment of the completed questionnaire.

6.2.1.2 Service Provider Risk Management Program

The Service Provider Risk Management Program addresses the risks to which a Service Provider may be exposed on an ongoing basis.

Following Service Provider registration, the National Scheme Operator segments the Service Provider's Portfolio to determine the entity's level of risk based on the types of services that the entity provides and its potential level of exposure to the network. Based on the results of this segmentation, the National Scheme Operator determines the most appropriate approach for evaluating the Service Provider's level of risk. These evaluations may include, but are not be limited to:

- Requesting information directly from the Service Provider to help determine the entity's risk profile and its ability to support Members; and
- Performing on-site reviews to evaluate the controls that the Service Provider has in place to mitigate risks.

The National Scheme Operator reserves the right as per a granted delegation from the CBL for Scheme Risk Management Program staff to conduct an on-site review of any Service Provider at any time.

The National Scheme Operator will provide a summary of the results of its review to any Member that has registered the Service Provider. A Service Provider that fails either or both of the following requirements may be subject to de-registration as a Service Provider:

- Demonstration to the satisfaction of the National Scheme Operator that the entity has adequate and effective controls in place to mitigate risk; and
- Adherence to a National Scheme Operator-approved action plan.

Topics covered during a Service Provider Risk Management Program review are listed below.

الإجراءات الخاصة بالمستويات الثلاثة التي سيتم تفويضها من قبل مصرف ليبيا المركزي إلى مشغل شبكة الدفع المحلية للتنفيذ والتدقيق على هذا النحو.

1.1.2.6.1 مراجعات تأهيل الأعضاء

تعد مراجعة تأهيل الأعضاء إلزامية، لجميع الكيانات التي تتقدم لتصبح عضوًا رئيسيًا أو عضوًا مشاركًا، وفقًا لتقدير موظفي برنامج إدارة مخاطر النظام.

تتم مراجعة تأهيل الأعضاء أثناء مرحلة الشهادة الأولية، وتتطلب من الكيان إكمال أحد الاستبيانين التاليين أو كليهما:

- استبيان جهة إصدار برنامج إدارة مخاطر النظام.
- استبيان جهة استحواذ برنامج إدارة مخاطر النظام.

إذا كان الكيان الذي تقدم بطلب ليصبح عضوًا لا يمثل للمعايير، فيجوز لمشغل شبكة الدفع المحلية حجب الموافقة على الطلب حتى يحقق هذا الكيان الامتثال.

بالإضافة إلى ذلك، يحتفظ مشغل شبكة الدفع المحلية بالحق في طلب مراجعة نظام الأعضاء إذا:

- كان موظفو برنامج إدارة مخاطر النظام طعنوا في الرد على استبيان تأهيل الأعضاء (من حيث السرعة أو المحتوى أو كليهما).
- قرر موظفو برنامج إدارة مخاطر النظام، أن العضو يمثل خطرًا محتملًا غير مقبول، أو تهديدًا محتملًا للأعضاء الآخرين.

ملاحظة: قد تكون هناك مراجعة إضافية في الموقع يتم إجراؤها من قبل موظفي برنامج إدارة مخاطر النظام ومصرف ليبيا المركزي، خلال سنة واحدة من تقييم الاستبيان المكتمل.

2.1.2.6.2 برنامج إدارة مخاطر مقدم الخدمة

يتناول برنامج إدارة مخاطر مقدم الخدمة، المخاطر التي قد يتعرض لها مقدم الخدمة بشكل مستمر. بعد تسجيل مقدم الخدمة، يقوم مشغل شبكة الدفع المحلية بتقسيم محفظة مقدم الخدمة، لتحديد مستوى مخاطر الكيان بناءً على أنواع الخدمات التي يقدمها هذا الكيان، ومستوى تعرضه المحتمل للشبكة. استنادًا إلى نتائج هذا التقسيم، ويحدد مشغل شبكة الدفع المحلية الطريقة الأنسب لتقييم مستوى مخاطر مقدم الخدمة. وقد تشمل هذه التقييمات، على سبيل المثال:

- طلب المعلومات مباشرة من مقدم الخدمة للمساعدة في تحديد ملف إدارة مخاطر الكيان، وقدرته على دعم الأعضاء.
 - إجراء مراجعات في الموقع لتقييم الضوابط التي يمتلكها مقدم الخدمة للتخفيف من المخاطر.
- لمشغل شبكة الدفع المحلية، ووفقًا للتفويض الممنوح من مصرف ليبيا المركزي، إجراء مراجعة، في أي وقت، لموظفي مقدم خدمة، وفي مقره، فيما يتعلق ببرنامج إدارة مخاطر النظام.
- يجب على مشغل شبكة الدفع المحلية أن يقدم ملخصًا لنتائج مراجعته لأي عضو قام بتسجيل مقدم الخدمة. وقد يخضع مقدم الخدمة الذي يخل بأحد المتطلبات التالية لإلغاء تسجيله بصفته مقدم خدمة:
- أن يثبت لمشغل شبكة الدفع المحلية أن الكيان لديه ضوابط كافية وفعالة للحد من المخاطر.
 - الالتزام بخطة العمل المعتمدة من قبل مشغل شبكة الدفع المحلية.
- الموضوعات التي يتم تناولها أثناء مراجعة برنامج إدارة مخاطر مقدم الخدمة مذكورة أدناه.

The Member must at all times be entirely responsible for and must manage, direct, and control all aspects of its Program and Program Service performed by Service Providers, and establish and enforce all Program management and operating policies in accordance with the Standards.

The completion of a Service Provid'r Ri'k Management Program review does not imply, suggest, or otherwise mean that the National Scheme Operator endorses the Service Provider or the nature or quality of Program Service or other performance or that the National Scheme Operator approves of, is a party to, or a participant in, any act or omission by a Service Provider or other entity acting for or on behalf of a Member.

6.2.1.3 Member Scheme Reviews

The National Scheme Operator requires that each Member (parent and child Member ID number) conduct its issuing and acquiring Activities in a prudent and financially sound manner so as to avoid inordinate risk to itself and other Members.

The national Scheme Operator under its' general power of supervision may select Members for a Member Scheme Review of their systems and Programs, in an effort to determine whether the selected Member has put in place adequate and effective controls to avoid and manage risk. The Member Scheme Review may be conducted on site by Scheme Risk Management Program staff or through the completion of an online questionnaire by the Member.

A Member must submit to and cooperate in a Member Scheme Review. The National Scheme Operator, at its sole discretion, may determine that a Member Scheme Review is necessary or appropriate.

The Member will receive a detailed"and comprehensive gap analysis report containing recommendations and benefits of critical findings during the course of the review. If required, the report will be supplemented by an action plan.

6.2.1.4 Member Consultative Reviews

The Member Consultative Review is optional and is available upon request by a Member. This review is consultation-oriented and is conducted on site. The Member will receive a detailed and comprehensive gap analysis report containing recommendations and benefits of critical findings during the course of the review. If required, the report will be supplemented by an action plan.

6.2.2 Scheme Risk Management Program Review Topics

This section describes the topics that are covered by Scheme Risk Management Program reviews, as applicable. Additional topics may be included during a review at the sole discretion of the National Scheme Operator.

Applicable to All Issuers, Acquirers, and Service Providers:

- Organizational structure
- Licensing and registration
- Business continuity
- Data governance and privacy
- Information security and Payment Card Industry Data Security Standard (PCI DSS) compliance
- Internal and external fraud
- AMLCFT
- Fraud loss control Standards

يجب أن يكون العضو مسؤولاً مسؤولاً كاملة وفي جميع الأوقات، كما يجب عليه إدارة وتوجيه ومراقبة جميع جوانب البرنامج، وخدمة البرنامج التي يقوم بها مقدمو الخدمة، وإنشاء وتنفيذ جميع سياسات إدارة البرامج وتشغيلها وفقاً للمعايير.

لا يعني إكمال مراجعة برنامج إدارة مخاطر مقدم الخدمة، أن مشغل شبكة الدفع المحلية يؤيد مقدم الخدمة أو طبيعة أو جودة خدمة البرنامج أو أي أداء آخر، أو أن مشغل شبكة الدفع المحلية يوافق عليه، هو طرف أو مشارك في أي فعل أو إغفال من قبل مقدم الخدمة أو أي كيان آخر يعمل لصالح أو نيابة عن العضو.

3.1.2.6. مراجعات نظام الأعضاء

يوجب مشغل شبكة الدفع المحلية، أن يقوم كل عضو (رقم هوية العضو الرئيسي والفرعي) بإصدار الأنشطة والحصول عليها بطريقة حكيمة وسليمة مالياً، لتجنب المخاطر التي يتعرض لها هو والأعضاء الآخريين.

يجوز لمشغل شبكة الدفع المحلية بناءً على سلطة التفويض، اختيار أعضاء، لمراجعة نظام الأعضاء لأنظمتهم وبرامجهم، في محاولة لتحديد ما إذا كان العضو المختار قد وضع ضوابط كافية وفعالة لتجنب المخاطر وإدارتها. ويمكن إجراء مراجعة نظام الأعضاء، وفي مقرهم، من قبل موظفي برنامج إدارة مخاطر النظام أو من خلال ملء استبيان عبر الإنترنت من قبل العضو.

يجب على العضو الالتزام بالتعاون عند مراجعة نظام الأعضاء. ووفقاً لسلطته التقديرية، قد يقرر مشغل شبكة الدفع المحلية، أن مراجعة نظام الأعضاء ضرورية أو مناسبة.

سيتلقى العضو تقريراً تفصيلياً وشاملاً عن تحليل أوجه القصور، يحتوي على توصيات وفوائد النتائج الحاسمة خلال فترة المراجعة. وإذا لزم الأمر، سيتم إرفاق تقرير المراجعة بخطة عمل.

4.1.2.6. مراجعات الأعضاء الاستشارية

تعد المراجعة الاستشارية للأعضاء، مراجعة اختيارية ومتاحة عند طلب العضو. وتعد هذه المراجعة ذات طابع استشاري، يتم إجراؤها في المقر. ويتلقى العضو تقريراً تفصيلياً وشاملاً عن تحليل أوجه القصور، يحتوي على توصيات وفوائد النتائج الحاسمة خلال فترة المراجعة. إذا لزم الأمر، سيتم إرفاق تقرير المراجعة بخطة عمل.

2.2.6. موضوعات مراجعة برنامج إدارة مخاطر النظام

يصف هذا القسم الموضوعات التي تغطيها مراجعات برنامج إدارة مخاطر النظام، حسب الاقتضاء. وقد يتم تضمين موضوعات إضافية أثناء المراجعة، وفقاً لتقدير مشغل شبكة الدفع المحلية وحده.

ينطبق على جميع جهات الإصدار، القبول ومقدمي الخدمات:

- الهيكل التنظيمي.
- الترخيص والتسجيل.
- استمرارية الأعمال.
- حوكمة البيانات والخصوصية.
- الامتثال لمعايير أمان البيانات، و صناعة بطاقات الدفع، وأمن المعلومات.
- الاحتيال الداخلي والخارجي.
- مكافحة غسل الأموال، و تمويل الإرهاب.
- معايير مكافحة خسائر الاحتيال.
- إدارة التفويض.

- Authorization management
- Chargebacks and recoveries
- Fraud strategy
- Franchise compliance programs
- Management information systems
- Account Data Compromise Event management
- Settlement risk

Applicable to Issuers and Issuer Service Providers:

- Card acquisition and application process
- Prepaid risk management

Applicable to Acquirers and Acquirer Service Providers:

- Merchant application and monitoring

6.2.3 Scheme Risk Management Program Reports

After a Scheme Risk Management Program review, the Member or non-Member, as the case may be, will receive a written report indicating its status as to compliance with the Standards, plus other required or recommended actions. In the case of noncompliance:

- The report will indicate a number of actions that must be taken to bring the Member or non-Member into compliance.
- The Member or non-Member, as the case may be, must complete an action plan and indicate implementation dates.
- The Scheme Risk Management Program staff assesses the action plan and the proposed implementation dates, monitors progress and results, and determines whether the Member or Service Provider meets National Scheme Operator requirements.

6.2.4 Member Scheme Review Conditions

The following conditions are examples of specific situations or conditions that may warrant a Member Scheme Review. Other conditions may also warrant a Member Scheme Review.

6.2.4.1 Member Scheme Review Issuer Criteria

The National Scheme Operator may subject an Issuer to a Member Scheme Review if any of the following conditions exist:

1. The National Scheme Operator determines that the Issuer creates or may create a burden to the system. By way of example and not limitation, this condition exists when the Issuer's fraud basis points exceed two times the country average.
2. The Issuer has been identified two or more times for noncompliance with National Scheme Operator fraud reporting Standards.

6.2.4.2 Member Scheme Review Acquirer Criteria

The National Scheme Operator may subject an Acquirer to a Member Scheme Review if any of the following conditions exist:

National Scheme Operator staff determines that the Acquirer creates or may create a burden to the system. By way of example and not limitation, this condition exists when the Acquirer's fraud basis points exceed two times the country average (averaged over four quarters).

- عمليات رد المبالغ المدفوعة، والمبالغ المستردة.
- استراتيجية الاحتيال.
- برامج امتثال الامتياز.
- نظم المعلومات الإدارية.
- إدارة حدث اختراق بيانات الحساب.
- مخاطر الاختراق.

ينطبق على جهات الإصدار ومقدمي خدمات جهة الإصدار:

- عملية الحصول والتقديم على البطاقة.
- إدارة مخاطر الدفع المسبق.
- ينطبق على جهات القبول ومقدمي خدمات جهة القبول:
- تطبيق التاجر والمراقبة.

3.2.5 تقارير برنامج إدارة مخاطر النظام

بعد مراجعة برنامج إدارة مخاطر النظام، يتلقى العضو أو غير العضو، حسب الحالة، تقريرًا مكتوبًا يشير إلى حالته فيما يتعلق بالامتثال للمعايير، بالإضافة إلى الإجراءات الأخرى المطلوبة أو الموصى بها. في حالة عدم الامتثال:

- سيشير التقرير إلى عدد من الإجراءات التي يجب اتخاذها لتحقيق امتثال العضو أو غير العضو.
- يجب على العضو أو غير العضو، حسب مقتضى الحال، إكمال خطة العمل والإشارة إلى تواريخ التنفيذ.
- يقوم موظفو برنامج إدارة مخاطر النظام بتقييم خطة العمل وتواريخ التنفيذ المقترحة، ومراقبة التقدم والنتائج، وتحديد ما إذا كان العضو أو مقدم الخدمة يفي بمتطلبات مشغل شبكة الدفع المحلية.

4.2.6 شروط مراجعة نظام الأعضاء

الشروط التالية هي أمثلة لحالات أو ظروف معينة قد تستدعي مراجعة نظام الأعضاء. قد تتطلب الشروط الأخرى أيضًا مراجعة نظام الأعضاء.

1.4.2.6 معايير جهة الإصدار لمراجعة نظام الأعضاء

يجوز لمشغل شبكة الدفع المحلية، إخضاع جهة الإصدار لمراجعة نظام الأعضاء في حالة وجود أحد الشروط التالية:

1. إذا قرر مشغل شبكة الدفع المحلية أن جهة الإصدار تنشئ، أو قد تخلق عبئًا على النظام على سبيل المثال، ويطبق هذا الشرط عندما تتجاوز النقاط الأساسية للاحتيال الخاصة بجهة الإصدار ضعف متوسط البلد.
2. إذا تم تحديد جهة الإصدار مرتين أو أكثر لعدم امتثالها لمعايير الإبلاغ عن الاحتيال لمشغل شبكة الدفع المحلية.

2.4.2.6 معايير جهة القبول لمراجعة نظام الأعضاء

يجوز لمشغل شبكة الدفع المحلية إخضاع جهة القبول لمراجعة نظام الأعضاء في حالة وجود أحد الشروط التالية:

إذا قرر موظفو مشغل شبكة الدفع المحلية أن جهة القبول تنشئ أو قد تخلق عبئًا على النظام. على سبيل المثال، يطبق هذا الشرط عندما تتجاوز النقاط الأساسية للاحتيال الخاصة بجهة القبول ضعف متوسط البلد (بمتوسط يزيد على أربعة أرباع).

The Acquirer has been notified of a violation of the Illegal or Brand-damaging Transactions Rule.

The Acquirer acquires Transactions for a Merchant that has engaged in activity that the National Scheme Operator deems inappropriate in connection with use of a Mark.

6.2.4.3 Basis Points Calculation

The calculation for fraud basis points is performed as follows:

- The gross fraud (as reported to the Fraud and Loss Database) for a given time frame (such as a quarter or a year)
- Is divided by the corresponding sales for the same time frame
- The result is multiplied by a factor of 10,000 to obtain fraud basis points.

6.3 Fraud Loss Control Standards

The existence and use of meaningful controls are an effective means to limit total fraud losses and losses for all fraud types. This section describes minimum requirements for Issuer and Acquirer fraud loss control programs.

A Member must establish adequate fraud loss controls for each of its issuing and acquiring Programs, and any tokenization-related Program, and use them actively and effectively.

An Acquirer must transmit full magnetic stripe or EMV chip data for all Point-of-Interaction (POI) Card-read Transactions. An Issuer must, at a minimum, incorporate all required Card security features and comply with Card production Standards.

Scheme Risk Management Program staff, in its sole discretion, will determine a Member's compliance with these fraud loss control Standards and has the authority, either directly or through its designee, to perform audits and to mandate implementation and use of controls deemed necessary to achieve compliance.

6.3.1 Issuer Fraud Loss Control Programs

An Issuer's fraud loss control program must meet the following minimum requirements, and preferably will include the recommended additional parameters. The program must automatically generate daily fraud monitoring reports or real-time alerts. Issuer staff trained to identify potential fraud must analyze the data in these reports within 24 hours.

6.3.1.1 Issuer Authorization Requirements

An Issuer must implement a rules-based authorization strategy with the following parameters:

- Decision matrix for Card validation number (CVV) 1, CVV 2, and CVV 3 validation results
- Limits on single-day and multiple-day Transaction velocity (number of Transactions)
- Limits on single-day and multiple-day monetary spending (value of Transactions)
- Limits for high-risk Card acceptor business codes (MCCs) and locations on a daily or, if necessary, more frequent basis
- Limits for particular POI entry modes (such as magnetic stripe-read, primary account number [PAN] key-entry, chip-read, Card-Not-Present [CNP])
- Limits for particular country codes

إذا تم إخطار جهة القبول بانتهاك قاعدة المعاملات غير القانونية أو الضارة بالعلامة التجارية.

إذا كانت جهة القبول قبلت حركات بيع لتاجر شارك في نشاط، يراه مشغل شبكة الدفع المحلية غير مناسب فيما يتعلق باستخدام العلامة.

3.4.2.6 حساب النقاط الأساسية

يتم احتساب النقاط الأساسية للاحتيال على النحو التالي:

- الاحتيال الإجمالي (كما تم إبلاغ قاعدة بيانات الاحتيال والخسارة) لفترة زمنية معينة (مثل ربع سنة أو سنة).
- مقسومًا على المبيعات المقابلة لنفس لفترة الزمنية.
- يتم ضرب النتيجة بعامل قدره 10,000 للحصول على النقاط الأساسية للاحتيال.

3.6 معايير التحكم في خسائر الاحتيال

يعد وجود واستخدام ضوابط ذات فاعلية، وسيلة فعالة للحد من خسائر الاحتيال والخسائر الإجمالية لجميع أنواع الاحتيال. ويصف هذا القسم الحد الأدنى من المتطلبات لبرامج مكافحة خسائر الاحتيال الخاصة بجهة الإصدار وجهة القبول.

يجب على العضو وضع ضوابط كافية للتحكم في خسائر الاحتيال لكل من برامج الإصدار والقبول وأي برنامج مرتبط بالترميز، واستخدامها بنشاط وفعالية.

يجب على جهة القبول إرسال بيانات الشريط المغناطيسي كاملة أو شريحة EMV لجميع معاملات قراءة بطاقة نقطة التفاعل. يجب على جهة الإصدار، على الأقل، دمج جميع ميزات أمان البطاقة المطلوبة والامتثال لمعايير إنتاج البطاقة.

ويحدد موظفو برنامج إدارة مخاطر النظام، وفقًا لتقديرهم الخاص، امتثال العضو لمعايير مكافحة خسائر الاحتيال، ولديهم السلطة، إما بشكل مباشر أو من خلال من ينوب عنهم، لإجراء عمليات التدقيق وفرض تطبيق الضوابط التي تعتبر ضرورية لتحقيق الامتثال.

1.3.6 برامج التحكم في خسائر الاحتيال لجهة الإصدار

يجب أن يفي برنامج مكافحة خسائر الاحتيال الخاص بجهة الإصدار بالحد الأدنى من المتطلبات التالية، ويفضل أن يتضمن المعايير الإضافية الموصى بها. ويجب أن يقوم البرنامج تلقائيًا بإنشاء تقارير يومية لمراقبة الاحتيال أو التنبيه عليها في الوقت الفعلي. ويجب أن يقوم موظفو جهة الإصدار اللذين تم تدريبهم على تحديد الاحتيال المحتمل بتحليل البيانات الواردة في هذه التقارير خلال 24 ساعة.

1.1.3.6 متطلبات تفويض جهة الإصدار

يجب أن تقوم جهة الإصدار بتنفيذ إستراتيجية تفويض قائمة على قواعد مع الضوابط التالية:

- مصفوفة القرار لنتائج التحقق من رقم التحقق من البطاقة (CVV1) و CVV 2 و CVV 3).
- حدود سرعة المعاملات ليوم واحد و عدة أيام (عدد المعاملات).
- حدود الإنفاق النقدي ليوم واحد وعدة أيام (قيمة المعاملات).
- حدود رموز الأعمال عالية المخاطر لمتقبلي البطاقات (sMCC) والمواقع على أساس يومي، وإذا لزم الأمر، على أساس مكرر.
- حدود لأوضاع إدخال نقاط تفاعل معينة (مثل قراءة الشريط المغناطيسي، مفتاح إدخال رقم الحساب الأساسي، قراءة الشريحة، البطاقة غير الموجودة)
- حدود رموز دول معينة.

- Decision matrix for expiration date errors
- Decision matrix for Track 1 validation errors
- Decision matrix for geographic anomalies

6.3.1.2 Issuer Fraud Monitoring Requirements

An Issuer must generate daily reports or real-time alerts monitoring both authorization and clearing data, if possible, at the latest on the day following the Transaction(s) for the following parameters:

- Single Transaction exceeding a certain amount (established by the Issuer)
- Multiple Transactions exceeding a certain amount (established by the Issuer)
- PAN key-entry Transactions exceeding a certain amount and/or number (established by the Issuer)
- Transactions taking place at high-risk MCCs and Merchant locations
- An Issuer with the conditions present in Table 10.1 must implement additional fraud loss controls.

Table 6.1—Additional Issuer Fraud Loss Control Requirement

(See appendix number 43)

6.3.1.3 Issuer Network Monitoring Requirements

An Issuer must use the network monitoring service provided by the National Scheme Operator for all Transactions arising from a prepaid Card Program that are Processed Transactions.

In the event that the National Scheme Operator detects fraudulent or potentially fraudulent activity (“suspicious activity”) involving a prepaid Account, the National Scheme Operator may impose a temporary block on the affected PAN of such prepaid Account with respect to all authorization requests received for Transactions that are of the same type as the suspicious activity (for example, ATM Transactions or CNP Transactions). The National Scheme Operator will attempt to notify the Issuer of the block, and thereby enable the Issuer to implement additional controls.

6.3.1.4 Product Portfolio Management

An Issuer is required to monitor its Account Portfolios for the following:

- Total Transaction fraud basis points
- Domestic Transaction fraud basis points
- Cross-border Transaction fraud basis points
- Fraud basis points by Transaction type (for example, electronic commerce [e-commerce] Transactions, mail order/telephone order [MO/TO] Transactions, Card-present Transactions)
- 3DS 2.0 or EMV 3DS fully authenticated Transaction fraud basis points

- مصفوفة القرار لأخطاء تاريخ انتهاء الصلاحية.
- مصفوفة القرار لأخطاء التحقق من المسار 1
- مصفوفة القرار بشأن الشذوذ الجغرافي.

2.1.3.6 متطلبات مراقبة الاحتيال لجهة الإصدار

يجب على جهة الإصدار إنشاء تقارير يومية أو تنبيهات في الوقت الفعلي لمراقبة كل من بيانات التفويض والمقاصة، وإن أمكن، على أبعد تقدير في اليوم التالي للمعاملة (المعاملات) وفقاً للمعاملات التالية:

- معاملة واحدة تتجاوز مبلغًا معينًا (تحددها جهة الإصدار).
 - معاملات متعددة تتجاوز مبلغًا معينًا (تحددها جهة الإصدار).
 - معاملات مفتاح إدخال رقم الحساب الأساسي التي تتجاوز مبلغًا، أو رقمًا معينًا (تحددها جهة الإصدار)
 - المعاملات التي تتم في MCCs ومواقع التجار عالية الخطورة
- بالإضافة إلى الشروط الواردة في الجدول 10.1 يجب على جهة الإصدار تنفيذ الضوابط الإضافية لخسائر الاحتيال الواردة في الجدول 6.1. التالية:

الجدول 6.1 - الضوابط الإضافية للتحكم في خسائر الاحتيال لجهة الإصدار:

(انظر الملحق رقم 43)

3.1.3.6 متطلبات مراقبة شبكة جهة الإصدار

يجب على جهة الإصدار أن تستخدم خدمة مراقبة الشبكة التي يوفرها مشغل شبكة الدفع المحلية لجميع المعاملات الناشئة عن برنامج بطاقة الدفع المسبق، والمعاملات التي تمت معالجتها. وفي حالة اكتشاف مشغل شبكة الدفع المحلية نشاطًا احتياليًا أو يشتبه أن يكون احتياليًا (“نشاط مشبوه“)، يتضمن حسابًا للدفع المسبق، يجوز له فرض حظر مؤقت على رقم الحساب الأساسي المتأثر بحساب الدفع المسبق فيما يتعلق بجميع طلبات التفويض المستلمة للمعاملات التي هي من نفس نوع النشاط المشبوه (على سبيل المثال، معاملات أجهزة الصراف الآلي أو معاملات البطاقة غير الموجودة). ويجب على مشغل شبكة الدفع المحلية إخطار جهة الإصدار بالحظر، وبالتالي تمكين جهة الإصدار من تنفيذ ضوابط إضافية.

4.1.3.6 إدارة محافظ المنتجات

يُطلب من جهة الإصدار مراقبة محافظ حساباتها من أجل ما يلي:

- إجمالي النقاط الأساسية للاحتيال في المعاملات.
- النقاط الأساسية للاحتيال في المعاملات الوطنية.
- النقاط الأساسية للاحتيال في المعاملات عبر الحدود
- النقاط الأساسية للاحتيال حسب نوع المعاملة (على سبيل المثال، معاملات التجارة الإلكترونية، معاملات الطلب عبر البريد/الطلب عبر الهاتف، معاملات البطاقة الموجودة)
- النقاط الأساسية للاحتيال الخاصة بمعاملات DS 2.03 أو DS3 MVE المصدق عليها بالكامل.

6.3.1.5 Recommended Additional Issuer Monitoring

The National Scheme Operator recommends that Issuers additionally monitor the following parameters:

- Account-generated attacks
- CVV 1, CVV 2, and CVV 3 validation failures
- Expiration date failures
- Invalid account number (mis-posting) Transactions
- Cardholder-activated Terminal (CAT) Transactions
- Account Data Compromise Event or Potential Compromise Event Transactions
- Credit Transactions (such as refunds) and Merchant authorization reversals
- PIN, Token, or Authorization Request Cryptogram (ARQC) validation failures
- Cardholder Verification Method (CVM)
- Stand-In verification of CVV 1

6.3.1.6 Additional Prepaid Monitoring Requirements

An Issuer must comply with the following additional monitoring requirements for its prepaid Card Programs.

Fraud Detection

An Issuer must develop, implement, and maintain formal prepaid Portfolio standards to monitor funding situations. An Issuer also must:

- Assess and monitor exposure to unfunded commitments; and
- Regularly analyze trends in Account volume and growth.

Program Monitoring

Adequate fraud controls must be in place to monitor the following Program activity:

- Number of Accounts for each Cardholder
- Number of loads performed a day—Loads arising from payment Card acceptance at a Point-of-Sale (POS) location identified with one of the following MCCs may require enhanced review:
 - MCC 4829 (Money Transfer)
 - MCC 6050 (Quasi Cash—Financial Institution)
 - MCC 6051 (Quasi Cash—Merchant)
- Number of loads arising from payment Card acceptance performed daily and over time (specific time period)
- Number of loads performed at the same agent daily and over time
- Value of loads performed at the same agent daily and over time
- •Origination of load—cash, Automated Clearing House (ACH), card-to-card balance transfer, or wire method used for load transfer (for example, e-commerce, MO/TO, or recurring payment Transaction)
- Refunds
- Reload and withdrawal patterns

5.1.3.6 مراقبة جهة الإصدار الإضافية الموصى بها

يوصي مشغل شبكة الدفع المحلية بأن تقوم جهات الإصدار بالإضافة إلى ذلك مراقبة المعايير التالية:

- الهجمات الناتجة عن الحسابات.
- حالات فشل التحقق من CVV 1 و CVV 2 و CVV 3.
- فشل تاريخ انتهاء الصلاحية.
- رقم الحساب غير الصحيح (خطأ في قيد) المعاملات.
- معاملات المحطة التي ينشطها حامل البطاقة.
- معاملات حدث اختراق بيانات الحساب أو حدث الاختراق المحتمل.
- معاملات الائتمان (مثل المبالغ المستردة) وإلغاء تفويض التاجر.
- حالات فشل التحقق من رقم التعريف الشخصي أو الترميز أو برنامج تشفير طلب التفويض.
- طريقة التحقق من حامل البطاقة.
- التحقق الاحتياطي من CVV 1.

6.1.3.6.متطلبات المراقبة الإضافية للدفع المسبق

يجب أن تلتزم جهة الإصدار بمتطلبات المراقبة الإضافية التالية لبرامج بطاقات الدفع المسبق.

الكشف عن الاحتيال

يجب على جهة الإصدار أن تطور وتنفذ وتحافظ على معايير محافظ الدفع المسبق الرسمية لمراقبة أوضاع التمويل. ويجب على جهة الإصدار أيضًا:

- تقييم ومراقبة التعرض للالتزامات غير الممولة.
- تحليل الاتجاهات في حجم ونمو الحساب بانتظام.

مراقبة البرنامج

يجب وضع ضوابط احتيال مناسبة لمراقبة نشاط البرنامج التالي:

- عدد الحسابات لكل حامل بطاقة.
- عدد عمليات التحميل التي يتم إجراؤها في اليوم - وقد تتطلب عملية التحميل الناشئة عن قبول بطاقة الدفع في أحد مواقع نقاط البيع المحددة بأحد MCCs التالية مراجعة محسّنة:
 - MCC 4829 (تحويل الأموال).
 - MCC 6050 (شبه نقدي - مؤسسة مالية).
 - MCC 6051 (شبه نقدي - تاجر).

عدد عمليات التحميل الناتجة عن قبول بطاقة الدفع التي يتم إجراؤها يوميًا، وعلى مدار الوقت (فترة زمنية محددة)

- عدد عمليات التحميل التي يتم إجراؤها على نفس الوكيل يوميًا، وعلى مدار الوقت.
- قيمة عمليات التحميل التي يتم إجراؤها على نفس الوكيل يوميًا، وعلى مدار الوقت.
- أصل عملية التحميل - النقد، أو غرفة المقاصة الآلية، أو تحويل الرصيد من بطاقة إلى بطاقة، أو طريقة التحويل المصرفي المستخدم لعمليات التحميل (على سبيل المثال، التجارة الإلكترونية، أو معاملات الطلب عبر البريد/الطلب عبر الهاتف، أو معاملة الدفع المتكررة)
- المبالغ المستردة.
- أنماط إعادة التحميل والسحب.

Card Limits

Adequate fraud controls must be in place to monitor the following Card activity:

- Minimum and maximum initial load values
- Card reloading procedures
- Maximum number of loads each Card a day
- Maximum value on each Card a day
- Accepted payment methods to purchase, load, or reload the Card

6.3.1.7 Fraud Detection Tool Implementation

An Issuer is required to implement a fraud detection tool, which appropriately complements the fraud strategy deployed by the Issuer. The combination of the authorization controls and the fraud detection tool should ensure that an Issuer controls fraud to an acceptable level.

The performance of an Issuer's fraud detection tool at least should achieve minimum performance requirements. The following performance indicators are required to help an Issuer manage an effective fraud detection tool. Such performance indicators must include, but are not limited to:

- Fraud Account detection rates
- Average number of Transactions per fraud case
- Average fraud case duration
- Average loss per fraud case
- Percentage of fraudulent e-commerce Transactions of LYD XX (or the local currency equivalent) or less for the purchase of Digital Goods reported through the Fraud and Loss Database, compared to the total of fraudulent e-commerce Transactions of LYD XX or less reported through the Fraud and Loss Database.

6.3.1.8 Cardholder Communication Strategy

An Issuer must implement a Cardholder communication strategy. A communication strategy consists of defining (i) the criteria for contacting a Cardholder, (ii) the communication channel for contacting the Cardholder, and (iii) the actions to be taken in case of failure to contact the Cardholder. Such communication channels may include short message service (SMS) alerts, email messages, phone calls, and letters.

6.3.2 Acquirer Fraud Loss Control Programs

An Acquirer must establish, and ensure that each of its Service Providers, ATM owners, and other agents implement, a fraud loss control program that meets the following minimum requirements, and preferably will include the recommended additional parameters. The program must automatically generate daily fraud monitoring reports or real-time alerts. Acquirer staff trained to identify potential fraud must analyze the data in these reports within 24 hours.

حدود البطاقة

يجب وضع ضوابط احتيال مناسبة لمراقبة نشاط البطاقة التالي:

- الحد الأدنى والحد الأقصى لقيم عملية التحميل الأولية.
- إجراءات إعادة تحميل البطاقة.
- الحد الأقصى لعدد عمليات التحميل لكل بطاقة في اليوم.
- الحد الأقصى لقيمة عملية التحميل لكل بطاقة في اليوم.
- طرق الدفع المقبولة لشراء البطاقة أو تحميلها أو إعادة تحميلها.

7.1.3.6. تطبيق أداة الكشف عن الاحتيال

يجب على جهة الإصدار تنفيذ أداة الكشف عن الاحتيال، والتي تُكمل بشكل مناسب استراتيجية الاحتيال التي تنشرها جهة الإصدار. ويجب أن يضمن الجمع بين ضوابط التفويض، وأداة الكشف عن الاحتيال، وأن جهة الإصدار تتحكم في الاحتيال إلى مستوى مقبول.

يجب أن تحقق وسيلة أداة الكشف عن الاحتيال الخاصة بجهة الإصدار الحد الأدنى من متطلبات الأداء. وتعد مؤشرات الأداء التالية مطلوبة لمساعدة جهة الإصدار على إدارة أداة فعالة، للكشف عن الاحتيال. ويجب أن تشمل مؤشرات الأداء هذه، على سبيل المثال:

- معدلات الكشف عن حساب الاحتيال.
- متوسط عدد المعاملات لكل حالة من حالات الاحتيال.
- متوسط مدة حالة الاحتيال.
- متوسط الخسارة لكل حالة من حالات الاحتيال.
- النسبة المئوية لمعاملات التجارة الإلكترونية الاحتيالية لـ XX دينار ليبي (أو ما يعادله بالعملية الوطنية) أو أقل لشراء السلع الرقمية التي تم الإبلاغ عنها من خلال قاعدة بيانات حالات الاحتيال والخسارة، مقارنة بإجمالي معاملات التجارة الإلكترونية الاحتيالية التي تبلغ XX دينار ليبي، أو أقل التي تم الإبلاغ عنها من خلال قاعدة بيانات حالات الاحتيال والخسارة.

8.1.3.6 إستراتيجية التواصل مع حامل البطاقة

يجب على جهة الإصدار تنفيذ إستراتيجية تواصل مع حامل البطاقة. وتتكون هذه الاستراتيجية من تحديد (1) معايير التواصل بحامل البطاقة. (2) قناة الاتصال للتواصل مع حامل البطاقة. (3) الإجراءات التي يجب اتخاذها في حالة فشل التواصل بحامل البطاقة.

وقد تتضمن قنوات الاتصال هذه تنبيهات خدمة الرسائل القصيرة ورسائل البريد الإلكتروني والمكالمات الهاتفية والرسائل.

2.3.6. برامج التحكم في خسائر الاحتيال لجهة القبول

يجب على جهة القبول أن تنشئ وتضمن أن كل من مقدمي الخدمة ومالكي أجهزة الصراف الآلي والوكلاء الآخرين ينفذون برنامجًا للتحكم في خسائر الاحتيال، ويحقق الحد الأدنى من المتطلبات المنصوص عليها، ويفضل أن يشمل الضوابط الإضافية الموصى بها. ويجب أن يقوم البرنامج تلقائيًا بإنشاء تقارير يومية لمراقبة حالات الاحتيال أو تنبيهات في الوقت الفعلي.

يجب أن يقوم موظفو جهة القبول المدربون على تحديد الاحتيال المحتمل بتحليل البيانات الواردة في هذه التقارير خلال 24 ساعة.

6.3.2.1 Acquirer Authorization Monitoring Requirements

Daily reports or real-time alerts monitoring Merchant authorization requests must be generated at the latest on the day following the authorization request, and must be based on the following parameters:

Number of authorization requests above a threshold set by the Acquirer for that Merchant
Ratio of non-Card-read to Card-read Transactions that is above the threshold set by the Acquirer for that Merchant

PAN key entry ratio that is above the threshold set by the Acquirer for that Merchant

Repeated authorization requests for the same amount or the same Cardholder Account

Increased number of authorization requests

Merchant authorization reversals that do not match a previous purchase Transaction

Out-of-pattern Transaction volume, including but not limited to:

Repeated authorization requests

- High velocity authorizations
- Technical fallback of chip to magnetic stripe
- High volume of Contactless Transactions
- Sequential Account generated attacks
- Unusual activity in connection with the use of Cards or Accounts issued under a particular bank identification number (BIN)

6.3.2.2 Additional Acquirer Authorization Monitoring Requirements for High-Risk Negative Option Billing Merchants

In addition to the Acquirer authorization monitoring requirements listed in section 6.2.2.1 of this manual, an Acquirer of a high-risk negative option billing Merchant must monitor authorization Transaction messages to identify when the same Account number appears among different high-risk negative option billing Merchant IDs in the Acquirer's Portfolio within 60 calendar days.

When the Acquirer identifies such an Account, the Acquirer must take reasonable steps to verify that each Transaction conducted by the valid Cardholder with the associated high-risk negative option billing Merchant is a bona fide Transaction. This verification may include, but is not limited to, an electronic copy or hard copy of the Transaction information document (TID). All such verification information must be:

- Retained by the Acquirer for a period of at least one year from the verification date; and
- Made available to the National Scheme Operator upon request.

6.3.2.3 Acquirer Merchant Deposit Monitoring Requirements

Daily reports or real-time alerts monitoring Merchant deposits must be generated at the latest on the day following the deposit, and must be based on the following parameters:

- Increases in Merchant deposit volume
- Increase in a Merchant's average ticket size and number of Transactions for each deposit
- Change in frequency of deposits
- Change in technical fallback rates, or a technical fallback rate that exceeds five percent of a Merchant's total Transaction volume

1.2.3.6 متطلبات مراقبة تفويض جهة القبول

يجب إصدار التقارير اليومية أو تنبيهات الوقت الفعلي التي تراقب طلبات تفويض التاجر على أبعد تقدير في اليوم التالي لطلب التفويض، ويجب أن تستند إلى المعايير التالية:

عدد طلبات التفويض فوق الحد التي تحدده جهة القبول لذلك التاجر.

نسبة المعاملات غير المقروءة بالبطاقة، إلى نسبة المعاملات المقروءة بالبطاقة، والتي تكون أعلى من الحد التي حددته جهة القبول لذلك التاجر.

نسبة إدخال مفتاح الحساب الأساسي أعلى من التي حددته جهة القبول لذلك التاجر.

طلبات التفويض المتكررة لنفس المبلغ أو نفس حساب حامل البطاقة.

زيادة عدد طلبات التفويض.

عمليات إلغاء تفويض التاجر التي لا تتطابق مع معاملة شراء سابقة

حجم المعاملات خارج النطاق، بما في ذلك على سبيل المثال:

- طلبات التفويض المتكررة
- تصاريح السرعة العالية
- الرجوع الفني من الشريحة إلى الشريط المغناطيسي
- عدد كبير من المعاملات الغير متصلة
- إنشاء حساب متسلسل الهجمات
- نشاط غير اعتيادي فيما يتعلق باستخدام البطاقات أو الحسابات الصادرة بموجب رقم تعريف مصرفي معين.

2.2.3.6 متطلبات مراقبة تفويض جهة القبول الإضافية لتجار فواتير الخيارات السلبية عالية المخاطر

بالإضافة إلى متطلبات مراقبة تفويض جهة القبول المدرجة في القسم 6.2.2.1 من هذا الدليل، يجب على جهة استحوذ تاجر فواتير الخيارات السلبية عالية المخاطر أن يراقب رسائل معاملات التفويض لتحديد متى يظهر رقم الحساب نفسه بين مختلف معرفات تاجر فواتير الخيارات السلبية عالية المخاطر في محفظة جهة القبول خلال 60 يومًا تقويميًا.

عندما تحدد جهة القبول مثل هذا الحساب، يجب عليها اتخاذ خطوات معقولة للتحقق من أن كل معاملة يتم إجراؤها من قبل حامل البطاقة الصالح مع تاجر فواتير الخيارات السلبية عالية المخاطر، هي معاملة حسنة النية. وقد يشمل هذا التحقق، على سبيل المثال، نسخة إلكترونية أو نسخة ورقية من مستند معلومات المعاملة. ويجب أن تكون جميع معلومات التحقق:

- محفوظة لدى جهة القبول لمدة سنة واحدة على الأقل من تاريخ التحقق.
- متاحة لمشغل شبكة الدفع المحلية عند الطلب.

3.2.3.6 متطلبات مراقبة إيداع التاجر القابل

يجب إصدار التقارير اليومية أو التنبيهات في الوقت الفعلي لمراقبة إيداع التاجر على أبعد تقدير في اليوم التالي للإيداع، ويجب أن تستند إلى المعايير التالية:

- الزيادات في حجم إيداع التاجر.
- زيادة متوسط حجم تذكرة التاجر، وعدد المعاملات لكل إيداع.
- التغيير في طريقة الإيداعات.
- تغيير في معدلات التراجع الفني، أو معدل التراجع الفني الذي يتجاوز خمسة بالمائة من إجمالي حجم معاملات التاجر.

NOTE: Any report generated by the Acquirer relating to the investigation of a Merchant whose rate of technical fallback exceeds five percent of its total Transaction volume must be made available to the National Scheme Operator upon request.

- Force-posted Transactions (i.e., a Transaction that has been declined by the Issuer or the chip or any Transaction for which authorization was required but not obtained)
- Frequency of Transactions on the same Account, including credit (refund) Transactions
- Unusual number of credits, or credit dollar volume, exceeding a level of sales dollar volume appropriate to the Merchant category
- Large credit Transaction amounts, significantly greater than the average ticket size for the Merchant's sales
- Credit (refund) Transaction volume that exceeds purchase Transaction volume
- Credits issued by a Merchant subsequent to the Acquirer's receipt of a chargeback with the same PAN
- Credits issued by a Merchant to a PAN not previously used to effect a Transaction at the Merchant location
- Increases in Merchant chargeback volume

90-day Rule

The Acquirer must compare daily deposits against the average Transaction count and amount for each Merchant over a period of at least 90 days, to lessen the effect of normal variances in a Merchant's business. For new Merchants, the Acquirer should compare the average Transaction count and amount for other Merchants within the same MCC assigned to the Merchant. In the event that suspicious credit or refund Transaction activity is identified, if appropriate, the Acquirer should consider the suspension of Transactions pending further investigation.

6.3.2.4 Acquirer Channel Management Requirements

The National Scheme Operator requires the Acquirer to monitor, on a regular basis, each parent Member ID, child Member ID, and individual Merchant in its Portfolio for the following:

- Total Transaction fraud basis points
- Domestic Transaction fraud basis points
- Cross-border Transaction fraud basis points (both Intraregional Transactions and Interregional Transactions)
- Fraud basis points at the parent Member ID/ICA level for the following:
 - Card-present Transactions
 - POS
 - Mobile POS (MPOS)
 - Cardholder-activated Terminal (CAT) (for example, CAT 1, CAT 2, and CAT 3)
 - Card-not-present (CNP) Transactions
 - E-commerce, including separate monitoring of non-authenticated, attempted authentication, and fully authenticated Transactions
 - Mail order/telephone order (MO/TO)

ملاحظة: يجب إتاحة التقرير الذي تم إصداره بواسطة جهة القبول فيما يتعلق بالتحقيق مع تاجر يتجاوز معدل التراجع الفني له خمسة بالمائة من إجمالي حجم معاملاته لمشغل شبكة الدفع المحلية عند الطلب.

- المعاملات التي تم قيدها بالاكراه (أي ، معاملة تم رفضها من قبل جهة الإصدار أو الشريحة أو أي معاملة تتطلب تفويضًا ولكن لم يتم الحصول عليه).
- تكرار المعاملات على نفس الحساب، بما في ذلك معاملات الائتمان (المستردة).
- عدد غير اعتيادي من الائتمانات، أو حجم الائتمان بالدولار، يتجاوز مستوى حجم المبيعات بالدولار المناسب لفئة التاجر
- مبالغ معاملات ائتمانية كبيرة، أكبر من متوسط حجم التذكرة لمبيعات التاجر.
- حجم معاملات الائتمان (المستردة) والذي يتجاوز حجم معاملات الشراء.
- الائتمانات الصادرة عن التاجر بعد استلام جهة القبول لرد المبالغ المدفوعة بنفس رقم الحساب الأساسي.
- الائتمانات الصادرة عن التاجر إلى رقم الحساب الأساسي، ولم تُستخدم سابقًا لإجراء معاملة في مقر التاجر.
- الزيادات في حجم رد المبالغ المدفوعة من التاجر.

قاعدة 90 يومًا

يجب على جهة القبول مقارنة الإيداعات اليومية بمتوسط عدد المعاملات، والمبلغ لكل تاجر خلال فترة لا تقل عن 90 يومًا، ولتقليل تأثير الفروق العادية في أعمال التاجر. بالنسبة للتجار الجدد، يجب على جهة القبول مقارنة متوسط عدد المعاملات والمبلغ للتجار الآخرين داخل نفس MCC المعين للتاجر. في حالة تحديد نشاط المعاملات الائتمانية أو المستردة المشبوهة، إذا كان مناسبًا، يجب على جهة القبول القيام بمزيد من التحقيق للنظر في تعليق المعاملات المنتظرة.

4.2.3.6 متطلبات إدارة قناة جهة القبول

يفرض مشغل شبكة الدفع المحلية على جهة القبول أن تراقب، بشكل منتظم، كل معرف عضو رئيسي ومعرف عضو فرعي وتاجر فردي في محفظته من أجل ما يلي:

- إجمالي النقاط الأساسية لحالات الاحتيال في المعاملات.
- النقاط الأساسية لحالات الاحتيال في المعاملات الوطنية.
- النقاط الأساسية لحالات الاحتيال في المعاملات عبر الحدود (كل من المعاملات داخل الدولة، والمعاملات الخارجية).
- النقاط الأساسية لحالات الاحتيال على مستوى معرف العضو الرئيسي / ICA لما يلي:
 - معاملات البطاقة الموجودة.
 - نقاط البيع.
 - نقاط البيع المتنقلة.
 - المحطة التي يتم تنشيطها بواسطة حامل البطاقة (على سبيل المثال، CAT 1 و CAT 2 و 3CAT).
 - معاملات البطاقة غير الموجودة.
 - التجارة الإلكترونية، بما في ذلك المراقبة المنفصلة للمعاملات غير المصدق عليها، محاولة التصديق عليها، والمعاملات المصدق عليها بالكامل.
 - الطلب عبر البريد/ الطلب عبر الهاتف.

6.3.2.5 Recommended Additional Acquirer Monitoring

The National Scheme Operator recommends that Acquirers additionally monitor the following parameters:

- Mismatch of Merchant name, MCC, Merchant ID, and/or Terminal ID
- Mismatch of e-commerce Merchant Internet Protocol (IP) addresses
- Transactions conducted at high-risk Merchants
- PAN key-entry Transactions exceeding ratio
- Abnormal hours (i.e., outside of normal business hours) or seasons
- Inactive Merchants (i.e., those Merchants that have not yet started to accept Cards as well as those that have ceased to accept Cards)
- Transactions with no approval code
- Transaction decline rate
- Inconsistent authorization and clearing data elements for the same Transactions
- 3DS 1.0 and/or EMV 3DS authentication rate
- Fraud volume per Merchant
- Any Merchant exceeding the Acquirer's total Merchant average for fraud by 150 percent or more

6.3.2.6 Recommended Fraud Detection Tool Implementation

An Acquirer is recommended to implement a fraud detection tool that appropriately complements the fraud strategy deployed by the Acquirer. The combination of the authorization requirements, Merchant deposit monitoring requirements, and fraud detection tool should ensure that an Acquirer controls fraud to an acceptable level.

For effective performance, an Acquirer's fraud detection tool should minimally measure the amount and number of fraud Transactions incurred, calculated for each of its Merchants, Payment Facilitators and other Service Providers, and deployed Terminals.

6.3.2.7 Ongoing Merchant Monitoring

An Acquirer must implement procedures for the conduct of periodic ongoing reviews of a Merchant's Card acceptance activity, for the purpose of detecting changes over time, including but not limited to:

- Monthly Transaction volume with respect to:
 - Total Transaction count and amount
 - Number of credit (refund) Transactions
 - Number of fraudulent Transactions
 - Average ticket size
 - Number of chargebacks
- Activity inconsistent with the Merchant's business model
- Transaction laundering
- Activity that is or may potentially be illegal or brand-damaging

As a best practice, an Acquirer is recommended to use a Merchant monitoring solution for e-commerce Merchant activity so as to avoid processing illegal or brand-damaging Transactions.

5.2.3.6 مراقبة جهة القبول الإضافية الموصى بها

يوصي مشغل شبكة الدفع المحلية بأن تقوم جهات القبول بالإضافة إلى ماسبق، بتطبيق المعايير التالية للمراقبة:

- عدم تطابق اسم التاجر و/ أو MCC و/أو هوية التاجر و/أو هوية المحطة.
- عدم تطابق عناوين بروتوكول إنترنت التجارة الإلكترونية للتاجر.
- عدم إجراء المعاملات لدى التاجر ذوي المخاطر العالية.
- معاملات رقم الحساب الأساسي الرئيسية التي تجاوزت النسبة.
- ساعات غير عادية (أي خارج ساعات العمل العادية) وخارج وقت ممارسة النشاط.
- التاجر غير النشطين (أي التاجر الذين لم يبدأوا بعد في قبول البطاقات بالإضافة إلى التاجر الذين توقفوا عن قبول البطاقات).
- المعاملات بدون رمز الموافقة.
- معدل رفض المعاملة.
- التفويض غير المتسق وعناصر بيانات المقاصة لنفس المعاملات.
- معدل المصادقة 3DS 1.0 و/أو EMV 3DS
- حجم حالات الاحتيال لكل تاجر.
- أي تاجر يتجاوز متوسط التاجر الإجمالي للقبول فيما يتعلق بالاحتيال بنسبة 150 بالمائة أو أكثر.

6.2.3.6 تنفيذ أداة الكشف عن حالات الاحتيال الموصى بها

يجب على جهة القبول تنفيذ أداة الكشف عن حالات الاحتيال التي تكمل بشكل مناسب استراتيجية الاحتيال التي تنشرها القبول. ويجب أن يضمن الجمع بين متطلبات التفويض، ومتطلبات مراقبة إيداع التاجر وأداة الكشف عن حالات الاحتيال، وأن تتحكم جهة القبول في حالات الاحتيال إلى مستوى مقبول.

وللحصول على أداء فعال ، يجب أن تقيس وسيلة الكشف عن حالات الاحتيال الخاصة بجهة القبول الحد الأدنى من مقدار وعدد معاملات الاحتيال التي تم تكبدها، والمحسوبة لكل من التاجر وميسري الدفع ومقدمي الخدمات الآخرين والمحطات التي تم نشرها.

7.2.3.6 المراقبة المستمرة للتاجر

يجب على جهة القبول تنفيذ الخطوات اللازمة لإجراء المراجعات الدورية المستمرة لنشاط قبول بطاقة التاجر، بغرض اكتشاف التغييرات بشكل دوري، بما في ذلك على سبيل المثال:

- حجم المعاملات الشهرية فيما يتعلق بـ:
 - إجمالي عدد و مبلغ المعاملات.
 - عدد معاملات الائتمان (المستردة).
 - عدد المعاملات الاحتيالية.
 - متوسط حجم التذكرة.
 - عدد عمليات رد المبالغ المدفوعة.
 - نشاط يتعارض مع نموذج عمل التاجر.
 - غسل المعاملات.
 - النشاط الذي قد يكون أو يحتمل أن يكون غير قانوني أو ضار بالعلامة التجارية.
- وطبقاً لأفضل الممارسات، توصي جهة القبول باستخدام نظام مراقبة التاجر، عند ممارسته للتجارة الإلكترونية، وذلك لتجنب معالجة المعاملات الغير القانونية أو الضارة بالعلامة التجارية.

6.3.3 Noncompliance with Fraud Loss Control Standards

Noncompliance with the fraud loss control Standards may require a Member to undergo a Scheme Risk Management Program onsite review. The noncompliant Member will receive a formal written report with requirements that must be satisfied within an established period to achieve compliance with the fraud loss control Standards.

Following a Scheme Risk Management Program review, a noncompliant Member will receive a written report with requirements that must be satisfied within an established period to achieve compliance with the fraud loss control Standards and minimum fraud loss control program requirements.

If a Member fails to take the required actions to achieve compliance, one or more of the following may occur:

- Noncompliance assessments, as indicated in Table 10.2.
- Revocation of the Member's License. A Member may appeal such a revocation to the National Scheme Operator. Any decision by the National Scheme Operator is final.

Table 6.2—Noncompliance Assessments with Loss Control Program Requirements
(See appendix number 44)

6.3.4 Counterfeit Card Fraud Loss Control Standards

The National Scheme Operator actively assists law enforcement in the pursuit of organized and informal criminal groups engaged in counterfeit fraud. Although the National Scheme Operator has achieved substantial success in this area, including numerous convictions of counterfeiters and seizures of their physical plants, organized criminal elements continue to expand, with new groups emerging almost daily.

In addition to implementing the fraud loss controls described in Rule 10.3, Members must also make a good-faith attempt to limit counterfeit losses. At a minimum, an Issuer is required to incorporate the required Card security features on all Cards, and an Acquirer must transmit full magnetic stripe or chip data on all Card-read POS Transactions.

6.3.4.1 Counterfeit Card Notification

All Members must notify the National Scheme Operator immediately upon suspicion or detection of counterfeit Cards.

Notification by Issuer

An Issuer must notify the National Scheme Operator immediately upon detection of a counterfeit Card bearing its BIN or, in the absence of a valid BIN, its Member ID. This step must be completed by the most prompt and practical means possible, employing such methods as email, tape transmissions, phone, or telex communication.

Notification by Acquirer

An Acquirer detecting or suspecting a counterfeit Card bearing neither a valid BIN nor a valid Member ID immediately must notify its representative and the Issuer by phone, email, or telex communication. The National Scheme Operator will add the account number to the Account Management System.

3.3.6 عدم الامتثال لمعايير التحكم في خسائر الاحتيال

قد يتطلب عدم الامتثال لمعايير مكافحة خسائر عمليات الاحتيال، أن يخضع العضو لمراجعة برنامج إدارة مخاطر النظام في الموقع. ويتلقى العضو غير الممتثل تقريرًا رسميًا مكتوبًا بالمتطلبات التي يجب الوفاء بها خلال الفترة المحددة لتحقيق الامتثال لمعايير مكافحة خسائر عمليات الاحتيال. وبعد مراجعة برنامج إدارة مخاطر النظام، سيتلقى العضو غير الممتثل تقريرًا مكتوبًا بالمتطلبات التي يجب الوفاء بها خلال الفترة المحددة لتحقيق الامتثال لمعايير مكافحة خسائر الاحتيال، وتطبيق الحد الأدنى من متطلبات برنامج مكافحة خسائر عمليات الاحتيال. وإذا أخل العضو بتطبيق الإجراءات المطلوبة لتحقيق الامتثال، فيجب إتخاذ كل، أو بعض الخطوات التالية:

- تقييمات عدم الامتثال، كما هو مبين في الجدول 10.2.
- إلغاء ترخيص العضو. ويجوز للعضو في هذه الحالة التظلم من هذا الإلغاء، أمام مشغل شبكة الدفع المحلية. يعتبر القرار الذي يتخذه مشغل شبكة الدفع المحلية عند فصله في هذا التظلم قرار نهائيًا.

الجدول 6.2 - تقييمات عدم الامتثال مع متطلبات برنامج مكافحة الخسائر
(انظر الملحق رقم 44)

4.3.6 معايير مكافحة خسائر احتيال البطاقات المزورة

يجب على مشغل شبكة الدفع المحلية التدخل بشكل فعال لمساعدة السلطات المختصة، في ملاحقة الجماعات الإجرامية المنظمة، وغير المنظمة، المرتكبة لعمليات الاحتيال. بالإضافة إلى تنفيذ ضوابط خسائر عمليات الاحتيال الموضحة في القاعدة 10.3، يجب على جميع الأعضاء الالتزام ببذل العناية الكافية للحد من خسائر عمليات التزوير. وكحد أدنى، يُطلب من جهة الإصدار دمج ميزات أمان البطاقة المطلوبة في جميع البطاقات، ويجب على جهة القبول إرسال بيانات الشريط المغناطيسي أو الشريحة بالكامل في جميع معاملات نقاط البيع التي تتم قراءتها بالبطاقة.

1.4.3.6 إشعار البطاقة المزورة

يجب على جميع الأعضاء إخطار مشغل شبكة الدفع المحلية فور اكتشاف بطاقات مزورة، أو الاشتباه في وجودها.

الإخطار من قبل جهة الإصدار

يجب على جهة الإصدار إخطار مشغل شبكة الدفع المحلية فور اكتشاف بطاقة مزورة تحمل رقم التعريف المصرفي الخاص بها، أو في حالة عدم وجود رقم تعريف مصرفي صالح، أو معرفة العضو الخاص بها. ويجب إكمال هذه الخطوة بأسرع الوسائل الممكنة، وباستخدام طرق مثل البريد الإلكتروني، أو الإرسال الشريطي، أو الهاتف، أو الاتصال بالتلكس.

الإخطار من قبل جهة القبول

يجب على جهة القبول التي يكتشف أو يشتبه في وجود بطاقة مزورة لا تحمل رقم تعريف شخصي صالح أو معرفة العضو الخاص بها، على الفور إخطار ممثل جهة الإصدار عن طريق الهاتف أو البريد الإلكتروني أو الاتصال عبر التلكس. وسيضيف مشغل شبكة الدفع المحلية رقم الحساب إلى نظام إدارة الحساب.

Failure to Give Notice

Failure by the Acquirer or Issuer to give notice within 24 hours of detecting a counterfeit Card relieves the National Scheme Operator of any responsibility for any resulting loss incurred by any party failing to give notice.

6.3.4.2 Responsibility for Counterfeit Loss

Certain losses resulting from counterfeit Transactions are the responsibility of either the Issuer or Acquirer based on the circumstances described in this section.

Loss from Internal Fraud

The National Scheme Operator is not responsible for any loss arising from or related to any fraudulent, dishonest, or otherwise wrongful act of any officer, director, or employee of a Member, or of a Member's Service Provider, agent, or representative.

Transactions Arising from Identified Counterfeit Cards

The Issuer is responsible for any counterfeit loss resulting from or related to the use of an identified counterfeit Card. An identified counterfeit Card is determined by the BIN identified in the Transaction record or, in the absence of a BIN, by the Member ID identified in the Transaction record. The Issuer is not responsible for counterfeit losses that were or could have been charged back in accordance with the Standards or for counterfeit losses that were assumed by the Acquirer as a result of a compliance case ruling.

DEFINITION:

A key-entered counterfeit Transaction occurs when the counterfeit Card is present at the POI and authorization is obtained in accordance with the Standards (but not as described for a Card-read Transaction).

DEFINITION:

An imprinted counterfeit Transaction occurs when the embossed counterfeit Card is present at the POI, the Card acceptor uses an imprinter to record the Card information, and authorization is obtained, if at all, in accordance with the Standards (but not as described for a Card-read Transaction).

DEFINITION:

A magnetic stripe-read counterfeit Transaction occurs when the counterfeit Card is present at the POI, in which authorization is affected electronically and in accordance with the Standards, with magnetic stripe data obtained from lost or stolen Card stock read by the Terminal and transmitted to the Issuer during the authorization process.

عدم القيام بالإخطار

يترتب على عدم قيام جهة القبول أو جهة الإصدار بتقديم إخطار إلى مشغل شبكة الدفع المحلية في الحالات السابقة، خلال 24 ساعة من اكتشاف البطاقة المزورة إلى إعفاء مشغل شبكة الدفع المحلية من أي مسؤولية عن الخسارة الناتجة عن عدم القيام بذلك والتي قد يتكبدها الطرف الذي أخل بالقيام بذلك.

2.4.3.6.المسؤولية عن خسارة التزوير

مسؤولية تحمل الخسائر الناتجة عن المعاملات المزورة، تقع إما على جهة الإصدار أو جهة القبول، بناءً على الظروف الموضحة في هذا القسم.

الخسارة من الاحتيال الداخلي

لا يتحمل مشغل شبكة الدفع المحلية المسؤولية عن الخسارة تنشأ عن عمل احتيالي أو غير مشروع، من جانب مسؤول أو مدير أو موظف لدى أحد الأعضاء، أو مقدم خدمة أو وكيل أو ممثل لعضو.

المعاملات الناشئة عن البطاقات المزورة المحددة

تعد جهة الإصدار مسؤولة عن الخسارة التي تنشأ عن البطاقات المزورة، متى كانت ناتجة عن استخدام بطاقة مزورة محددة. ويتم تحديد البطاقة المزورة المحددة بواسطة رقم التعريف المصرفي المحدد في سجل المعاملة، أو في حالة عدم وجود رقم تعريف مصرفي، بواسطة معرف العضو المحدد في سجل المعاملة. وجهة الإصدار غير مسؤولة عن خسائر التزوير التي تمت، أو كان من الممكن إعادة استردادها وفقًا للمعايير أو عن خسائر التزوير التي افترضها جهة القبول نتيجة لحكم حالة الامتثال.

تعريف:

تحدث المعاملة المزورة التي يتم إدخالها باستخدام مفتاح، عندما تكون البطاقة المزورة موجودة في نقطة الاهتمام، ويتم الحصول على التفويض وفقًا للمعايير (ولكن ليس كما هو موضح في المعاملة المقروءة بالبطاقة).

تعريف:

تحدث المعاملة المزورة المطبوعة، عندما تكون البطاقة المزورة المنقوشة موجودة في نقطة الاهتمام، ويستخدم قارئ البطاقة بصمة لتسجيل معلومات البطاقة، ويتم الحصول على التفويض، إن وجد، وفقًا للمعايير (ولكن ليس كما هو موضح في المعاملة المقروءة بالبطاقة).

تعريف:

تحدث المعاملة المزورة المقروءة بالشريط المغناطيسي، عندما تكون البطاقة المزورة موجودة في نقطة الاهتمام، حيث يتأثر التفويض إلكترونيًا ووفقًا للمعايير، مع بيانات الشريط المغناطيسي التي تم الحصول عليها من مخزون البطاقات المفقودة أو المسروقة التي تم قراءتها من قبل المحطة، ونقلها إلى جهة الإصدار أثناء عملية التفويض.

Transactions Arising from Unidentified Counterfeit Cards

The Acquirer is responsible for any counterfeit loss resulting from or related to the acceptance by a Merchant of a Card that cannot be identified by the BIN or Member ID imprinted in the Transaction record.

Loss or Theft of Unfinished Cards

If a counterfeit Card resulting from the loss or theft of Cards that had not yet been personalized or were otherwise unfinished is recovered, the Issuer that ordered the production of the Cards is responsible for losses arising from the use of the counterfeit Card. The Issuer is determined by the Card source identification printed on the Card back.

6.3.4.3 Acquirer Counterfeit Liability Program

The Acquirer Counterfeit Liability Program is intended to combat increases in worldwide counterfeiting in the credit card industry. The Program shifts partial counterfeit loss liability to Acquirers that exceed worldwide counterfeit Standards.

Scheme Risk Management Program staff uses the Acquirer counterfeit volume ratio to evaluate all Members' volumes of acquired counterfeit. The Acquirer counterfeit volume ratio is a Member's dollar volume of acquired counterfeit as a percentage of the total dollar volume acquired by that Member.

Scheme Risk Management Program staff monitors the 20 Members with the highest Acquirer counterfeit volume ratio on a quarterly basis. The National Scheme Operator notifies each Member with liability of its own Acquirer counterfeit volume ratio, the worldwide average, the reported counterfeit, and the amount of Member liability calculated on a quarterly basis.

The National Scheme Operator uses funds obtained from Acquirers that exceed established annual thresholds to provide the following support:

- Recover the costs associated with the administration of this Program,
- Fund the development of new fraud control programs, and
- Supplement the National Scheme Operator liability limit for the reimbursement of Issuers' counterfeit losses.

Acquirer Counterfeit Liability

An Acquirer is liable for any counterfeit volume that is above a threshold of 10 times the worldwide Acquirer counterfeit volume ratio.

Scheme Risk Management Program review teams will provide a report to Acquirers whose Acquirer counterfeit volume ratio exceeds 10 times the worldwide average with recommendations on how to reduce the volume of acquired counterfeit Transactions. If an Acquirer implements all of the programs recommended by Scheme Risk Management Program staff, or takes necessary action to curb counterfeit, the National Scheme Operator will review the actions taken and may adjust the cumulative liability that would otherwise be imposed by the Program.

Counterfeit experience inconsistent with the implementation of the required programs will result in further Member Scheme Reviews by the National Scheme Operator.

المعاملات الناشئة عن بطاقات مزورة مجهولة الهوية

جهة القبول مسؤولة عن خسارة البطاقة المزورة الناتجة عن قبول التاجر للبطاقة، والتي لا يمكن تحديدها بواسطة رقم التعريف المصرفي أو معرف العضو المطبوع في سجل المعاملة.

فقدان أو سرقة البطاقات غير المكتملة

إذا تم استرداد البطاقة المزورة الناتجة عن فقدان أو سرقة البطاقات التي لم يتم تخصيصها بعد، و لم يتم الانتهاء منها، فإن جهة الإصدار التي أمرت بإنتاج البطاقات تكون مسؤولة عن الخسائر الناتجة عن استخدام البطاقة المزورة. ويتم تحديد جهة الإصدار من خلال تحديد مصدر البطاقة المطبوع على ظهر البطاقة.

3.4.3.6 برنامج مسؤولية جهة القبول عن التزوير

يهدف برنامج مسؤولية جهة القبول عن تزوير البطاقات، إلى مكافحة عمليات التزوير في جميع أنحاء العالم في صناعة بطاقات الائتمان. ينقل البرنامج مسؤولية التزوير الجزئية إلى القابلين الذين يتجاوزون معايير التزوير العالمية.

ويستخدم موظفو برنامج إدارة مخاطر النظام، نسبة عمليات التزوير، لتقييم جميع أحجام الأعضاء من التزوير القابل. ونسبة عمليات تزوير جهة القبول: هي بحجم الدولار للعضو من التزوير القابل كنسبة مئوية من إجمالي حجم الدولار الذي حصل عليه هذا العضو.

يقوم موظفو برنامج إدارة مخاطر النظام، بمراقبة الأعضاء العشرين الذين لديهم أعلى نسبة عمليات تزوير للقابل على أساس ربع سنوي. ويقوم مشغل شبكة الدفع المحلية بإخطار كل عضو بمسؤوليته عن نسبة عمليات التزوير الخاص به، والمتوسط العالمي، والتزوير المبلغ عنه، ومبلغ مسؤولية الأعضاء المحسوبة على أساس ربع سنوي.

لمشغل شبكة الدفع المحلية استخدام الأموال التي تم الحصول عليها من جهات القبول، والتي تتجاوز الحدود السنوية المحددة، لتقديم الدعم التالي:

- استرداد التكاليف المرتبطة بإدارة هذا البرنامج.
- تمويل تطوير برامج جديدة لمكافحة عمليات الاحتيال.
- تغطية مسؤولية مشغل شبكة الدفع المحلية للتعويض عن خسائر التزوير الخاصة بجهات الإصدار.

مسؤولية جهة القبول عن التزوير

القابل مسؤول عن عملية التزوير الذي يتجاوز حد 10 أضعاف نسبة عمليات التزوير في جميع أنحاء العالم.

وتقدم فرق مراجعة برنامج إدارة مخاطر النظام، تقريرًا إلى جهات القبول التي تتجاوز نسبة عمليات التزوير القابل الخاصة بهم 10 أضعاف المتوسط العالمي، مع توصيات حول كيفية تقليل حجم المعاملات المزورة القابلة. وإذا نفذ جهة القبول جميع البرامج التي أوصى بها موظفو برنامج إدارة مخاطر النظام، أو اتخذ الإجراءات اللازمة للحد من التزوير، ولمشغل شبكة الدفع المحلية مراجعة الإجراءات المتخذة، وله تعديل أحكام المسؤولية التي قد يفرضها البرنامج، بخلاف ذلك.

ستؤدي تجربة التزوير غير المتسقة مع تنفيذ البرامج المطلوبة، إلى المزيد من مراجعات نظام الأعضاء بواسطة مشغل شبكة الدفع المحلية.

Acquirer Liability Period

The Acquirer's counterfeit volume ratio liability is computed for the period from 1 January through 31 December. Acquirer counterfeit volume ratio liability is determined after final submission of counterfeit reimbursement claims for each 12-month cycle.

Relief from Liability

To qualify for relief from liability, an Acquirer must meet the following criteria:

1. The Acquirer must comply with the Acquirer loss control program Standards described in Rule 10.3.2.
2. The Acquirer must issue internal procedures designating responsibilities for monitoring the exception reports, explaining how they should be used, and defining actions to be taken when thresholds are exceeded. Members will need to maintain internal records that clearly demonstrate supervisory review of such procedures and the periodic review of results by senior management.
3. The Acquirer must transmit the full, unedited International Organization for Standardization (ISO) 8583 (Financial transaction card originated messages—Interchange message specifications) authorization message from Terminal-read Transactions to the system.
4. The Acquirer that is subject to liability may be required by the National Scheme Operator to take additional action to attempt further to reduce its level of counterfeit losses.

The National Scheme Operator will provide relief from reversal of responsibility to Acquirers that exceed the threshold under the Acquirer Counterfeit Liability Program and that fully meet the aforementioned criteria.

NOTE: Acquirers must submit a written application for relief in order for the National Scheme Operator to provide relief from responsibility.

Application for Relief

An Acquirer must submit the written application for relief under signature of an appropriate officer, such as the Card center manager of that Member. The following information must be included in the application:

- Certification that the requisite controls are in place
- A detailed description of the controls
- The specific parameters being used
- A copy of the procedures document described in the "Relief from Liability" section
- Sample copies of the automated exception reports

The effective date of the provisions of relief will be no sooner than 90 days after the Acquirer has fully implemented the requisite controls. Release from responsibility for the Acquirer will not be granted until all of the requirements are in place for at least 90 days. Continued eligibility for relief will be subject to periodic review by Scheme Risk Management Program staff, and may be revoked at any time.

6.4 Information Security Program—Personal Data

As used in this Rule, "Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity.

مدة مسؤولية جهة القبول

يتم احتساب مسؤولية نسبة عملية تزوير جهة القبول: للفترة من 1 يناير حتى 31 ديسمبر. ويتم تحديد مسؤولية نسبة عملية تزوير جهة القبول بعد التقديم النهائي لمطالبات السداد المزورة لكل دورة مدتها 12 شهرًا.

الإعفاء من المسؤولية

لكي تطبق قواعد الإعفاء من المسؤولية، يجب على جهة القبول، استيفاء المعايير التالية:

1. يجب أن تلتزم جهة القبول بمعايير برنامج مكافحة خسارة جهة القبول الموضحة في القاعدة 10.3.2.
2. يجب أن تصدر جهة القبول إجراءات داخلية تحدد المسؤوليات لمراقبة تقارير الاستثناءات، وشرح كيفية استخدامها، وتحديد الإجراءات التي يجب اتخاذها عند تجاوز الحدود. سيحتاج الأعضاء إلى الاحتفاظ بسجلات داخلية، تبين بوضوح المراجعة الإشرافية لهذه الإجراءات والمراجعة الدورية للنتائج من قبل الإدارة العليا.
3. يجب على جهة القبول إرسال رسالة التفويض الكاملة غير المحررة للمنظمة الدولية للتوحيد القياسي 8583 (الرسائل الصادرة عن بطاقة المعاملات المالية - مواصفات رسالة التبادل) من المعاملات المقررة بالمحطة إلى النظام.
4. قد يطلب مشغل شبكة الدفع المحلية من جهة القبول التي تخضع للمسؤولية اتخاذ إجراءات إضافية لمحاولة تقليل مستوى خسائر التزوير.

ولمشغل شبكة الدفع المحلية أن يمنح إعفاءً من عكس المسؤولية إلى جهات القبول الذين يتجاوزون الحد بموجب برنامج مسؤولية القابل عن التزوير والذي يستوفي تمامًا المعايير المذكورة أعلاه. ملاحظة: يجب أن تقدم جهات القبول طلبًا مكتوبًا للإعفاء حتى يتمكن مشغل شبكة الدفع المحلية من تقديم الإعفاء من المسؤولية.

طلب الإعفاء

يجب على جهة القبول تقديم طلب مكتوب للإعفاء من المسؤولية، موقع من المسؤول المختص، مثل مدير مركز البطاقات لهذا العضو. يجب تضمين المعلومات التالية في الطلب:

- شهادة بأن الضوابط اللازمة قد طبقت.
- وصف مفصل للضوابط.
- الضوابط المحددة المستخدمة.
- نسخة من وثيقة الإجراءات الموضحة في قسم "الإعفاء من المسؤولية".
- نسخ نموذجية من تقارير الاستثناءات الآلية.

التاريخ الفعلي لأحكام الإعفاء يجب أن لا يقل عن 90 يومًا من تنفيذ جهة القبول لجميع الضوابط اللازمة للإعفاء. ولن يتم منح الإعفاء من المسؤولية لجهة القبول، حتى تقوم بتطبيق جميع المتطلبات لمدة 90 يومًا على الأقل، سابقة لمنح الإعفاء. ويخضع برنامج الاستمرار في الإعفاء من المسؤولية لمراجعة دورية من قبل موظفي برنامج إدارة مخاطر النظام، وقد يتم إلغاؤها في أي وقت.

4.6 برنامج أمن المعلومات - البيانات الشخصية

طبقاً لهذه القاعدة، تعني "البيانات الشخصية" أي معلومات تتعلق بشخص طبيعي محدد، أو يمكن تحديد هويته. والشخص الطبيعي يمكن تحديد هويته بشكل مباشر أو غير مباشر، ويتم ذلك على وجه الخصوص بالرجوع إلى رقم التعريف أو إلى عامل أو أكثر خاص بهويته الجسدية أو الفسيولوجية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية.

A Member must maintain a comprehensive written information security program that includes technical, physical, administrative, and organizational safeguards designed to:

1. Ensure the security and confidentiality of Personal Data;
2. Protect against any anticipated threats or hazards to the security, confidentiality, and integrity of Personal Data;
3. Protect against any actual or suspected unauthorized processing, loss, or unauthorized acquisition of any Personal Data; and
4. Ensure the proper and secure disposal of Personal Data.

6.4.1 Protection of Personal Data

A Member's information security program must regularly test or monitor the effectiveness of the safeguards stated in this Rule.

For purposes of this Rule, the following terms have the meanings set forth below.

Applicable Data Protection Law

The applicable laws, rules, regulations, directives and governmental requirements in Libya relating in any way to the privacy, protection and security of Personal Data, as amended from time to time.

Data Subject

A Cardholder, Account Holder, or Merchant or other natural person whose Personal Data is collected, used or disclosed by the National Scheme Operator or a Member in Libya.

Organization

Any individual, company, association or body of persons, corporate or unincorporated, whether or not formed or recognized under the applicable law of Libya, or resident, or having an office or a place of business, in Libya.

Personal Data

Any information or opinion, whether true or not, about an identified individual or an individual who can be identified or is reasonably identifiable from that information or opinion.

Processing of Personal Data

The carrying out of any operation or set of operations in relation to Personal Data, including recording, holding, organization, adaptation or alteration, retrieval, combination, transmission and erasure or destruction.

Transaction-related Personal Data

Personal Data required for authorizing, recording, settling, and clearing a Transaction processed by the National Scheme Operator.

6.4.1.1 Processing of Transaction-related Personal Data

A Member who collects, uses, or discloses Transaction-related Personal Data in Libya must comply with the Applicable Data Protection Law in that country. A Member is the Organization responsible for complying with the Applicable Data Protection Law in respect of the collection, use and disclosure of Personal Data, including the transfer of Personal Data outside Libya, for the purposes of authorizing, recording, clearing and settling

و يجب أن يحتفظ العضو ببرنامح شامل مكتوب لأمن المعلومات، يتضمن الضمانات الفنية والمادية والإدارية والتنظيمية المعدة من أجل:

1. ضمان أمن وسرية البيانات الشخصية.
2. الحماية من تهديدات أو مخاطر متوقعة على أمن وسرية وسلامة البيانات الشخصية.
3. الحماية من معالجة فعلية أو مشتبه بها وغير مصرح بها، أو خسارة أو حيازة غير المصرح بها لبيانات شخصية.
4. ضمان التخلص السليم، والآمن من البيانات الشخصية.

1.4.6. حماية البيانات الشخصية

يجب أن يقوم برنامج أمن المعلومات للعضو باختبار أو مراقبة فاعلية الضمانات المنصوص عليها في هذه القاعدة بشكل منتظم.

لأغراض تطبيق هذه القاعدة ، تحمل المصطلحات التالية المعاني الموضحة أدناه.

قانون حماية البيانات المعمول به

القوانين واللوائح والقرارات الحكومية المعمول بها في دولة ليبيا، والمتعلقة بأي شكل من الأشكال بحماية، وأمن خصوصية البيانات الشخصية.

صاحب البيانات

هو حامل البطاقة أو صاحب الحساب أو التاجر أو أي شخص طبيعي آخر، ويتم جمع بياناته الشخصية أو استخدامها أو الكشف عنها بواسطة مشغل شبكة الدفع المحلية أو أحد الأعضاء في دولة ليبيا. منظمة

هي أي شخص طبيعي أو اعتباري، سواء تم تشكيلها أو الاعتراف بها بموجب القانون الليبي المعمول به أو القانون الأجنبي، أو مقيماً، أو له مقر، أو لديه مكتب أو مكان عمل، في دولة ليبيا.

بيانات شخصية

هي أي معلومات، سواء كانت صحيحة أم لا، حول شخص محدد أو شخص يمكن تحديد هويته، أو يمكن التعرف على هويته بشكل معقول من تلك المعلومات.

معالجة البيانات الشخصية

هي تنفيذ عملية أو مجموعة من العمليات المتعلقة بالبيانات الشخصية، بما في ذلك التسجيل، والاحتفاظ، والتنظيم، والتكيف أو التغيير، والاسترجاع، والجمع، والنقل، والمسح أو الإزالة.

البيانات الشخصية المتعلقة بالمعاملات

هي البيانات الشخصية المطلوبة لتفويض المعاملة التي تتم معالجتها بواسطة مشغل شبكة الدفع المحلية، وتسجيلها، وتسويتها، وتصفياتها.

1.1.4.6. معالجة البيانات الشخصية المتعلقة بالمعاملات

يجب على العضو الذي يجمع البيانات الشخصية المتعلقة بالمعاملات في دولة ليبيا، أو يستخدمها أو يفصح عنها الامتثال لقوانين حماية البيانات المعمول في دولة ليبيا. ويعد العضو هو المؤسسة المسؤولة عن الامتثال لهذه القوانين فيما يتعلق بجمع البيانات الشخصية واستخدامها والإفصاح عنها، بما في ذلك نقل البيانات الشخصية خارج دولة ليبيا، لأغراض تفويض وتسجيل وتصفية وتسوية

transactions, and the National Scheme Operator acts as an entity that processes Personal Data on behalf of the Member for these purposes. The National Scheme Operator will only undertake Processing of Personal Data in accordance with the Member's instructions and the Standards and will comply with security obligations equivalent to those imposed on the Members under the Applicable Data Protection Law, and such other obligations as applicable to the National Scheme Operator under the Applicable Data Protection Law.

6.4.1.2 Data Subject Notice and Consent

A Member in Libya must ensure that Data Subjects are properly informed and, if necessary, have given proper consent in accordance with the Applicable Data Protection Law that Personal Data relating to them may be collected, used or disclosed by the applicable Member and the National Scheme Operator as set forth for the purposes provided for in the Confidential Information of Members Rule.

6.4.1.3 Data Subject Access to Personal Data

In accordance with the Applicable Data Protection Law, a Member in Libya must develop and implement appropriate procedures for handling requests by Data Subjects for access to and/or correction of Personal Data maintained by the applicable Member or the National Scheme Operator. The National Scheme Operator will cooperate with a Member in responding to such requests and will provide access to Personal Data maintained by the National Scheme Operator where appropriate.

If an access request is made directly to the National Scheme Operator, a Member must cooperate with the National Scheme Operator in promptly responding to the request.

6.4.1.4 Integrity of Personal Data

Each Member in Libya must take reasonable steps to ensure that Personal Data the Member provides to the National Scheme Operator is accurate, complete and current.

6.5 Information Security Program—Confidential Information and Account Data

Each Member and any agent thereof is expected to establish and maintain meaningful controls for any environment, system or device used to store or process Confidential Information or Account Data, whether temporarily or permanently and whether directly or indirectly.

For purposes of this Rule:

- “Confidential Information” means any information of any nature resulting from Activity, Digital Activity, or any service provided by or product of the National Scheme Operator and which information is deemed by a person other than the National Scheme Operator (including, by way of example and not limitation, a Member or Merchant or Cardholder) to be confidential information of such person; and
- “Account Data” means any Cardholder Data and/or Sensitive Authentication Data, where these terms have the meanings set forth in the Payment Card Industry (PCI) Data Security Standard and in this section, and include, by way of example and not limitation:
 - Cardholder Data—The Cardholder name, primary account number (PAN) and expiration date associated with an Account (including any Token or Virtual

المعاملات، و يعمل مشغل شبكة الدفع المحلية ككيان يقوم بمعالجة البيانات الشخصية نيابة عن العضو لهذه الأغراض. ويتولى مشغل شبكة الدفع المحلية فقط معالجة البيانات الشخصية وفقاً لتعليمات العضو والمعايير، ويمثل للالتزامات الأمنية المفروضة على الأعضاء بموجب قانون حماية البيانات المعمول به، والتي تنطبق على مشغل شبكة الدفع المحلية بموجب قانون حماية البيانات المعمول به.

2.1.4.6 إخطار وموافقة صاحب البيانات

يجب على العضو الذي يمارس نشاطه في ليبيا التحقق من أن أصحاب البيانات قد تم إخطارهم بشكل صحيح، وأنهم قد أعطوا الموافقة في الشكل المناسب طبقاً لقوانين حماية البيانات المعمول به، على أنه يمكن جمع البيانات الشخصية المتعلقة بهم أو استخدامها أو الإفصاح عنها من قبل العضو المعني ومشغل شبكة الدفع المحلية على النحو المبين للأغراض المنصوص عليها في قاعدة المعلومات السرية للأعضاء.

3.1.4.6 وصول صاحب البيانات إلى البيانات الشخصية

وفقاً لقانون حماية البيانات المعمول به ، يجب على العضو في ليبيا تطوير وتنفيذ الإجراءات المناسبة للتعامل مع طلبات أصحاب البيانات للوصول إلى و/أو تصحيح البيانات الشخصية التي يحتفظ بها العضو المعني أو مشغل شبكة الدفع المحلية. ويلتزم مشغل شبكة الدفع المحلية بالتعاون مع أحد الأعضاء في الاستجابة لمثل هذه الطلبات، وسيوفر الوصول إلى البيانات الشخصية التي يحتفظ بها مشغل شبكة الدفع المحلية عند الاقتضاء.

إذا تم تقديم طلب وصول مباشرة إلى مشغل شبكة الدفع المحلية، يجب على العضو التعاون مع مشغل شبكة الدفع المحلية في الاستجابة السريعة لهذا الطلب.

4.1.4.6 سلامة البيانات الشخصية

يجب على كل عضو في ليبيا اتخاذ الخطوات المعقولة للتحقق من أن البيانات الشخصية التي يقدمها العضو لمشغل شبكة الدفع المحلية دقيقة وصحيحة وكاملة وحديثة.

5.6 برنامج أمن المعلومات - المعلومات السرية وبيانات الحساب

يتوقع من كل عضو ووكيله، إنشاء ضوابط ذات فاعلية لأي بيئة أو نظام أو جهاز مستخدم لتخزين أو معالجة المعلومات السرية أو بيانات الحساب، سواء بشكل مؤقت أو دائم وسواء بشكل مباشر أو غير مباشر.

لأغراض تطبيق هذه القاعدة يقصد بالمصطلحات التالية المعاني الموضحة أمامها:

- “المعلومات السرية” هي أي معلومات من أي نوع ناتجة عن نشاط أو نشاط رقمي أو أي خدمة مقدمة أو منتج من مشغل شبكة الدفع المحلية، وأي معلومات يعتبرها شخص آخر غير مشغل شبكة الدفع المحلية (بما في ذلك، على سبيل المثال، العضو أو التاجر أو حامل البطاقة) معلومات سرية لهذا الشخص.
- “بيانات الحساب” هي أي بيانات لحامل البطاقة، أو بيانات مصادقة حساسة، حيث يكون لهذه المصطلحات المعاني الموضحة في معيار أمان بيانات صناعة بطاقات الدفع وفي هذا القسم، وتشمل، على سبيل المثال:
 - بيانات حامل البطاقة - اسم حامل البطاقة ورقم الحساب الأساسي وتاريخ انتهاء الصلاحية المرتبط بالحساب (بما في ذلك أي رمز أو حساب افتراضي)، ورمز الخدمة على بطاقة الشريط المغناطيسي

- Account), the service code on a magnetic stripe Card, and any Payment Account Reference (PAR) value; and
- Sensitive Authentication Data—The full contents of a Card’s magnetic stripe or the equivalent on a chip, Card validation code 2 (CVV 2) data, and PIN or PIN block data.

Cybersecurity Minimum Requirement

Each Member must ensure that any Member environment that stores, processes, or transmits Account Data complies with the PCI Data Security Standard, in accordance with the Site Data Protection Program, and all other applicable PCI Security Standards (as listed in Table 10.3) and cybersecurity programs described in this Rule.

Cybersecurity Best Practice

As a best practice to ensure sufficient cybersecurity controls are established and maintained, all Member environments, systems or devices used to store, process or transmit Confidential Information are recommended to comply with at least one of the following:

- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF); or
- One of the standards included as “Informative References” to the NIST CSF, currently:
 - Control Objectives for Information and Related Technology (COBIT)
 - CIS Critical Security Controls for Effective Cyber Defense (CIS Controls)
 - American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009
 - ISO/IEC 27001
 - NIST SP 800-53 Rev. 4 – NIST Special Publication 800-53

(See appendix number 45)

6.5.1 Payment Card Industry (PCI) Security Standards

PCI Security Standards are technical and operational requirements established by the Payment Card Industry Security Standards Council (PCI SSC) to act as a minimum baseline to protect Account data. The National Scheme Operator requires that all Members, Merchants, Service Providers, and other Member agents that store, process, or transmit Card, Cardholder, or Transaction data adhere to the most current PCI Security Standards.

The following table describes the PCI Security Standards and compliance requirements applicable to Issuers, Acquirers, Merchants, Service Providers, Card production vendors, and other Member agents. All of the PCI Security Standards documents referenced in this table are available on the PCI SSC website at www.pcisecuritystandards.org.

Table 6.3—PCI Security Standard Documentation and Compliance Requirements
(See appendix number 46)

- وأي قيمة مرجعية لحساب الدفع.
- بيانات المصادقة الحساسة - المحتويات الكاملة للشريط المغناطيسي للبطاقة أو ما يعادله على شريحة، وبيانات رمز التحقق من البطاقة 2 (CVV 2)، ورقم التعريف الشخصي أو بيانات حظر رقم التعريف الشخصي.

الحد الأدنى لمتطلبات الأمن السيبراني

يجب على كل عضو التحقق من أن أي بيئة عضو تقوم بتخزين بيانات الحساب أو معالجتها أو نقلها تتوافق مع معيار أمان بيانات صناعة بطاقات الدفع، وفقاً لبرنامج حماية بيانات الموقع، وجميع معايير أمان صناعة بطاقات الدفع المعمول بها (على النحو الوارد في الجدول 10.3) وبرامج الأمن السيبراني الموضحة في هذه القاعدة.

أفضل ممارسات الأمن السيبراني

- طبقاً لأفضل ممارسة لضمان وضع ضوابط كافية للأمن السيبراني وصيانتها، يوصى بجميع بيئات الأعضاء أو الأنظمة أو الأجهزة المستخدمة لتخزين المعلومات السرية أو معالجتها أو نقلها للامتثال لواحد على الأقل مما يلي:
- المعهد الوطني للمعايير والتكنولوجيا إطار الأمن السيبراني .
 - أحد المعايير المدرجة باسم “المراجع الإعلامية” إلى المعهد الوطني للمعايير والتكنولوجيا إطار الأمن السيبراني ، حالياً:
 - أهداف الرقابة للمعلومات والتقنيات ذات الصلة.
 - ضوابط أمان CIS الحرجة للدفاع السيبراني الفعال (ضوابط CIS).
 - المعهد الوطني الأمريكي للمعايير/ الجمعية الدولية للأتمتة ((99.02.01)-62443-2-1 (ANSI / ISA -2009
 - ISO / IEC 27001
 - NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53

(انظر الملحق رقم 45)

1.5.6. معايير الأمان الخاصة بصناعة بطاقات الدفع

معايير أمان صناعة بطاقات الدفع هي متطلبات فنية وتشغيلية وضعها مجلس معايير أمان صناعة بطاقات الدفع، لتمثل الأساس الأدنى لحماية بيانات الحساب، ويوجب مشغل شبكة الدفع المحلية أن يلتزم جميع الأعضاء والتجار ومقدمي الخدمات والوكلاء الأعضاء الآخرين الذين يقومون بتخزين أو معالجة أو نقل بيانات البطاقة أو حامل البطاقة أو المعاملة بتطبيق أحدث معايير أمان صناعة بطاقات الدفع.

يصف الجدول التالي معايير أمان صناعة بطاقات الدفع ومتطلبات الامتثال المطبقة على جهات الإصدار وجهات القبول والتجار ومقدمي الخدمات وبائعي إنتاج البطاقات والوكلاء الأعضاء الآخرين. تتوفر جميع مستندات معايير أمان صناعة بطاقات الدفع المشار إليها في هذا الجدول على موقع مجلس معايير أمان صناعة بطاقات الدفع على www.pcisecuritystandards.org .

الجدول 6.3 - متطلبات الامتثال والتوثيق القياسي لأمن صناعة بطاقات الدفع
(انظر الملحق رقم 46)

6.5.2 Cybersecurity Incentive Program

The Cybersecurity Incentive Program (CSIP) provides eligible Merchants using secure technologies such as EMV chip and point-to-point encryption (P2PE) technology increased flexibility within the SDP Standards. The CSIP is a component of the SDP Program and is optional for Merchants. The CSIP incentivizes Merchant participation by either reducing PCI compliance validation requirements or by eliminating the requirement to annually validate compliance with the PCI DSS.

PCI DSS Risk-based Approach

A qualifying Level 1 or Level 2 Merchant is permitted to use the PCI DSS Risk-based Approach, which reduces a Merchant's compliance requirements to validating compliance with the first two of the six total milestones set forth in the PCI DSS Prioritized Approach, as follows:

- A Level 1 Merchant must validate compliance through an onsite assessment conducted by a PCI SSC-approved QSA or PCI SSC-certified ISA;
- A Level 2 Merchant must validate compliance through an onsite assessment or self-assessment conducted by a PCI SSC-approved QSA or PCI SSC-certified ISA; and
- Each Level 1 and Level 2 Merchant must annually revalidate compliance with milestones one and two using a Self-Assessment Questionnaire (SAQ) completed by a PCI SSC-approved QSA or PCI SSC-certified ISA.

To qualify as compliant with the PCI DSS Risk-based Approach, a Merchant must satisfy all of the following:

- The Merchant must certify that it is not storing Sensitive Authentication Data.
- On a continuous basis, the Merchant must keep fully segregated the “Card-not-present” Transaction environment from the “face-to-face” Transaction environment. A face-to-face Transaction requires the Card, the Cardholder, and the Merchant to all be present together at the time and place of the Transaction.
- At least 75 percent of the Merchant's annual total count of Card-present Transactions must occur at Hybrid POS Terminals.
- The Merchant must not have experienced an Account Data Compromise Event within the last twelve (12) months. At the discretion of the National Scheme Operator, this and other criteria may be waived if the Merchant validated full PCI DSS compliance at the time of the Account Data Compromise Event or Potential Account Data Compromise Event.
- The Merchant must establish and annually test an Account Data Compromise Event incident response plan.

Information about the PCI DSS Prioritized Approach is available at:

www.pcisecuritystandards.org/education/prioritized.shtml

PCI DSS Compliance Validation Exemption Program

A qualifying Level 1, Level 2, or Level 4 Merchant may participate in the PCI DSS Compliance Validation Exemption Program (the “Exemption Program”), which exempts the Merchant from annually validating its compliance with the PCI DSS.

To qualify or remain qualified to participate in the Exemption Program, a duly authorized and empowered officer of the Merchant must certify to the Merchant's Acquirer in writing that the Merchant has satisfied all of the following:

2.5.6. برنامج حوافز الأمن السيبراني

يوفر برنامج حوافز الأمن السيبراني للتجار المؤهلين الذين يستخدمون تقنيات آمنة مثل شريحة EMV، وتقنية التشفير من نقطة إلى نقطة مرونة متزايدة ضمن معايير SDP. ويعد CSIP أحد مكونات برنامج SDP وهو تطبيق اختياري للتجار. يحفز CSIP مشاركة التاجر إما عن طريق تقليل متطلبات التحقق من توافق PCI أو عن طريق إلغاء شرط التحقق سنوياً من الامتثال لـ PCI DSS.

نهج PCI DSS القائم على المخاطر

يُسمح للتاجر المؤهل من المستوى 1 أو المستوى 2 باستخدام نهج PCI DSS القائم على المخاطر، والذي يقلل من متطلبات امتثال التاجر للتحقق من الامتثال للمرحلة الأولى والثانية، من إجمالي ستة مراحل منصوص عليها في خطة أولوية PCI DSS، على النحو التالي:

- يجب على التاجر من المستوى 1 التحقق من الامتثال من خلال تقييم في الموقع يتم إجراؤه بواسطة QSA المعتمد من PCI SSC أو ISA المعتمد من PCI SSC.
- يجب على التاجر من المستوى 2 التحقق سنوياً من الامتثال من خلال تقييم في الموقع أو تقييم ذاتي يتم إجراؤه بواسطة QSA المعتمد من PCI SSC أو ISA المعتمد من PCI SSC.
- يجب على كل تاجر من المستوى 1 والمستوى 2 إعادة التحقق سنوياً من الامتثال للمراحل الرئيسية الأولى والثانية باستخدام استبيان التقييم الذاتي الذي تم إكماله بواسطة PCI SSC المعتمد من QSA أو PCI SSC المعتمد من ISA.

للتأهل للامتثال لخطة PCI DSS القائم على المخاطر، يجب على التاجر تلبية جميع ما يلي:

- يجب أن يتعهد التاجر أنه لا يقوم بتخزين بيانات المصادقة الحساسة.
- يجب على التاجر بصفة مستمرة الاحتفاظ ببيئة معاملات “البطاقة غير الموجودة” منفصلة تمامًا عن بيئة معاملات “وجهًا لوجه”. تتطلب معاملة وجهًا لوجه أن تكون البطاقة وحامل البطاقة والتاجر حاضرين معًا في وقت ومكان المعاملة.
- يجب أن يحدث 75 بالمائة على الأقل من إجمالي العدد السنوي للتاجر لمعاملات البطاقة الموجودة في محطات نقاط البيع الهجينة.
- يجب ألا يكون التاجر قد واجه حدث اختراق في بيانات الحساب خلال الاثني عشر (12) شهرًا الماضية. ووفقًا للسلطة التقديرية لمشغل شبكة الدفع المحلية، فإنه قد يتم التنازل عن هذه المعايير وغيرها إذا قام التاجر بالتحقق من امتثال PCI DSS الكامل في وقت حدث اختراق بيانات الحساب أو حدث اختراق بيانات الحساب المحتمل.
- يجب على التاجر إنشاء واختبار خطة الاستجابة لحدث اختراق في بيانات الحساب سنوياً.

تتوفر معلومات حول نهج أولوية PCI DSS على:

www.pcisecuritystandards.org/education/prioritized.shtml

برنامج الإعفاء من التحاقق من امتثال PCI DSS

يجوز للتاجر المؤهل من المستوى 1 أو المستوى 2 أو المستوى 4 المشاركة في برنامج الإعفاء من التحقق من الامتثال لـ PCI DSS (“برنامج الإعفاء”)، والذي يعفي التاجر من التحقق سنوياً من امتثاله لـ PCI DSS.

يشترط للتأهل أو البقاء مؤهلاً للمشاركة في برنامج الإعفاء، أن يقدم مسؤول التاجر المفوض والمخول بذلك لجهة القبول للتاجر تقرير كتابياً يفيد بأن التاجر قد استوفى كل ما يلي:

1. The Merchant validated its compliance with the PCI DSS within the previous twelve (12) months or, alternatively, has submitted to its Acquirer, and the Acquirer has submitted to the National Scheme Operator, a defined remediation plan satisfactory to the National Scheme Operator designed to ensure that the Merchant achieves PCI DSS compliance based on a PCI DSS gap analysis;
2. The Merchant does not store Sensitive Authentication Data. The Acquirer must notify the National Scheme Operator through compliance validation reporting of the status of Merchant storage of Sensitive Card Authentication Data;
3. The Merchant has not been identified by the National Scheme Operator as having experienced an Account Data Compromise Event during the prior twelve (12) months;
4. The Merchant has established and annually tests an Account Data Compromise Event incident response plan in accordance with PCI DSS requirements; and
5. The Merchant has satisfied either of the following:
 - a. At least 75 percent of the Merchant's annual total acquired Transaction count is processed through Hybrid POS Terminals, as determined based on the Merchant's transactions processed during the previous twelve (12) months through the Interchange System. The National Scheme Operator will include Transactions that were not processed through the Interchange System in the annual acquired Transaction count only if the data is readily available to the National Scheme Operator; OR
 - b. The Merchant has implemented a point-to-point encryption (P2PE) solution listed on the PCI SSC website.

An Acquirer must retain all Merchant certifications of eligibility for the Exemption Program for a minimum of five (5) years. Upon request by the National Scheme Operator, the Acquirer must provide a Merchant's certification of eligibility for the Exemption Program and any documentation and/or other information applicable to such certification. An Acquirer is responsible for ensuring that each Exemption Program certification is truthful and accurate. A Merchant that does not satisfy the Exemption Program's eligibility criteria, including any Merchant whose Transaction volume is primarily from e-commerce and Mail Order/Telephone Order (MO/TO) acceptance channels, must continue to validate its PCI DSS compliance.

All Merchants must maintain ongoing compliance with the PCI DSS regardless of whether annual compliance validation is a requirement.

6.5.2.1 Site Data Protection Noncompliance Assessments

The National Scheme Operator has the right to audit Member compliance with the Site of Data requirements. Noncompliance on or after the required implementation date may result in assessments described in Table 6.4.

Table 6.4—Assessments for Noncompliance
(See appendix number 47)

Noncompliance also may result in Merchant termination; deregistration of a TPP, DSE, PF, SDWO, DASP, TSP, TS, or 3-DSSP as a Service Provider; or termination of the Issuer or Acquirer as a Member.

1. قام التاجر بالتحقق من امتثاله لـ PCI DSS خلال الاثني عشر (12) شهرًا السابقة، أو بدلًا من ذلك، قدم إلى جهة القبول، وقدمت جهة القبول إلى مشغل شبكة الدفع المحلية، خطة علاج محددة يقبلها مشغل شبكة الدفع المحلية الذي يوجب التحقق من أن التاجر يحقق امتثال PCI DSS بناءً على تحليل فجوة PCI DSS.
2. أن التاجر لا يقوم بتخزين بيانات المصادقة الحساسة. ويجب على جهة القبول إخطار مشغل شبكة الدفع المحلية من خلال تقارير التحقق من الامتثال بحالة تخزين التاجر لبيانات مصادقة البطاقة الحساسة.
3. أن لا يكون التاجر قد تم تحديده من قبل مشغل شبكة الدفع المحلية على أنه تعرض لحدث اختراق في بيانات الحساب خلال الاثني عشر (12) شهرًا السابقة.
4. أن يكون التاجر قد قام بإنشاء واختبار خطة الاستجابة لحوادث اختراق في بيانات الحساب سنويًا، وفقًا لمتطلبات PCI DSS.
5. استوفى التاجر أيًا مما يلي:
 - أ. تتم معالجة 75 بالمائة على الأقل من إجمالي عدد المعاملات السنوية المكتسبة من التاجر من خلال محطات نقاط البيع الهجينة، وعلى النحو المحدد بناءً على معاملات التاجر التي تمت معالجتها خلال الاثني عشر (12) شهرًا السابقة من خلال نظام التبادل. مشغل شبكة الدفع المحلية سيشمل المعاملات التي لم تتم معالجتها من خلال نظام التبادل في عدد المعاملات السنوية المكتسبة فقط، إذا كانت البيانات متاحة بسهولة لمشغل شبكة الدفع المحلية.
 - ب. نفذ التاجر حل تشفير من نقطة إلى نقطة مدرج في موقع PCI SSC.

يجب على جهة القبول أن تحتفظ بجميع شهادات التاجر الخاصة بالأهلية لبرنامج الإعفاء لمدة لا تقل عن خمس (5) سنوات. وبناءً على طلب مشغل شبكة الدفع المحلية، يجب على جهة القبول أن تقوم بتقديم شهادة التاجر للأهلية لبرنامج الإعفاء وأي وثائق و/أو معلومات أخرى تنطبق على هذه الشهادة. وتعد جهة القبول هي المسؤولة عن التحقق من أن كل شهادة برنامج إعفاء صحيحة ودقيقة.

يجب على التاجر الذي لا يفي بمعايير الأهلية لبرنامج الإعفاء، بما في ذلك التاجر التي تكون حجم معاملاته في الأساس من التجارة الإلكترونية، وقنوات قبول الطلب عبر البريد/ الطلب عبر الهاتف، أن يستمر في التحقق من امتثال PCI DSS.

يجب على جميع التجار الحفاظ على الامتثال المستمر لـ PCI DSS، وبغض النظر عما إذا كان التحقق من الامتثال السنوي كان شرطًا أم لا.

1.2.5.6. تقييمات عدم الامتثال لحماية بيانات الموقع

لمشغل شبكة الدفع المحلية إجراء تدقيق امتثال الأعضاء لمتطلبات موقع البيانات. وقد يؤدي عدم الامتثال في تاريخ التنفيذ المحدد أو بعده إلى التقييمات الموضحة في الجدول 6.4.

الجدول 6.4 - تقييمات عدم الامتثال
(انظر الملحق رقم 47)

قد يؤدي عدم الامتثال أيضًا إلى إنهاء العلاقة مع التاجر؛ إلغاء تسجيل TPP أو DSE أو PF أو SDWO أو DASP أو TSP أو TS أو 3-DSSP كمقدم خدمة؛ أو إنهاء جهة الإصدار أو جهة القبول كعضو.

The Issuer or Acquirer must provide annual PCI validation for each Level 1 and Level 2 Service Provider. The PCI Attestation of Compliance (AOC) and latest ASV Scan AOC must be submitted to [email address] after initial registration with the National Scheme Operator and every year thereafter. If a newly registered Service Provider is not yet compliant, the PCI Action Plan available on the Service Provider page of the SDP Program website must be completed and submitted for review.

The Acquirer must provide semi-annual compliance reporting for each of its Level 1, Level 2, and Level 3 Merchants. The SDP Acquirer Submission and Compliance Status Form, available on the Acquirer page of the SDP Program website, must be submitted to [email address] as indicated below.

(See appendix number 48)

6.5.2.2 Mandatory Compliance Requirements for Compromised Entities

The Acquirer must ensure that a detailed forensics evaluation is conducted. At the conclusion of the forensics evaluation, the National Scheme Operator will provide a Site Data Protection Account Data Compromise Information Form for completion by the compromised entity itself, if the compromised entity is a Service Provider, or by its Acquirer, if the compromised entity is a Merchant. The form must be returned by email message to [email address] within 30 calendar days of its receipt, and must include:

- The names of the QSA and the ASV that conducted the forensics evaluation;
- The entity's current level of compliance; and
- A gap analysis providing detailed steps required for the entity to achieve full compliance.

As soon as practical, but no later than 60 calendar days from the conclusion of the forensics evaluation, the compromised entity or its Acquirer must provide evidence from a QSA and an ASV that the compromised entity has achieved full compliance with the Payment Card Industry Data Security Standard and if applicable, the PCI TSP Security Requirements or the PCI 3DS Core Security Standard.

Such evidence (for example, a completed PCI SSC Attestation of Compliance [AOC] and a network scan AOC conducted by a PCI SSC ASV) must be submitted to the National Scheme Operator by email message to [email address].

Failure to comply with these requirements may result in SDP noncompliance assessments as described in Table 6.4. Any Merchant or Service Provider that has suffered a confirmed Account Data Compromise Event will be automatically reclassified to become a Level 1 Merchant or a Level 1 Service Provider, respectively. All compliance validation requirements for such Level 1 entities will apply.

6.5.3 Account Data Compromise Events

Definitions

As used in this Rule, the following terms have the meaning set forth below:

Account Data Compromise Event

An occurrence that results, directly or indirectly, in the unauthorized access to or disclosure of Account data or the unauthorized manipulation of Account data controls, such as Account usage and spending limits.

يجب على جهة الإصدار أو جهة القبول التحقق من صناعة بطاقات الدفع سنويًا لكل مقدم خدمة من المستوى 1 والمستوى 2. ويجب تقديم شهادة PCI للائتمان (AOC) وآخر فحص ASV AOC إلى [عنوان البريد الإلكتروني] بعد التسجيل المبدئي مع مشغل شبكة الدفع المحلية وكل سنة بعد ذلك بشكل دوري. وإذا لم يكن مقدم الخدمة المسجل حديثًا مستوفيًا للمتطلبات، فيجب إكمال خطة العمل PCI المتاحة على صفحة مقدم الخدمة على موقع برنامج SDP وإرسالها للمراجعة.

يجب على جهة القبول أن تقوم بتقديم تقارير الائتمان نصف السنوية لكل من التجار من المستوى 1 والمستوى 2 والمستوى 3. ويجب تقديم نموذج حالة التقديم والائتمان لجهة القبول SDP، المتاح في صفحة جهة القبول على موقع برنامج SDP، إلى [عنوان البريد الإلكتروني] كما هو موضح أدناه.

(انظر الملحق رقم 48)

2.2.5.6 متطلبات الائتمان الإلزامية للكيانات المعرضة للاختراق

يجب على جهة القبول التحقق من إجراء تقييم مفصل عن عدم مخالفة القوانين الجنائية. وفي ختام هذا التقييم، يقدم مشغل شبكة الدفع المحلية نموذج معلومات اختراق في بيانات حساب حماية بيانات الموقع لإكمالها من قبل الكيان المخترق نفسه، إذا كان الكيان المخترق هو مقدم الخدمة، أو من قبل القابل عليه، إذا كان الكيان المخترق تاجر. يجب إعادة النموذج عن طريق رسالة بريد إلكتروني إلى [عنوان البريد الإلكتروني] خلال 30 يومًا تقويميًا من استلامه، ويجب أن يتضمن:

- أسماء QSA و ASV الذي أجرى التقييم الجنائي .
- مستوى الائتمان الحالي للكيان.
- تحليل الفجوات يوفر الخطوات التفصيلية المطلوبة للكيان لتحقيق الائتمان الكامل.

في أقرب وقت ممكن، وبشرط أن لا يتجاوز الموعد 60 يومًا تقويميًا من انتهاء التقييم عدم مخالفة القوانين الجنائية، يجب على الكيان المخترق أو القابل عليه، تقديم الدليل من QSA و ASV على أنه قد حقق الائتمان الكامل لمعيار أمن بيانات صناعة بطاقات الدفع وإذا أمكن، متطلبات أمان PCI TSP أو معيار الأمان الأساسي PCI 3DS .

وقد تتمثل هذه الأدلة (على سبيل المثال، شهادة PCI SSC كاملة للائتمان [AOC] ومسح شبكة AOC بواسطة PCI SSC ASV) إلى مشغل شبكة الدفع المحلية عن طريق رسالة بريد إلكتروني إلى [عنوان البريد الإلكتروني] .

ويؤدي عدم الائتمان لهذه المتطلبات إلى تقييمات عدم امتثال SDP كما هو موضح في الجدول 6.4 . سيتم تلقائيًا إعادة تصنيف أي تاجر أو مقدم خدمة تعرض لحدث اختراق في بيانات حساب مؤكد، ليصبح تاجرًا من المستوى 1 أو مقدم خدمة من المستوى 1، على التوالي. سيتم تطبيق جميع متطلبات التحقق من الائتمان لهذه الكيانات من المستوى 1.

3.5.6 حالات المساومة في بيانات الحساب

تعريفات

كما هو مستخدم في هذه القاعدة ، فإن المصطلحات التالية لها المعنى الموضح أدناه:

حدث اختراق في بيانات الحساب

هو حدث يؤدي، بشكل مباشر أو غير مباشر، إلى الوصول غير المصرح به إلى بيانات الحساب، أو الكشف عنها أو التلاعب غير المصرح به في ضوابط بيانات الحساب، مثل استخدام الحساب وحدود الإنفاق.

Agent

Any entity that stores, processes, transmits, or has access to Account data by virtue of its contractual or other relationship, direct or indirect, with a Member. For the avoidance of doubt, Agents include, but are not limited to, Merchants, Third Party Processors (TPPs), Data Storage Entities (DSEs), and Terminal Servicers (TSs) (regardless of whether the TPP, DSE, or TS is registered with the National Scheme Operator).

Member

This term appears in the Key Terms defined in chapter 1 of this Manual. For the avoidance of doubt, for purposes of this Book, any entity that the National Scheme Operator licenses to issue Cards and/or acquire Transactions shall be deemed a Member.

Potential Account Data Compromise Event or Potential Event

An occurrence that could result, directly or indirectly, in the unauthorized access to or disclosure of Account data or the unauthorized manipulation of Account data controls, such as Account usage and spending limits.

Sensitive Authentication Data

This term has the meaning set forth in the Payment Card Industry Data Security Standard (PCI DSS), and includes, by way of example and not limitation, the full contents of a Card's magnetic stripe or the equivalent on a chip, Card validation number 2 (CVV 2) data, and PIN or PIN block data.

6.5.3.1 Policy Concerning Account Data Compromise Events and Potential Account Data Compromise Events

The National Scheme Operator operates a payment solutions system for all of its Members. Each Member benefits from, and depends upon, the integrity of that system. Account Data Compromise Events and Potential Account Data Compromise Events threaten the integrity of the scheme and undermine the confidence of Merchants, Members, Cardholders, and the public at large in the security and viability of the system. Each Member therefore acknowledges that the National Scheme Operator has a compelling interest in adopting, interpreting, and enforcing its Standards to protect against and respond to Account Data Compromise Events and Potential Account Data Compromise Events.

Given the abundance and sophistication of criminals, Account Data Compromise Events and Potential Account Data Compromise Events are risks inherent in operating and participating in any system that utilizes payment card account data for financial or non-financial transactions. The Standards are designed to place responsibility for Account Data Compromise Events and Potential Account Data Compromise Events on the Member that is in the best position to guard against and respond to such risk. That Member is generally the Member whose network, system, or environment was compromised or was vulnerable to compromise or that has a direct or indirect relationship with an Agent whose network, system, or environment was compromised or was vulnerable to compromise. In the view of the National Scheme Operator, that Member is in the best position to safeguard its systems, to require and monitor the safeguarding of its Agents' systems, and to insure against, and respond to, Account Data Compromise Events and Potential Account Data Compromise Events.

وكيل

هو أي كيان يقوم بتخزين بيانات الحساب أو معالجتها أو نقلها أو الوصول إليها بموجب علاقة تعاقدية أو علاقة أخرى، مباشرة أو غير مباشرة، مع أحد الأعضاء. ومنعاً لحدوث الشك في التفسير، يشمل الوكلاء، على سبيل المثال، التجار ومعالجي الطرف الثالث، وكيانات تخزين البيانات والخوادم الطرفية (بغض النظر عما إذا كان معالجي الطرف الثالث أو كيانات تخزين البيانات أو الخوادم الطرفية مسجلة مع مشغل شبكة الدفع المحلية).

عضو

ينصرف هذا المصطلح كما تم تحديده في المصطلحات الأساسية المحددة في الفصل الأول من هذا الدليل. ومنعاً لحدوث الشك في التفسير، فإن أي كيان يرخص له مشغل شبكة الدفع المحلية لإصدار البطاقات و/أو الحصول على المعاملات يعتبر عضوًا.

حدث اختراق بيانات الحساب المحتمل أو حدث محتمل

هو حدث يؤدي، بشكل مباشر أو غير مباشر، إلى الوصول غير المصرح به إلى بيانات الحساب أو الكشف عنها أو التلاعب غير المصرح به في ضوابط بيانات الحساب، مثل استخدام الحساب وحدود الإنفاق.

بيانات المصادقة الحساسة

ينصرف هذا المصطلح إلى المعنى المنصوص عليه في معيار أمان بيانات صناعة بطاقات الدفع، ويتضمن، على سبيل المثال، المحتويات الكاملة للشريط المغناطيسي للبطاقة أو ما يعادله على شريحة، رقم التحقق من البطاقة 2 بيانات (CVV 2) ورقم التعريف الشخصي أو بيانات حظر رقم التعريف الشخصي.

1.3.5.6 السياسة المتعلقة بحالات المساومة في بيانات الحساب والحساب المحتملة

على مشغل شبكة الدفع المحلية أن يقوم بتشغيل نظام حلول الدفع لجميع أعضائه. ويجب على كل عضو الاعتماد هذا النظام، وباعتبار أن أحداث اختراق في بيانات الحساب وأحداث اختراق بيانات الحساب المحتملة تهدد سلامة النظام وتمس ثقة التجار والأعضاء وحاملي البطاقات والجمهور بشكل عام في أمان النظام وإمكانية استمراره، لذلك يقر كل عضو بأن لمشغل شبكة الدفع المحلية مصلحة في تبني المعايير التي يحددها وفرضها للحماية من أحداث اختراق في بيانات الحساب وأحداث اختراق بيانات الحساب المحتملة والاستجابة لها.

نظرًا لتطور وسائل اختراق البيانات، فإن أحداث اختراق بيانات الحساب وأحداث اختراق بيانات الحساب المحتملة هي مخاطر متأصلة في التشغيل والمشاركة في أي نظام يستخدم في بيانات حساب بطاقة الدفع للمعاملات المالية أو غير المالية. وقد تم تصميم هذه المعايير لتحميل المسؤولية عن أحداث اختراق في بيانات الحساب وأحداث اختراق بيانات الحساب المحتملة على العضو الذي يكون في أفضل وضع للحماية من هذه المخاطر والاستجابة لها.

ويحدد هذا العضو بشكل عام بأنه العضو الذي تعرضت شبكته أو نظامه أو بيئته للاختراق أو كانت عرضة للاختراق أو لديه علاقة مباشرة أو غير مباشرة مع وكيل تعرضت شبكته أو نظامه أو بيئته للاختراق أو كانت عرضة للاختراق. من وجهة نظر مشغل شبكة الدفع المحلية، فإن هذا العضو في أفضل وضع لحماية أنظمتها، وطلب ومراقبة حماية أنظمة وكلائه، والتأمين ضد أحداث اختراق بيانات الحساب وأحداث اختراق بيانات الحساب المحتملة والاستجابة لها.

The National Scheme/Network Operator requires that each Member apply the utmost diligence and forthrightness in protecting against and responding to any Account Data Compromise Event or Potential Account Data Compromise Event. Each Member acknowledges and agrees that the National Scheme Operator has both the right and need to obtain full disclosure (as determined by the National Scheme Operator) concerning the causes and effects of an Account Data Compromise Event or Potential Account Data Compromise Event as well as the authority to impose assessments, recover costs, and administer compensation, if appropriate, to Members that have incurred costs, expenses, losses, and/or other liabilities in connection with Account Data Compromise Events and Potential Account Data Compromise Events.

Except as otherwise expressly provided for in the Standards, the National Scheme Operator determinations with respect to the occurrence of and responsibility for Account Data Compromise Events or Potential Account Data Compromise Events are conclusive and are not subject to appeal or review within the National Scheme Operator.

Any Member that is uncertain with respect to rights and obligations relating to or arising in connection with the Account Data Compromise Event Standards and Programs set forth in this Rule should request advice from the National Scheme Operator.

Notwithstanding the generality of the foregoing, the relationship of network, system, and environment configurations with other networks, systems, and environments will often vary, and each Account Data Compromise Event and Potential Account Data Compromise Event tends to have its own particular set of circumstances. The National Scheme Operator has the sole authority to interpret and enforce the Standards, including those set forth in this Book. Consistent with the foregoing and pursuant to the definitions set forth above, the National Scheme Operator may determine, as a threshold matter, whether a given set of circumstances constitutes a single Account Data Compromise Event or multiple Account Data Compromise Events.

In this regard, and by way of example, where a Member or Merchant connects to, utilizes, accesses, or participates in a common network, system, or environment with one or more other Members, Merchants, Service Providers, or third parties, a breach of the common network, system, or environment that results, directly or indirectly, in the compromise of local networks, systems, or environments connected thereto may be deemed to constitute a single Account Data Compromise Event.

6.5.3.2 Responsibilities in Connection with Account Data Compromise Events and Potential Account Data Compromise Events

The Member whose system or environment, or whose Agent's system or environment, was compromised or vulnerable to compromise (at the time that the Account Data Compromise Event or Potential Account Data Compromise Event occurred) is fully responsible for resolving all outstanding issues and liabilities to the satisfaction of the National Scheme Operator, notwithstanding any subsequent change in the Member's relationship with any such Agent after the Account Data Compromise Event or Potential Account Data Compromise Event occurred. In the event of any dispute, the National Scheme Operator will determine the responsible Member(s).

يوجب مشغل شبكة الدفع المحلية على كل عضو أن يبذل أقصى درجات العناية والصراحة في الحماية من حدث اختراق في بيانات الحساب أو حدث لاختراق بيانات الحساب محتمل و الاستجابة لها. ويقر كل عضو ويوافق على أن مشغل شبكة الدفع المحلية لديه الحق في الحصول على إفصاح كامل (على النحو الذي يحدده مشغل شبكة الدفع المحلية) فيما يتعلق بأسباب وتأثيرات حدث اختراق في بيانات الحساب أو الحدث المحتمل اختراق في بيانات الحساب، بالإضافة إلى سلطة فرض التقييمات واسترداد التكاليف وإدارة التعويضات، إذا كان ذلك مناسبًا، للأعضاء الذين تكبدوا تكاليف ونفقات وخسائر و/أو التزامات أخرى فيما يتعلق بأحداث اختراق بيانات الحساب وأحداث اختراق بيانات الحساب المحتملة.

باستثناء ما هو منصوص عليه صراحةً في المعايير، فإن قرارات مشغل شبكة الدفع المحلية فيما يتعلق بحدوث أحداث اختراق في بيانات الحساب أو أحداث الاختراق بيانات الحساب المحتملة ومسؤوليتها هي نهائية ولا تخضع للطعن أو المراجعة من خلال مشغل شبكة الدفع المحلية.

يجب على أي عضو غير متحقق من الحقوق والالتزامات المتعلقة بتطبيق المعايير، وبرامج أحداث اختراق في بيانات الحساب المنصوص عليها في هذه القاعدة أن يطلب المشورة من مشغل شبكة الدفع المحلية.

بغض النظر عن عمومية تطبيق القاعدة السابقة، إلا أنه غالبًا ما تختلف علاقة تكوينات الشبكة والنظام والبيئة مع الشبكات والأنظمة والبيئات الأخرى، ويميل كل حدث اختراق في بيانات الحساب واحتمال حدوث اختراق في بيانات الحساب إلى مجموعة الظروف الخاصة به. ويتمتع مشغل شبكة الدفع المحلية بالسلطة الوحيدة لتفسير المعايير وتطبيقها، بما في ذلك تلك المنصوص عليها في هذا الكتاب. وعليه، تمشيا مع ما سبق ووفقا للتعريفات الواردة أعلاه، يجوز لمشغل شبكة الدفع المحلية أن يحدد، ما إذا كانت مجموعة معينة من الظروف تشكل حدثًا واحدًا لاختراق في بيانات الحساب أو أحداث متعددة لاختراق بيانات الحساب.

في هذا الصدد، وعلى سبيل المثال، عندما يتصل عضو، أو تاجر بشبكة أو نظام أو بيئة مشتركة، أو يستخدمها أو يصل إليها أو يشارك فيها مع عضو، أو أكثر من الأعضاء الآخرين أو التجار أو مقدمي الخدمات، أو الأطراف الثالثة، يمكن اعتبار خرق الشبكة أو النظام أو البيئة المشتركة الذي ينتج بشكل مباشر أو غير مباشر عن اختراق الشبكات أو الأنظمة أو البيئات المحلية المتصلة بها، بمثابة حدث واحد لاختراق في بيانات الحساب.

2.3.5.6. المسؤوليات المتعلقة بحالات المساومة في بيانات الحساب، وبيانات الحساب المحتملة

يكون العضو الذي تعرض نظامه أو بيئته، أو نظام وكيله أو بيئته، للاختراق أو كان عرضة للاختراق (في الوقت الذي حدث فيه حدث اختراق في بيانات الحساب أو احتمال حدث اختراق في بيانات الحساب) مسؤولاً مسؤولية كاملة عن حل جميع المشكلات والالتزامات، طبقاً للسلطة التقديرية لمشغل شبكة الدفع المحلية، وبغض النظر عن أي تغيير لاحق في علاقة العضو مع أي وكيل، وبعد حدث اختراق في بيانات الحساب، احتمال حدث اختراق بيانات الحساب. وفي حالة وجود منازعة، يحدد مشغل شبكة الدفع المحلية من هو العضو (الأعضاء) المسؤول.

Should a Member, in the judgment of the National Scheme Operator, fail to fully cooperate with the investigation of an Account Data Compromise Event or Potential Account Data Compromise Event, the National Scheme Operator (i) may infer that information sought by the National Scheme Operator, but not obtained as a result of the failure to cooperate, would be unfavorable to that Member and (ii) may act upon that adverse inference in the application of the Standards. By way of example and not limitation, a failure to cooperate can result from a failure to provide requested information; a failure to cooperate with investigation guidelines, procedures, practices, and the like; or a failure to ensure that the National Scheme Operator has reasonably unfettered access to the forensic examiner.

A Member may not, by refusing to cooperate with the investigation, avoid a determination that there was an Account Data Compromise Event. Should a Member fail without good cause to comply with its obligations in this chapter 6 or to respond fully and in a timely fashion to a request for information to which the National Scheme Operator is entitled in this chapter 6, the National Scheme Operator may draw an adverse inference that information to which the National Scheme Operator is entitled, but that was not timely obtained as a result of the Member's noncompliance, would have supported or, where appropriate, confirmed a determination that there was an Account Data Compromise Event.

Before drawing such an adverse inference, the National Scheme Operator will notify the Member of its noncompliance and give the Member an opportunity to show good cause, if any, for its noncompliance. The drawing of an adverse inference is not exclusive of other remedies that may be invoked for a Member's noncompliance.

The following provisions set forth requirements and procedures to which each Member and its Agent(s) must adhere upon becoming aware of an Account Data Compromise Event or Potential Account Data Compromise Event.

6.5.3.3 Time-Specific Procedures for Account Data Compromise Events and Potential Account Data Compromise Events

A Member is deemed to be aware of an Account Data Compromise Event or Potential Account Data Compromise Event when the Member or the Member's Agent first knew or, in the exercise of reasonable security practices should have known of an Account Data Compromise Event or a Potential Account Data Compromise Event. A Member or its Agent is deemed to be aware of an Account Data Compromise Event or Potential Account Data Compromise Event under circumstances that include, but are not limited to, any of the following:

- the Member or its Agent is informed, through any source, of the installation or existence of any malware in any of its systems or environments, or any system or environment of one of its Agents, no matter where such malware is located or how it was introduced;
- the Member or its Agent receives notification from the National Scheme Operator or any other source that the Member or its Agent(s) has experienced an Account Data Compromise Event or a Potential Account Data Compromise Event; or
- The Member or its Agent discovers or, in the exercise of reasonable diligence, should have discovered a security breach or unauthorized penetration of its own system or environment or the system or environment of its Agent(s).

A Member must notify the National Scheme Operator immediately when the Member becomes aware of an Account Data Compromise Event or Potential Account Data

وفي حالة فشل العضو، وفقًا لتقدير مشغل شبكة الدفع المحلية، في التعاون بشكل كامل مع التحقيق في حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، يجوز لمشغل شبكة الدفع المحلية: (1) استنتاج تلك المعلومات التي سعى إليها مشغل شبكة الدفع المحلية، ولكن لم يتم الحصول عليها نتيجة لعدم التعاون، سيكون غير موافٍ لذلك العضو. (2) قد يتصرف بناءً على هذا الاستنتاج المعاكس في تطبيق المعايير. على سبيل المثال، يمكن أن ينتج عدم التعاون عن عدم تقديم المعلومات المطلوبة؛ وعدم التعاون مع إرشادات التحقيق وإجراءاته وممارساته وما شابه ذلك؛ أو الفشل في التأكد من أن مشغل شبكة الدفع المحلية لديه وصول غير مقيد بشكل معقول إلى التقييم في التحقيق الجنائي.

لا يجوز للعضو، برفضه التعاون مع التحقيق، تجنب اتخاذ قرار بوجود حدث لاختراق في بيانات الحساب. وفي حالة فشل العضو دون سبب، في الامتثال لالتزاماته الواردة في هذا الفصل 6، أو الاستجابة بشكل كامل، وفي الوقت المناسب لطلب الحصول على المعلومات التي يحق لمشغل شبكة الدفع المحلية الحصول عليها في هذا الفصل 6، يجوز لمشغل شبكة الدفع المحلية أن يرسم الاستنتاج المعاكس لتلك المعلومات التي يحق لمشغل شبكة الدفع المحلية الحصول عليها، ولكن لم يتم الحصول عليها في الوقت المناسب نتيجة لعدم امتثال العضو، وكان من شأنه أن يدعم أو يؤكد، عند الاقتضاء، قرارًا بوجود حدث اختراق في بيانات الحساب.

قبل استخلاص مثل هذا الاستنتاج المعاكس، يقوم مشغل شبكة الدفع المحلية بإخطار العضو بعدم امتثاله، ويمنحه فرصة لإظهار سبب عدم الامتثال، إن وجد. لا يقتصر رسم الاستدلال المعاكس على العلاجات الأخرى التي يمكن التذرع بها لعدم امتثال العضو.

تحدد الأحكام التالية المتطلبات والإجراءات التي يجب على كل عضو ووكيله (وكلائه) الالتزام بها عند علمه بحدث اختراق في بيانات الحساب أو احتمال حدث اختراق في بيانات الحساب.

3.3.5.6 الإجراءات المحددة بميعاد حالات المساومة في بيانات الحساب، و بيانات الحساب المحتملة

يُعتبر العضو على علم بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، عندما علم العضو أو وكيل العضو لأول مرة، أو أثناء ممارسة أمنية معقولة، ويجب أن يكون على علم بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب. ويُعتبر العضو أو وكيله على علم بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب في ظل ظروف تشمل، على سبيل المثال الحالات التالية:

- يتم إخطار العضو أو وكيله، من خلال أي مصدر، بتثبيت أو وجود أي برامج ضارة في أي من أنظمتها أو بيئاتها، أو أي نظام أو بيئة لأحد وكلائه، وبغض النظر عن مكان وجود هذه البرامج الضارة أو كيف تم تقديمها.
- يتلقى العضو أو وكيله إخطاراً من مشغل شبكة الدفع المحلية، أو أي مصدر آخر بأن العضو أو وكيله (وكلائه) قد تعرض لحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب.
- يكتشف العضو أو وكيله، أو في إطار ممارسة العناية المعقولة، أنه كان ينبغي له اكتشاف خرق أممي أو اختراق غير مصرح به لنظامه أو بيئته أو نظام أو بيئة وكيله (وكلائه).

يجب على العضو إخطار مشغل شبكة الدفع المحلية على الفور عندما يعلم العضو بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، وكان من شأنه التأثير على أي نظام أو بيئة للعضو أو وكيله. وبالإضافة إلى ذلك، يجب على العضو، بموجب العقد، التحقق من أن وكيله

Compromise Event in or affecting any system or environment of the Member or its Agent. In addition, a Member must, by contract, ensure that its Agent notifies the National Scheme Operator immediately when the Agent becomes aware of an Account Data Compromise Event or Potential Account Data Compromise Event in or affecting any system or environment of the Member or the Agent.

When a Member or its Agent becomes aware of an Account Data Compromise Event or Potential Account Data Compromise Event either in any of its own systems or environments or in the systems or environments of its Agent(s), the Member must take (or cause the Agent to take) the following actions, unless otherwise directed in writing by the National Scheme Operator.

- Immediately commence a thorough investigation into the Account Data Compromise Event or Potential Account Data Compromise Event.
- Immediately, and no later than within twenty-four (24) hours, identify, contain, and mitigate the Account Data Compromise Event or Potential Account Data Compromise Event, secure Account data and preserve all information, in all media, concerning the Account Data Compromise Event or Potential Account Data Compromise Event, including:
 1. preserve and safeguard all potential evidence pertinent to a forensic examination of an Account Data Compromise Event or Potential Account Data Compromise Event using industry best practices;
 2. isolate compromised systems and media from the network;
 3. preserve all Intrusion Detection Systems, Intrusion Prevention System logs, all firewall, Web, database, and events logs;
 4. document all incident response actions thoroughly; and
 5. refrain from restarting or rebooting any compromised or potentially compromised system or taking equivalent or other action that would have the effect of eliminating or destroying information that could potentially provide evidence of an Account Data Compromise Event or Potential Account Data Compromise Event.
- Within twenty-four (24) hours, and on an ongoing basis thereafter, submit to the National Scheme Operator all known or suspected facts concerning the Account Data Compromise Event or Potential Account Data Compromise Event, including, by way of example and not limitation, known or suspected facts as to the cause and source of the Account Data Compromise Event or Potential Account Data Compromise Event to the satisfaction of the National Scheme Operator.
- Within twenty-four (24) hours and continuing throughout the investigation and thereafter, provide to the National Scheme Operator, in the required format, all primary account numbers (PANs) associated with Account data that were actually or potentially accessed or disclosed in connection with the Account Data Compromise Event or Potential Account Data Compromise Event and any additional information requested by the National Scheme Operator. As used herein, the obligation to obtain and provide PANs to the National Scheme Operator applies to any the National Scheme Operator or Maestro Account number in a bank identification number (BIN)/Issuer identification number (IIN) range assigned by the National Scheme Operator. This obligation applies regardless of how or why such PANs were received, processed, or stored, including, by way of example and not limitation, in connection with or relating to a credit, debit (signature- or PIN-based) proprietary, or any other kind of payment Transaction, incentive, or reward program.

يخطر مشغل شبكة الدفع المحلية على الفور عندما يعلم الوكيل بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق بيانات الحساب، وكان من شأنه التأثير على أي نظام أو بيئة للعضو أو الوكيل .

عندما يعلم العضو أو وكيله بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، إما في أنظمتهم أو بيئاته الخاصة، أو كان في أنظمة أو بيئات وكيله (وكلائه)، فإنه يجب على العضو اتخاذ (أو بسبب الوكيل في اتخاذ) الإجراءات التالية، ما لم يوجه على خلاف ذلك بطريقة كتابية من قبل مشغل شبكة الدفع المحلية.

- البدء فوراً في إجراء تحقيق شامل في حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق بيانات الحساب.
- على الفور، وفي موعد لا يتجاوز أربع وعشرين (24) ساعة، تحديد واحتواء وتخفيف حدث الاختراق في بيانات الحساب أو احتمال حدث اختراق في بيانات الحساب، وتأمين بيانات الحساب والاحتفاظ بجميع المعلومات، في جميع الوسائط، وفيما يتعلق بحدث اختراق في بيانات الحساب أو احتمال حدث اختراق بيانات الحساب، بما في ذلك:
 1. الحفاظ على جميع الأدلة المحتملة ذات الصلة بفحص التحقيق الجنائي لحدث اختراق في بيانات الحساب أو احتمال حدث اختراق في بيانات الحساب، باستخدام أفضل الممارسات التقنية.
 2. عزل الأنظمة، والوسائط المخترقة عن الشبكة.
 3. الحفاظ على جميع أنظمة الكشف عن التطفل، وسجلات نظام منع التطفل، وجميع سجلات جدار الحماية، والويب، وقواعد البيانات والأحداث.
 4. توثيق جميع إجراءات الاستجابة للحوادث بدقة.
 5. الامتناع عن إعادة تشغيل النظام الذي تم اختراقه أو كان من المحتمل تعرضه للاختراق، أو اتخاذ آخر من شأنه أن يؤدي إلى إزالة أو إتلاف المعلومات التي قد توفر دليلاً على حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق بيانات الحساب.
- خلال أربع وعشرين (24) ساعة، وبطريقة مستمرة، التقديم إلى مشغل شبكة الدفع المحلية بجميع الحقائق المعروفة أو المشتبه بها المتعلقة بحدث اختراق في بيانات الحساب أو احتمال حدث اختراق في بيانات الحساب، بما في ذلك، على سبيل المثال، الحقائق المعروفة أو المشتبه بها فيما يتعلق بالسبب، والمصدر لحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، طبقاً لما يقدره مشغل شبكة الدفع المحلية.
- خلال أربع وعشرين (24) ساعة وبطريقة مستمرة، التقديم إلى مشغل شبكة الدفع المحلية، بالتنسيق المطلوب، وجميع أرقام الحسابات الأساسية المرتبطة ببيانات الحساب التي تم الوصول إليها بالفعل، أو من المحتمل أن يتم الوصول إليها، أو الكشف عنها فيما يتعلق بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، وأي معلومات إضافية يطلبها مشغل شبكة الدفع المحلية كما هو مستخدم هنا، فإن الالتزام بالحصول على أرقام الحسابات الأساسية وتقديمها إلى مشغل شبكة الدفع المحلية ينطبق على أي رقم مشغل شبكة الدفع المحلية، أو حساب Maestro في نطاق رقم تعريف مصرفي / رقم تعريف جهات الإصدار المعين من قبل مشغل شبكة الدفع المحلية. وينطبق هذا الالتزام بغض النظر عن كيفية أو سبب تلقي أرقام الحسابات الأساسية، أو معالجتها أو تخزينها، بما في ذلك، على سبيل المثال، فيما يتعلق أو يرتبط بملكية ائتمان أو خصم (قائم على التوقيع أو رقم التعريف الشخصي) ، أو أي نوع آخر من معاملات الدفع أو الحوافز أو برنامج المكافآت.

- Within seventy-two (72) hours, engage the services of a PCI SSC Forensic Investigator (PFI) to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration, and effects of the Account Data Compromise Event or Potential Account Data Compromise Event. The PFI engaged to conduct the investigation must remain free of conflict of interest as defined in the PFI Program Guide. Prior to the commencement of such PFI's investigation, the Member must notify the National Scheme Operator of the proposed scope and nature of the investigation and obtain preliminary approval of such proposal by the National Scheme Operator or, if such preliminary approval is not obtained, of a modified proposal acceptable to the National Scheme Operator. The National Scheme Operator and the responsible Member(s) may agree that a PFI's investigation of, investigation findings, and recommendations concerning fewer than all of the Merchants (or other Agents) within the scope of the Account Data Compromise Event or Potential Account Data Compromise Event will be deemed to be representative of and used for purposes of the application of the Standards as the investigation findings and recommendations by the PFI with respect to all of the Merchants (or other Agents) within the scope of the Account Data Compromise Event or Potential Account Data Compromise Event.
- Within two (2) business days from the date on which the PFI was engaged, identify to the National Scheme Operator the engaged PFI and confirm that such PFI has commenced its investigation.
- Within five (5) business days from the commencement of the forensic investigation, ensure that the PFI submits to the National Scheme Operator a preliminary forensic report detailing all investigative findings to date.
- Within ten (10) business days from the end of the PFI investigation, provide to the National Scheme Operator a final forensic report detailing all findings, conclusions, and recommendations of the PFI, continue to address any outstanding exposure, and implement all recommendations until the Account Data Compromise Event or Potential Account Data Compromise Event is resolved to the satisfaction of the National Scheme Operator. In connection with the independent forensic investigation and preparation of the final forensic report, no Member may engage in or enter into (or permit an Agent to engage in or enter into) any conduct, agreement, or understanding that would impair the completeness, accuracy, or objectivity of any aspect of the forensic investigation or final forensic report. The Member shall not engage in any conduct (or permit an Agent to engage in any conduct) that could or would influence, or undermine the independence of, the PFI or undermine the reliability or integrity of the forensic investigation or final forensic report. By way of example, and not limitation, a Member must not itself, or permit any of its Agents to, take any action or fail to take any action that would have the effect of:
 1. precluding, prohibiting, or inhibiting the PFI from communicating directly with the National Scheme Operator;
 2. permitting a Member or its Agent to substantively edit or otherwise alter the forensic report; or
 3. Directing the PFI to withhold information from the National Scheme Operator.
 Notwithstanding the foregoing, the National Scheme Operator may engage a PFI on behalf of the Member in order to expedite the investigation. The Member on whose behalf the PFI is so engaged will be responsible for all costs associated with the investigation.

- خلال اثنتيْن وسبعين (72) ساعة، الاستعانة بخدمات (النيابة العامة) المحقق الجنائي (PFI) PCI SSC لإجراء تحقيق جنائي مستقل، لتقييم سبب ونطاق وحجم ومدة وتأثيرات حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب. ويجب أن يظل PFI المشارك لإجراء التحقيق خاليًا من تضارب المصالح على النحو المحدد في دليل برنامج PFI. وقبل الشروع في هذا التحقيق مع PFI، يجب على العضو إخطار مشغل شبكة الدفع المحلية بالنطاق والطبيعة المقترحين للتحقيق والحصول على موافقته المبدئية على هذا الاقتراح، وإذا لم يتم الحصول على هذه الموافقة المبدئية، اقتراح معدل مقبول لمشغل شبكة الدفع المحلية. وقد يتفق مشغل شبكة الدفع المحلية والعضو (الأعضاء) المسؤول على أن تحقيق PFI لنتائج التحقيق والتوصيات المتعلقة بعدد أقل من جميع التجار (أو الوكلاء الآخرين) في نطاق حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق بيانات الحساب، وسيعتبر الحدث ممثلًا ومستخدمًا لأغراض تطبيق المعايير مثل نتائج التحقيق والتوصيات المقدمة من PFI فيما يتعلق بجميع التجار (أو الوكلاء الآخرين) في نطاق حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق بيانات الحساب.
- خلال يومين (2) عمل من التاريخ الذي تم فيه إشراك PFI، وتحديد مشغل شبكة الدفع المحلية بـ PFI المشارك وتأكيد أن هذا PFI قد بدأ التحقيق.
- خلال خمسة (5) أيام عمل من بدء التحقيق الجنائي، وتأكيد أن (PFI) يقدم إلى مشغل شبكة الدفع المحلية تقريرًا جنائيًا أوليًا يوضح بالتفصيل جميع نتائج التحقيق حتى الآن.
- خلال عشرة (10) أيام عمل من نهاية تحقيق PFI، تقديم مشغل شبكة الدفع المحلية تقريرًا جنائيًا نهائيًا يوضح بالتفصيل جميع النتائج والاستنتاجات والتوصيات الخاصة بـ PFI، والاستمرار في معالجة أي تعرض معلق، وتنفيذ جميع التوصيات، حتى تتم معالجة حدوث الاختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، طبقاً لما يقدره مشغل شبكة الدفع المحلية. وفيما يتعلق بالتحقيق الجنائي المستقل، وإعداد التقرير الجنائي النهائي، لا يجوز لأي عضو ممارسة أو الدخول في (أو السماح للوكيل بالممارسة أو الدخول في) أي سلوك أو اتفاق من شأنه أن يؤثر على دقة أو موضوعية التحقيق الجنائي، أو التقرير الجنائي النهائي. ولا يجوز للعضو ممارسة أي سلوك (أو السماح للوكيل بممارسة أي سلوك) يمكن أو من شأنه التأثير أو التقليل من استقلالية PFI أو يقلل مصداقية أو سلامة التحقيق الجنائي أو التقرير الجنائي النهائي. على سبيل المثال، لا يجب على العضو بذاته، أو السماح لأي من وكلائه، باتخاذ أي إجراء أو عدم اتخاذ أي إجراء من شأنه أن يكون له تأثير:
 1. منع أو حظر أو تثبيط PFI من الاتصال مباشرة ومشغل شبكة الدفع المحلية.
 2. السماح لعضو أو وكيله بتعديل التقرير الجنائي بشكل جوهري أو تغييره بطريقة أخرى.
 3. توجيه PFI لحجب المعلومات عن مشغل شبكة الدفع المحلية.
 وعلى الرغم مما سبق ذكره، يجوز لمشغل شبكة الدفع المحلية إشراك PFI نيابة عن العضو من أجل تسريع التحقيق. وسيكون العضو الذي يشارك PFI نيابة عنه مسؤولاً عن جميع التكاليف المرتبطة بالتحقيق.

6.5.3.4 Ongoing Procedures for Account Data Compromise Events and Potential Account Data Compromise Events

- From the time that the Member or its Agent becomes aware of an Account Data Compromise Event or Potential Account Data Compromise Event until the investigation is concluded to the satisfaction of the National Scheme Operator, the Member must:
- Provide weekly written status reports containing current, accurate, and updated information concerning the Account Data Compromise Event or Potential Account Data Compromise Event, the steps being taken to investigate and remediate same, and such other information as the National Scheme Operator may request.
- Preserve all files, data, and other information pertinent to the Account Data Compromise Event or Potential Account Data Compromise Event, and refrain from taking any actions (e.g., rebooting) that could result in the alteration or loss of any such files, forensic data sources, including firewall and event log files, or other information.
- Respond fully and promptly, in the manner prescribed by the National Scheme Operator, to any questions or other requests (including follow-up requests) from the National Scheme Operator with regard to the Account Data Compromise Event or Potential Account Data Compromise Event and the steps being taken to investigate and remediate same.
- Authorize and require the PFI to respond fully, directly, and promptly to any written or oral questions or other requests from the National Scheme Operator, and to so respond in the manner prescribed by the National Scheme Operator, with regard to the Account Data Compromise Event or Potential Account Data Compromise Event, including the steps being taken to investigate and remediate same.
- Consent to, and cooperate with, any effort by the National Scheme Operator to engage and direct a PFI to perform an investigation and prepare a forensic report concerning the Account Data Compromise Event or Potential Account Data Compromise Event, in the event that the Member fails to satisfy any of the foregoing responsibilities.
- Ensure that the compromised entity develops a remediation action plan, including implementation and milestone dates related to findings, corrective measures, and recommendations identified by the PFI and set forth in the final forensic report.
- Monitor and validate that the compromised entity has fully implemented the remediation action plan, recommendations, and corrective measures.

6.5.3.5 Forensic Report

The responsible Member (or its Agent) must ensure that the PFI retains and safeguards all draft forensic report(s) pertaining to the Account Data Compromise Event or Potential Account Data Compromise Event and, upon request of the National Scheme Operator, immediately provides to the National Scheme Operator any such draft. The PFI should adhere to the PCI SSC PFI Program Guide as it pertains to the work products produced by the PFI.

The National Scheme Operator may require the Member to cause a PFI to conduct a PCI gap analysis and include the result of that analysis in the final forensic report.

4.3.5.6. الإجراءات المستمرة لحالات المساومة في بيانات الحساب، و بيانات الحساب المحتملة

- من الوقت الذي علم فيه العضو أو وكيله، بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، وحتى انتهاء التحقيق طبقاً لما يقرره مشغل شبكة الدفع المحلية، يجب على العضو:
- تقديم تقارير مكتوبة بشكل أسبوعي، تحتوي على معلومات حالية ودقيقة ومحدثة فيما يتعلق بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، والخطوات التي يتم اتخاذها للتحقيق ومعالجتها، والمعلومات الأخرى التي قد يطلبها مشغل شبكة الدفع المحلية.
- الاحتفاظ بجميع الملفات والبيانات والمعلومات الأخرى ذات الصلة بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، والامتناع عن اتخاذ أي إجراءات (على سبيل المثال، إعادة التشغيل) قد تؤدي إلى تغيير أو فقدان أي من هذه الملفات أو مصادر بيانات التحقيق الجنائي، بما في ذلك ملفات سجل الأحداث و جدار الحماية، أو أي معلومات أخرى.
- الرد الكامل والفوري، وبالطريقة التي يحددها مشغل شبكة الدفع المحلية، على الأسئلة أو الطلبات أخرى (بما في ذلك طلبات المتابعة) من مشغل شبكة الدفع المحلية فيما يتعلق بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، والخطوات يتم أخذها للتحقيق ومعالجتها.
- تحويل وطلب PFI للرد بشكل كامل ومباشر وسريع على أي أسئلة مكتوبة أو شفوية أو طلبات أخرى من مشغل شبكة الدفع المحلية، والرد على ذلك بالطريقة التي يحددها مشغل شبكة الدفع المحلية وفيما يتعلق بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، بما في ذلك الخطوات التي يتم اتخاذها للتحقيق ومعالجتها.
- الموافقة والتعاون مع ما يبذله مشغل شبكة الدفع المحلية لإشراك وتوجيه PFI مشارك لإجراء تحقيق وإعداد تقرير جنائي يتعلق بحدث اختراق في بيانات الحساب، أو حدث اختراق في بيانات الحساب، وفي حالة فشل العضو في استيفاء أي من المسؤوليات السابقة.
- التحقق من أن الكيان المخترق يطور خطة عمل علاجية، طبقاً للمواعيد المحددة، بما في ذلك التنفيذ تدابير التصحيحية، والتوصيات التي حددها PFI والواردة في التقرير الجنائي النهائي.
- المراقبة والتحقق من أن الكيان المخترق قد نفذ بالكامل خطة عمل الإصلاح، والتوصيات والتدابير التصحيحية.

5.3.5.6. التقرير الجنائي

يجب على العضو المسؤول (أو وكيله) التأكد من أن PFI يحتفظ ويحمي جميع مسودات التقرير (التقارير) الجنائي المتعلقة بحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، وبناءً على طلب مشغل شبكة الدفع المحلية، يجب عليه أن يقدم على الفور إلى مشغل شبكة الدفع المحلية أي مسودة من هذا القبيل. ويجب أن يلتزم PFI بدليل برنامج (PCI SSC) PFI لأنه يتعلق بمنتجات العمل التي ينتجها PFI.

قد يطلب مشغل شبكة الدفع المحلية من العضو التسبب في قيام PFI بإجراء تحليل فجوة PCI وإدراج نتيجة هذا التحليل في التقرير الجنائي النهائي.

The Member must direct the PFI to submit a copy of the preliminary and final forensic reports to the National Scheme Operator immediately upon completion.

6.5.3.6 Alternative Standards Applicable to Certain Merchants or Other Agents

In the event of an Account Data Compromise Event or Potential Account Data Compromise Event (for purposes of this Rule, an “Event”) for which the subject is a Level 2, Level 3, or Level 4 Merchant, in lieu of complying with the responsible Member obligations set forth in Rule 6.5.3.3, the first bullet point of Rule 6.5.3.4, and Rule 6.5.3.5, a responsible Member may comply with the Standards set forth in this Rule provided all of the following criteria are satisfied:

Criterion A

The National Scheme Operator determines that fewer than 30,000 Accounts are potentially at risk of unauthorized disclosure as a result of the Event; and

Criterion B

The National Scheme Operator determines that the Merchant (or other Agent) has not been the subject of an Account Data Compromise Event or Potential Account Data Compromise Event for the thirty-six (36) consecutive months immediately preceding the date that the National Scheme Operator determines likely to be the earliest possible date of the Event; and

Criterion C

The responsible Member determines that the Merchant (or other Agent) uses a payment acceptance system that does not share connectivity with another Merchant (or Agent) or Merchant’s (or Agent’s) system and that is not operated by a Service Provider.

Should the National Scheme Operator determine that the subject of the Event is a Level 2, 3, or 4 Merchant and that Criteria A and B, above, are satisfied, the National Scheme Operator will provide notice to the responsible Member by way of an email message to the responsible Member’s Security Contact.

Upon receipt of such notice, the responsible Member may elect to cause a PFI to conduct an examination of the Merchant or other Agent. Should the responsible Member cause a PFI to conduct an examination, the responsible Member must notify the National Scheme Operator within 24 hours of the engagement of the PFI.

Failure to notify the National Scheme Operator within the 24-hour time frame may result in a noncompliance assessment. Alternatively, and provided the responsible Member determines that Criterion C is satisfied, the responsible Member itself may elect to investigate the Event in lieu of causing a PFI to conduct an examination of the Merchant or other Agent.

If the responsible Member itself elects to conduct the investigation, not later than twenty (20) business days following the date of the notice by the National Scheme Operator described above, the responsible Member must provide to the National Scheme Operator a written certification by an officer of the responsible Member certifying that all of the following are true:

يجب على العضو توجيه PFI لتقديم نسخة من التقارير الجنائية الأولية، والنهائية إلى مشغل شبكة الدفع المحلية فور الانتهاء منها.

6.5.3.6 المعايير البديلة المطبقة على تجار معينين أو وكلاء آخرين

في حالات مساومة في بيانات الحساب، أو احتمال حالات مساومة بيانات الحساب (لأغراض تطبيق هذه القاعدة، “حدث”) يكون الموضوع فيه هو تاجرًا من المستوى 2 أو المستوى 3 أو المستوى 4 ، بدلاً من الامتثال لالتزامات العضو المسؤول المنصوص عليها في القاعدة 6.5.3.3 ، النقطة الأولى من القاعدة 6.5.3.4 ، والقاعدة 6.5.3.5، ويجوز للعضو المسؤول الامتثال للمعايير المنصوص عليها في هذه القاعدة شريطة استيفاء جميع المعايير التالية:

المعيار (أ)

يقرر مشغل شبكة الدفع المحلية أن أقل من 30000 حساب معرضة لخطر الكشف غير المصرح به نتيجة للحدث.

المعيار (ب)

يقرر مشغل شبكة الدفع المحلية أن التاجر (أو أي وكيل آخر) لم يكن محلاً لحدوث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب لستة وثلاثين (36) شهرًا متتاليًا، يسبق مباشرة التاريخ الذي يحدده مشغل شبكة الدفع المحلية من المحتمل أن يكون أقرب تاريخ ممكن للحدث.

المعيار (ج)

يقرر العضو المسؤول أن التاجر (أو أي وكيل آخر) يستخدم نظام قبول الدفع لا يشارك الاتصال مع تاجر آخر (أو وكيله) أو نظام التاجر (أو وكيله) ولا يتم تشغيله من قبل مقدم الخدمة.

إذا قرر مشغل شبكة الدفع المحلية أن موضوع الحدث هو تاجر من المستوى 2 أو 3 أو 4 وأن المعايير أ و ب أعلاه مستوفاة، فإن مشغل شبكة الدفع المحلية سيقدم إخطارًا إلى العضو المسؤول عن طريق رسالة بريد إلكتروني إلى جهة الاتصال الخاصة بالعضو المسؤول.

عند استلام مثل هذا الإخطار، يجوز للعضو المسؤول أن يسبب PFI في إجراء فحص للتاجر أو أي وكيل آخر. وإذا تسبب العضو المسؤول في PFI لإجراء فحص، فيجب على العضو المسؤول إخطار مشغل شبكة الدفع المحلية خلال 24 ساعة من مشاركة PFI.

قد يؤدي عدم إخطار مشغل شبكة الدفع المحلية خلال 24 ساعة إلى تقييم عدم الامتثال. بدلاً من ذلك، شريطة أن يقرر العضو المسؤول أن المعيار ج مستوفى، ويجوز للعضو المسؤول نفسه أن يختار التحقيق في الحدث بدلاً من التسبب في قيام PFI بإجراء فحص للتاجر أو أي وكيل آخر.

إذا اختار العضو المسؤول نفسه إجراء التحقيق، في موعد لا يتجاوز عشرين (20) يوم عمل بعد تاريخ الإخطار من قبل مشغل شبكة الدفع المحلية الموضح أعلاه، يجب على العضو المسؤول أن يقدم لمشغل شبكة الدفع المحلية شهادة مكتوبة من قبل مسؤول من العضو المسؤول يشهد على صحة جميع ما يلي:

- The responsible Member elected to investigate the Account Data Compromise Event or Potential Account Data Compromise Event in lieu of causing a PFI to investigate the Account Data Compromise Event or Potential Account Data Compromise Event; and
- The Merchant (or other Agent) that is the subject of the Account Data Compromise Event or Potential Account Data Compromise Event does not use a computer-based acceptance system that is used by another Merchant (or Agent) or Merchants (or Agents); and
- The responsible Member's investigation of the Account Data Compromise Event or Potential Account Data Compromise Event has been completed and the Account Data Compromise Event or Potential Account Data Compromise Event has been fully contained.

Documentation satisfactory to the National Scheme Operator confirming such containment (including the date of containment) and a written explanation of how the security breach was contained (including the steps taken to ensure that Account data are no longer at risk of compromise) must be provided to the National Scheme Operator with the officer certification; and

- The Merchant has newly validated or revalidated compliance with the PCI DSS.

Documentation confirming such validation or revalidation must be provided to the National Scheme Operator with the officer certification.

Failure to comply with any obligation of the responsible Member may result in the imposition of a noncompliance assessment.

The National Scheme Operator may conduct periodic reviews of an Account Data Compromise Event or Potential Account Data Compromise Event investigated by the responsible Member to confirm that the Event has been fully contained.

Should the National Scheme Operator determine that an Event certified by an officer of the responsible Member as fully contained continues to place Accounts at risk of unauthorized disclosure, the National Scheme Operator will provide notice to the responsible Member by way of an email message to the responsible Member's Security Contact.

Within ten (10) business days of such notice, the responsible Member must provide to the National Scheme Operator a remediation action plan describing the steps (and relevant dates of the steps) that the responsible Member will take to ensure that Account data are no longer at risk of compromise. Failure to provide the National Scheme Operator with the remediation action plan within the 10-day time frame may result in a noncompliance assessment.

Within twenty (20) business days after the National Scheme Operator provides approval of the responsible Member's remediation action plan, the responsible Member must implement all required steps of the action plan, including but not limited to officer certification to the National Scheme Operator that such remediation action plan has taken effect. Failure to implement the remediation action plan to the satisfaction of the National Scheme Operator within the 20-day time frame may result in a noncompliance assessment.

- العضو المسؤول المختار للتحقيق في حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق بيانات الحساب، بدلاً من التسبب في قيام PFI بالتحقيق في حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق بيانات الحساب.

- لا يستخدم التاجر (أو أي وكيل آخر) موضوع حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق بيانات الحساب، نظام قبول قائم على الكمبيوتر يستخدمه تاجر آخر (أو وكيل) أو تاجر (أو وكلاء).
- اكتمال تحقيق العضو المسؤول في حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، وتمت معالجة حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب بالكامل.

يجب أن تكون المستندات المقدمة مقبولة من مشغل شبكة الدفع المحلية، وتؤكد مثل هذه المعالجة (بما في ذلك تاريخ الاحتواء) وشرح مكتوب لكيفية معالجة الخرق الأمني (بما في ذلك الخطوات المتخذة لضمان عدم تعرض بيانات الحساب لخطر الاختراق) إلى مشغل شبكة الدفع المحلية مع شهادة المسؤول.

- قيام التاجر بالتحقق من صحة أو إعادة التحقق من التوافق مع PCI DSS.

يجب تقديم المستندات التي تؤكد هذا التحقق أو إعادة التحقق إلى مشغل شبكة الدفع المحلية مع شهادة المسؤول.

قد يؤدي عدم الامتثال لأي التزام من العضو المسؤول إلى فرض تقييم عدم الامتثال.

يجوز لمشغل شبكة الدفع المحلية إجراء مراجعات دورية لحدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب الذي يحقق فيه العضو المسؤول للتأكد من احتواء الحدث بالكامل.

إذا قرر مشغل شبكة الدفع المحلية أن حدثًا معتمدًا من قبل مسؤول من العضو المسؤول كما هو وارد بالكامل يستمر في تعريض الحسابات لخطر الكشف غير المصرح به، فسوف يقدم مشغل شبكة الدفع المحلية إخطاراً إلى العضو المسؤول عن طريق رسالة بريد إلكتروني إلى جهة الاتصال الأمانة الخاصة بالعضو المسؤول.

خلال عشرة (10) أيام عمل من هذا الإخطار، يجب على العضو المسؤول أن يقدم لمشغل شبكة الدفع المحلية خطة عمل علاجية تحدد الخطوات (والتواريخ ذات الصلة بالخطوات) التي سيتخذها العضو المسؤول لضمان أن بيانات الحساب لم تعد متعرضة لخطر اختراق. قد يؤدي عدم تزويد مشغل شبكة الدفع المحلية بخطة العمل العلاجية خلال 10 أيام إلى تقييم عدم الامتثال.

خلال عشرين (20) يوم عمل بعد تقديم مشغل شبكة الدفع المحلية لموافقته على خطة العمل العلاجية الخاصة بالعضو المسؤول، يجب على العضو المسؤول تنفيذ جميع الخطوات المنصوص عليها في هذه الخطة، بما في ذلك على سبيل المثال، شهادة المسؤول لمشغل شبكة الدفع المحلية بأن خطة العمل العلاجية هذه سارية المفعول. قد يؤدي عدم تنفيذ خطة العمل العلاجية طبقاً لما يقرره مشغل شبكة الدفع المحلية خلال 20 يومًا إلى تقييم عدم الامتثال.

If the Merchant (or Agent) that was the subject of an Account Data Compromise Event or Potential Account Data Compromise Event investigated by the responsible Member is the subject of a different Event within thirty-six (36) months of the date on which the National Scheme Operator provided notice to the responsible Member of the initial Event, the National Scheme Operator:

- Will require the responsible Member to engage the services of a PFI to conduct an independent examination of the Merchant or other Agent; and
- May impose an assessment of up to LYD XXXX upon the responsible Member for failure to safeguard Account data.

Except as specifically set forth in this Rule, all other National Scheme Operator and Member rights and obligations with respect to an Account Data Compromise Event or Potential Account Data Compromise Event shall continue with respect to any Account Data Compromise Event or Potential Account Data Compromise Event that a responsible Member itself elects to investigate in accordance with this Rule. Further, and for the avoidance of doubt, the National Scheme Operator has a right at any time to require a responsible Member to cause a PFI to conduct a forensic examination of a Merchant notwithstanding the provisions of this Rule.

6.5.3.7 Determination of Account Data Compromise Event or Potential Account Data Compromise Event

The National Scheme Operator will evaluate the totality of known circumstances, including but not limited to the following, to determine whether or not an occurrence constitutes an Account Data Compromise Event or Potential Account Data Compromise Event:

- a Member or its Agent acknowledges or confirms the occurrence of an Account Data Compromise Event or Potential Account Data Compromise Event;
- any PFI report; or
- any information determined by the National Scheme Operator to be sufficiently reliable at the time of receipt.

6.5.3.8 Assessments for PCI Violations in Connection with Account Data Compromise Events

Based on the totality of known circumstances surrounding an Account Data Compromise Event or Potential Account Data Compromise Event, including the knowledge and intent of the responsible Member, the National Scheme Operator (in addition to any assessments provided for elsewhere in the Standards) may assess a responsible Member up to LYD XXXX for each violation of a requirement of the PCI SSC.

6.5.3.9 Potential Reduction of Financial Responsibility

Notwithstanding a determination by the National Scheme Operator that an Account Data Compromise Event occurred, the National Scheme Operator may consider any actions taken by the compromised entity to establish, implement, and maintain procedures and support best practices to safeguard Account data prior to, during, and after the Account Data Compromise Event or Potential Account Data Compromise Event, in order to relieve, partially or fully, an otherwise responsible Member of responsibility for any assessments, Account Data Compromise operational reimbursement, and/or investigative costs.

إذا كان التاجر (أو الوكيل) الذي كان موضوع حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق بيانات الحساب الذي حقق فيه العضو المسؤول، موضوع حدث مختلف خلال ستة وثلاثين (36) شهرًا من التاريخ الذي قدم فيه مشغل شبكة الدفع المحلية إخطارًا إلى العضو المسؤول عن هذا الحدث المبدئي، في هذه الحالة فإن مشغل شبكة الدفع المحلية قد يقوم بالخطوات التالية:

- سيتطلب من العضو المسؤول الاستعانة بخدمات PFI لإجراء فحص مستقل للتاجر أو وكيله.
- قد يفرض تقييماً يصل إلى XXXX دينار ليبي على العضو المسؤول عن الأهمال في حماية بيانات الحساب.

وباستثناء ما هو منصوص عليه على وجه التحديد في هذه القاعدة، فإن جميع حقوق والتزامات مشغل شبكة الدفع المحلية والأعضاء الآخرين فيما يتعلق بحدث اختراق في بيانات الحساب، أو احتمال حدوث اختراق بيانات الحساب، يجب أن تستمر فيما يتعلق بأي حدث اختراق في بيانات الحساب، أو احتمال حدوث اختراق بيانات الحساب، الذي يختار العضو المسؤول نفسه التحقيق فيه وفقاً لهذه القاعدة. علاوة على ذلك، ولتجنب الشك، يحق لمشغل شبكة الدفع المحلية في أي وقت أن يطلب من عضو مسؤول أن يسبب PFI في إجراء فحص جنائي للتاجر، وبغض النظر عن أحكام هذه القاعدة.

7.3.5.6 تحديد حدث حالات المساومة في بيانات الحساب، أو بيانات الحساب المحتمل

سيقوم مشغل شبكة الدفع المحلية بتقييم جميع الظروف المعروفة، لتحديد ما إذا كان الحدث يمثل حالات مساومة في بيانات الحساب، أو احتمال مساومة في بيانات الحساب، أم لا:

- يقر العضو أو وكيله، بوقوع حالات مساومة في بيانات الحساب، أو احتمال حالات مساومة في بيانات الحساب.
- أي تقرير PFI .
- أي معلومات يحددها مشغل شبكة الدفع المحلية لتكون موثوقة بدرجة كافية وقت الاستلام.

8.3.5.6 تقييمات لانتهاكات PCI فيما يتعلق بحالات المساومة في بيانات الحساب

استنادًا إلى جميع الظروف المعروفة، والمحيطه بحالات المساومة في بيانات الحساب، أو احتمال حدوث اختراق في بيانات الحساب، بما في ذلك معرفة العضو المسؤول ووكيله، فإنه يجوز لمشغل شبكة الدفع المحلية (بالإضافة إلى أي تقييمات منصوص عليها في مكان آخر في المعايير) تقييم عضو مسؤول حتى XXXX دينار ليبي عن كل انتهاك لأحد متطلبات PCI SSC.

9.3.5.6. الأتعاف من المسؤولية المالية

بصرف النظر عن قرار مشغل شبكة الدفع المحلية بحدوث حدث اختراق في بيانات الحساب، يجوز لمشغل شبكة الدفع المحلية الوطني النظر في أي إجراءات يتخذها الكيان المخترق لإنشاء وتنفيذ والحفاظ على الإجراءات ودعم أفضل الممارسات لحماية بيانات الحساب قبل وأثناء وبعد حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، من أجل إعفاء العضو المسؤول جزئيًا، أو كليًا من المسؤولية عن أي تقييمات و تسديد التكاليف التشغيلية لخرق بيانات الحساب و/أو تكاليف التحقيق.

6.5.3.10 Account Data Compromise Operational Reimbursement

Account Data Compromise operational reimbursement (OR) enables an Issuer to partially recover costs incurred in reissuing Cards and for enhanced monitoring of compromised and/or potentially compromised Accounts associated with an Account Data Compromise Event. The National Scheme Operator determines Account Data Compromise operational reimbursement.

The National Scheme Operator may invoke OR for an Account Data Compromise Event impacting 30,000 Accounts or more on a calendar year basis.

For purposes of this Rule, the National Scheme Operator generally deems an Account Data Compromise Event to occur in the year in which the National Scheme Operator publishes an initial Account Data Compromise Alert to impacted Issuers concerning the Account Data Compromise Event.

Following the conclusion of an investigation, the OR liability, if any, will be disclosed to the responsible Member(s) in a final financial liability letter. The responsible Member(s) has 30 days following the date of the final financial liability letter to appeal the liability. If after the conclusion of any appeal, the National Scheme Operator determines that the responsible Member has any financial liability related to the Account Data Compromise Event, the responsible Member may either agree to or refuse to agree to the determined amount.

In the event that the compromised entity is:

- an electronic commerce (e-commerce) Merchant and only the Cardholder name, PAN, expiration date, and/or the CVV 2 data were compromised, only partial Account Data Compromise operational reimbursement will be invoked; or
- a Terminal Servicer and only the Cardholder name, PAN, expiration date, and/or the CVV 2 data were compromised, only partial Account Data Compromise operational reimbursement will be invoked.

With regard to any particular Account Data Compromise Event, the National Scheme Operator has no obligation to disburse an amount in excess of the amount that the National Scheme Operator actually and finally collects from the responsible Member. In that regard, (i) any such amount actually and finally charged to a responsible Member with respect to a particular Account Data Compromise Event is determined by the National Scheme Operator following the full and final resolution of any claim asserted against the National Scheme Operator that arises from or is related to that Account Data Compromise Event; and (ii) any funds disbursed by the National Scheme Operator to a Member as Account Data Compromise operational reimbursement is disbursed conditionally and subject to “claw back” until any claim and all claims asserted against the National Scheme Operator that arise from or are related to the Account Data Compromise Event are fully and finally resolved.

In the administration of the Account Data Compromise OR programs, the National Scheme Operator may determine the responsible Member’s financial responsibility with respect to an Account Data Compromise Event. When determining financial responsibility, the National Scheme Operator may take into consideration the compromised entity’s PCI level, annual sales volume, and the factors set forth in Rule 6.5.3.9. The annual sales volume is derived from the Merchant’s clearing Transactions processed during the previous calendar year.

10.3.5.6. السداد التشغيلي لمساومة بيانات الحساب

يُمكن السداد التشغيلي لمساومة في بيانات الحساب جهة الإصدار من استرداد التكاليف المتكبدة في إعادة إصدار البطاقات جزئياً، ولتحسين المراقبة للحسابات المُخرقة، أو التي يُحتمل أن تتعرض للاختراق، والمرتبطة بحدث اختراق في بيانات الحساب. ويحدد مشغل شبكة الدفع المحلية السداد التشغيلي لاختراق في بيانات الحساب.

يجوز لمشغل شبكة الدفع المحلية اللجوء للسداد التشغيلي لحدث اختراق في بيانات الحساب الذي يؤثر على 30000 حساب أو أكثر على أساس السنة التقويمية.

لأغراض تطبيق هذه القاعدة، يعتبر مشغل شبكة الدفع المحلية، بشكل عام، أن حدث اختراق في بيانات الحساب سيحدث في السنة الذي ينشر فيها مشغل شبكة الدفع المحلية تنبيهاً أولياً بشأن اختراق في بيانات الحساب لجهات الإصدار المتأثرة فيما يتعلق بحدث اختراق في بيانات الحساب.

بعد الانتهاء من التحقيق، سيتم الكشف عن مسؤولية السداد التشغيلية، إن وجدت، للعضو (الأعضاء) المسؤول في خطاب المسؤولية المالية النهائي. ويمنح العضو (الأعضاء) المسؤول 30 يومًا من تاريخ خطاب المسؤولية المالية النهائي لاستئناف المسؤولية. وإذا قرر مشغل شبكة الدفع المحلية، بعد الانتهاء من الاستئناف، يتحمل العضو المسؤول المسؤولية المالية التي تتعلق بحدث اختراق في بيانات الحساب، ويجوز للعضو المسؤول إما الموافقة على المبلغ المحدد، أو رفض الموافقة عليه.

في حالة كون الكيان المخترق:

- كان تاجراً يمارس التجارة إلكترونية (تجارة إلكترونية)، واسم حامل البطاقة ورقم الحساب الأساسي وتاريخ انتهاء الصلاحية و/أو بيانات (CVV 2) فقط ، سيتم استدعاء السداد التشغيلي الجزئي لاختراق في بيانات الحساب.
- إذا تم اختراق الخدمة الطرفية، واسم حامل البطاقة ورقم الحساب الشخصي وتاريخ انتهاء الصلاحية و/أو بيانات CVV 2 فقط ، وسيتم استدعاء السداد التشغيلي الجزئي لاختراق بيانات الحساب.

فيما يتعلق بحدث اختراق في بيانات الحساب المعين، لا يلتزم مشغل شبكة الدفع المحلية بصرف مبلغ يزيد عن المبلغ الذي يجمعه مشغل شبكة الدفع المحلية فعلياً ونهائياً من العضو المسؤول. في هذا الصدد (1) أي مبلغ يتم تحميله فعلياً ونهائياً على العضو المسؤول فيما يتعلق بحدث اختراق في بيانات حساب معين يتم تحديده بواسطة مشغل شبكة الدفع المحلية بعد الحل الكامل والنهائي لأي مطالبة تم تأكيدها ضد مشغل شبكة الدفع المحلية، والتي ينشأ من، أو يرتبط بحدث اختراق في بيانات هذا الحساب (2) أي أموال يصرفها مشغل شبكة الدفع المحلية لعضو ما على أنها سداد تشغيلي لاختراق في بيانات الحساب، تصرف بشكل مشروط، ويخضع “لاسترداد” المطالبات المؤكدة ضد مشغل شبكة الدفع المحلية التي تتعلق بحدث اختراق في بيانات الحساب تم حلها بشكل كامل ونهائي.

في إدارة برامج السداد التشغيلي لاختراق في بيانات الحساب، يجوز لمشغل شبكة الدفع المحلية تحديد المسؤولية المالية للعضو المسؤول فيما يتعلق بحدث اختراق في بيانات الحساب. عند تحديد المسؤولية المالية ، يجوز لمشغل شبكة الدفع المحلية أن يأخذ في الاعتبار مستوى PCI للكيان المخترق، وحجم المبيعات السنوية والعوامل المنصوص عليها في القاعدة 6.5.3.9. حجم المبيعات السنوية مشتق من معاملات المقاصة الخاصة بالتاجر التي تمت معالجتها خلال السنة التقويمية السابقة.

Transactions that are not processed by the National Scheme Operator will be included in the annual sales volume if such data is available. In the event that the Merchant's annual sales volume is not known, the National Scheme Operator will use the Merchant's existing sales volume to project the annual sales volume or request said volume from the responsible Member.

Determination of Operational Reimbursement (OR)

The National Scheme Operator generally determines OR in accordance with the following steps. The National Scheme Operator reserves the right to determine OR by an alternative means if it determines that information needed to use the following steps is not readily available.

1. The National Scheme Operator determines the number of at-risk Accounts per Issuer ICA number by type of Card. Accounts that have been disclosed in a previous Account Data Compromise Alert in connection with a different Account Data Compromise Event within 180 days prior to the publication of the Account Data Compromise Alert for the Account Data Compromise Event under review will be excluded from the calculation. At-risk magnetic stripe-only Card Accounts (i.e., non-EMV chip Card Accounts) will be excluded from the calculation as well.
2. The National Scheme Operator multiplies the number of at-risk Accounts by an amount fixed by the National Scheme Operator from time to time.
3. From the results of Steps 1 and 2, the National Scheme Operator may subtract a fixed deductible, to account for Card expirations and Card re-issuance cycles.

6.5.3.11 Assessments and/or Disqualification for Noncompliance

If the Member fails to comply with the procedures set forth in this Rule, the National Scheme Operator may impose an assessment of up to LYD XXXX a day for each day that the Member is noncompliant and/or disqualify the Member from participating as a recipient of Account Data Compromise operational reimbursement disbursements, whether such disbursements are made in connection with the subject Account Data Compromise Event or any other Account Data Compromise Event, from the date that the National Scheme Operator provides the member with written notice of such disqualification until the National Scheme Operator determines that the Member has resolved all compliance issues.

6.5.3.12 Final Financial Responsibility Determination

Upon completion of its investigation, if the National Scheme Operator determines that a Member bears financial responsibility for an Account Data Compromise Event or Potential Account Data Compromise Event, the National Scheme Operator will notify the responsible Member of such determination and, either contemporaneous with such notification or thereafter, specify the amount of the Member's financial responsibility for the Account Data Compromise Event or Potential Account Data Compromise Event.

The responsible Member has thirty (30) calendar days from the date of such notification of the amount of the Member's financial responsibility to submit a written appeal to the National Scheme Operator, together with any documentation and/or other information that the Member wishes the National Scheme Operator to consider in connection with the appeal. Only an appeal that both contends that the National Scheme Operator financial responsibility determination was not in accordance with the Standards and specifies with particularity the basis for such contention will be considered. The National Scheme Operator will assess a non-refundable LYD XXX fee to consider and act on a request for review of an appeal.

وسيتم تضمين المعاملات التي لم تتم معالجتها بواسطة مشغل شبكة الدفع المحلية في حجم المبيعات السنوية إذا كانت هذه البيانات متوفرة، وفي حالة عدم معرفة حجم المبيعات السنوية للتاجر، سيستخدم مشغل شبكة الدفع المحلية حجم مبيعات التاجر الحالية، لتوقع حجم المبيعات السنوية، أو طلب الحجم المذكور من العضو المسؤول.

تحديد السداد التشغيلي

يحتفظ مشغل شبكة الدفع المحلية بالسلطة التقديرية في تحديد السداد التشغيلي بأي وسيلة، فله اختيار وسيلة بديلة إذا قرر أن المعلومات اللازمة لاستخدام الخطوات العامة التالية غير متاحة بسهولة.

1. يحدد مشغل شبكة الدفع المحلية عدد الحسابات المعرضة للخطر لكل رقم ICA لجهة الإصدار حسب نوع البطاقة. وسيتم استبعاد الحسابات التي تم الكشف عنها في تنبيه سابق باختراق في بيانات الحساب فيما يتعلق بحدث اختراق في بيانات الحساب المختلف، خلال 180 يومًا قبل نشر تنبيه اختراق في بيانات الحساب، لحدث اختراق في بيانات الحساب قيد المراجعة من الحساب. وسيتم أيضاً، استبعاد حسابات البطاقات ذات الشريط المغناطيسي فقط المعرضة للخطر (على سبيل المثال ، حسابات بطاقات الشريحة (EMV) من الحساب أيضاً.
2. يقوم مشغل شبكة الدفع المحلية، بالعملية الحسابية التالية: ضرب عدد الحسابات المعرضة للخطر، بمقدار يحدده مشغل شبكة الدفع المحلية من وقت لآخر.
3. من نتائج الخطوات 1 و 2 ، يجوز لمشغل شبكة الدفع المحلية طرح خصم ثابت، لحساب انتهاء صلاحية البطاقة ودورات إعادة إصدار البطاقة.

6.11.3.5.6. التقييمات، و عدم الأهلية لعدم الامتثال

إذا فشل العضو في الامتثال للإجراءات المنصوص عليها في هذه القاعدة، يجوز لمشغل شبكة الدفع المحلية فرض تقييم يصل إلى XXXX دينارليبي ليوم واحد، لكل يوم يكون فيه العضو غير ممتثل و/أو يستبعد العضو من المشاركة كمستلم مدفوعات السداد التشغيلية لاختراق في بيانات الحساب، سواء تم إجراء هذه المدفوعات فيما يتعلق بحدث اختراق في بيانات الحساب أو أي حدث آخر لاختراق في بيانات الحساب، فمن التاريخ الذي يقدم فيه مشغل شبكة الدفع المحلية للعضو إخطاراً كتابياً بهذا الاستبعاد، حتى يقرر مشغل شبكة الدفع المحلية أن العضو قد عالج جميع مشاكل الامتثال.

6.12.3.5.6. تحديد المسؤولية المالية النهائية

بعد الانتهاء من التحقيق، إذا قرر مشغل شبكة الدفع المحلية أن أحد الأعضاء يتحمل المسؤولية المالية عن حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب، فإنه يلتزم بإخطار العضو المسؤول بهذا القرار، وإما بالتزامن مع هذا الإخطار أو بعد ذلك، وتحديد مقدار المسؤولية المالية للعضو عن حدث اختراق في بيانات الحساب، أو احتمال حدث اختراق في بيانات الحساب.

يستطيع العضو المسؤول خلال ثلاثون (30) يومًا تقويميًا من تاريخ هذا الإخطار بمبلغ المسؤولية المالية، التقديم باستئناف مكتوب إلى مشغل شبكة الدفع المحلية، مرفقاً بالمستندات والمعلومات التي يرغب العضو في أن يراعيها مشغل شبكة الدفع المحلية فيما يتعلق بالاستئناف. وسيتم النظر في هذا الاستئناف، والذي يتضمن بشكل خاص أساس هذا الخلاف في تطبيق المعايير، ويقوم مشغل شبكة الدفع المحلية بفرض رسوم XXXX دينار ليبي غير القابلة للاسترداد للنظر في طلب مراجعة الاستئناف.

If the appeal is timely and meets these criteria, the National Scheme Operator will consider the appeal and the documentation and/or other information submitted therewith in determining whether or not the National Scheme Operator final financial responsibility determination was made in accordance with the Standards. An appeal that is not timely or does not meet these criteria will not be considered.

The National Scheme Operator decision with respect to an appeal is final and there are no additional internal appeal rights.

After reviewing the appeal, the National Scheme Operator will notify the responsible Member of the appeal decision. If the National Scheme Operator denies or does not act on the appeal, the National Scheme Operator will debit the responsible Member's billing account on the date specified in the appeal decision notification letter.

This section does not relieve a Member of any responsibility set forth in this Book, including the responsibility to submit to the National Scheme Operator on a continuing basis throughout the pendency of the National Scheme Operator investigation the information required by those sections. If the National Scheme Operator determines that a Member knew or should have known with reasonable diligence of documents or other information that the Member was required to submit to the National Scheme Operator during the pendency of the National Scheme Operator investigation, but failed to do so, such documents or other information will not be considered by the National Scheme Operator in deciding the appeal.

6.6 Fraud Reporting Standards

For the benefit of all Members, the National Scheme Operator analyzes the data and produces statistics relating to the fraudulent use of Accounts and all chargebacks that originate from Transactions using Accounts with a fraud status.

Reporting by Issuers

An Issuer must submit all fraudulent Transactions on its Accounts to the Fraud and Loss Database on a monthly basis, regardless of whether the Issuer has or expects to recover losses through chargebacks, compliance cases, restitution, insurance, or any other means. Each Issuer must ensure that the Transaction information submitted to the National Scheme Operator is accurate and delivered within the time frames described in this Book. The National Scheme Operator monitors the Transaction information submitted by Members to ensure data quality.

An Issuer must not report the following Transactions to the Fraud and Loss Database:

- Fraudulent credits (refunds) on an Account
- Authorizations that the Issuer declined due to suspicion of potential fraud
- “Buyer's remorse” or “friendly fraud” Transactions

A “buyer's remorse” or “friendly fraud” Transaction is a Transaction disputed by the Cardholder as fraudulent, but which the Issuer determines was conducted by the Cardholder or a person for whom the Cardholder is financially responsible, and the Cardholder's credentials and Card or Access Device were not lost or stolen. This includes, but is not limited to, situations where:

- The Cardholder was unable to obtain a refund from the Merchant;
- A person, for whom the Cardholder is financially responsible, engaged in the Transaction without the Cardholder's knowledge or consent; or

وإذا كان الاستئناف قد رفع في الوقت المناسب، واستوفي هذه المعايير، فسوف يأخذ مشغل شبكة الدفع المحلية في اعتباره الاستئناف والمستندات والمعلومات الأخرى المرفقة معه، لتحديد ما إذا كان تحديد المسؤولية المالية النهائية لمشغل شبكة الدفع المحلية قد تم وفقًا للمعايير أم لا. و لا يتم النظر في الاستئناف الذي يرفع بعد الميعاد، أو لا يستوفي المعايير.

ويعتبر قرار مشغل شبكة الدفع المحلية عند فصله في الاستئناف، قراراً نهائياً. بعد مراجعة الاستئناف، سيقوم مشغل شبكة الدفع المحلية بإخطار العضو المسؤول بقرار الاستئناف. إذا رفض مشغل شبكة الدفع المحلية الاستئناف، فسيقوم مشغل شبكة الدفع المحلية بالخصم من حساب فواتير العضو المسؤول في التاريخ المحدد في خطاب إخطار قرار الاستئناف.

لا يعفي هذا القسم العضو من أي مسؤولية منصوص عليها في هذا الكتاب، بما في ذلك المسؤولية التقديم إلى مشغل شبكة الدفع المحلية، وعلى أساس مستمر، بالتحقيق في المعلومات المطلوبة من قبل تلك الأقسام. وإذا قرر مشغل شبكة الدفع المحلية أن عضواً يعلم أو كان ينبغي أن يعلم إذا بذل العناية المعقولة بالمستندات أو المعلومات الأخرى التي كان مطلوباً من العضو تقديمها إلى مشغل شبكة الدفع المحلية أثناء فترة التحقيق الخاصة ومشغل شبكة الدفع المحلية، ولكنه فشل في القيام بذلك، فإنه لن يتم النظر في مثل هذه المستندات أو المعلومات الأخرى من قبل مشغل شبكة الدفع المحلية عند البت في الاستئناف.

6.6 معايير الإبلاغ عن الاحتيال

لمصلحة جميع الأعضاء، يقوم مشغل شبكة الدفع المحلية بتحليل البيانات وإصدار إحصائيات تتعلق بالاستخدام الاحتيالي للحسابات، وجميع عمليات رد المبالغ المدفوعة التي تنشأ من المعاملات باستخدام الحسابات ذات طبيعة الاحتيال.

التقارير من قبل جهات الإصدار

يجب على جهة الإصدار إرسال جميع المعاملات الاحتيالية على حساباتها إلى قاعدة بيانات الاحتيال والخسارة على أساس شهري، وبغض النظر عما إذا كانت جهة الإصدار لديها، أو يتوقع استردادها الخسائر من خلال عمليات رد المبالغ المدفوعة أو حالات الامتثال أو الاسترداد أو التأمين أو أي وسيلة أخرى.

يجب على كل جهة إصدار التحقق من أن معلومات المعاملة المقدمة إلى مشغل شبكة الدفع المحلية دقيقة، ويتم تسليمها خلال المدد الزمنية المحددة في هذا الكتاب، ويراقب مشغل شبكة الدفع المحلية المعلومات المتعلقة بالمعاملة المقدمة من الأعضاء لضمان جودة البيانات.

ويجب ألا تقوم جهة الإصدار بالإبلاغ عن المعاملات التالية إلى قاعدة بيانات الاحتيال والخسارة:

- اتسمانات احتيالية (المبالغ المستردة) على الحساب.
- التفويضات التي رفضتها جهة الإصدار بسبب الاشتباه في عملية احتيال محتملة.
- معاملات “ندم المشتري” أو “الاحتيال الودي”.

معاملة “ندم المشتري” أو “الاحتيال الودي” هي معاملة متنازع عليها من قبل حامل البطاقة باعتبارها احتيالية، ولكن تحدد جهة الإصدار أنها تمت من قبل حامل البطاقة، أو شخص يكون حامل البطاقة مسؤولاً عنه مالياً، وبيانات اعتماد حامل البطاقة وبطاقته أو جهاز وصوله لم يضيع أو يُسرق. وهذا يشمل، على سبيل المثال، الحالات التالية:

- لم يتمكن حامل البطاقة من استرداد الأموال من التاجر.
- الشخص الذي يكون حامل البطاقة مسؤولاً مالياً عنه، يشارك في المعاملة دون علم حامل البطاقة أو موافقته.

- The Cardholder is also the Merchant or employed by the Merchant.
- A Transaction determined to be “buyer’s remorse” or “friendly fraud” is considered a Cardholder dispute or credit issue rather than a fraudulent Transaction.

Reporting by Acquirers

An Acquirer receiving a Transaction that cannot be identified by a BIN or Member ID is liable for that Transaction. If it is determined that the Transaction is a fraudulent or counterfeit Transaction, the Acquirer must notify, in writing, the National Scheme Operator of such an occurrence. This notification must include all mandatory information.

6.6.1 Reporting Lost and Stolen Cards

A Member, or a Third Party Processor (TPP) acting as the Member’s or its Sponsor’s authorized agent, that receives a lost or stolen Card report must promptly notify the Issuer of the report. The Member should send the notice by phone and direct it to the Issuer’s Security Contact. If an Issuer requests to receive such notice by another method, then the Member should comply with the Issuer’s request.

The notice must include all relevant available information, such as:

- Member ID of the institution sending the notice
- Issuer’s name
- Cardholder’s Account number
- Cardholder’s name and address
- Phone number and an address where the Cardholder can be reached

If the Member cannot immediately reach the Issuer by phone, the Member must make another attempt at the first opportunity during the Issuer’s normal business hours. Issuers must accept all collect calls placed to report a lost or stolen Card.

NOTE: The Issuer will be responsible for the reasonable costs of transmitting the notice. The Member that receives and transmits the report may submit to the Issuer a request through National Scheme Operator for Fee Collection message with message reason code to collect the LYD XX lost or stolen Card report fee in addition to any transmission costs that it may incur.

If the Account number is unknown, the reporting Member still may use the National Scheme operator system to request Fee Collection message by zero-filling the Account Number field and by providing the Cardholder’s name and address, and the Issuer’s name or service mark, in the Data Text field.

Receipt of Reports by the National Scheme Operator

The National Scheme Operator will help its Members by receiving lost or stolen Card reports, and will (at each Member’s option) either take the report and promptly notify the Issuer or, if the report is by phone, direct the call to the Issuer (when such capability is available). The National Scheme Operator will, only at each Issuer’s request, promptly update the authorization negative file used for Stand-In processing.

The national Scheme Operator may charge the Issuer LYD XX per report in addition to any transmission costs that it may incur for receiving and transmitting the report.

- حامل البطاقة هو نفسه التاجر، أو موظف من قبل التاجر.
- تعتبر المعاملة التي يتم تحديدها على أنها “ندم المشتري” أو “الاحتيال الودي” نزاع حامل البطاقة أو مشكلة ائتمانية، وليست معاملة احتيالية.

التقارير من قبل جهات القبول

جهة القبول التي تتلقي معاملة لا يمكن تحديدها بواسطة رقم التعريف المصرفي، أو معرفّ العضو، فإنها تكون مسؤولاً عن تلك المعاملة. وإذا تم تحديد أن المعاملة هي معاملة احتيالية أو مزورة، فيجب على جهة القبول أن تخطر، كتابيًا، مشغل شبكة الدفع المحلية بهذه الواقعة، ويجب أن يتضمن هذا الإخطار جميع المعلومات الإلزامية.

1.6.6. الإبلاغ عن البطاقات المفقودة والمسروقة

يجب على العضو ، أو معالج الطرف الثالث الذي يتصرف بصفته الوكيل المعتمد للعضو أو الجهة الراعية له، والذي يتلقى تقرير عن البطاقة المفقودة أو المسروقة ، إخطار جهة الإصدار بالتقرير على الفور. ويجب على العضو إرسال الإخطار عبر الهاتف وتوجيهه إلى جهة الاتصال الأمانة لجهة الإصدار. وإذا طلبت جهة الإصدار استلام هذا الإخطار بطريقة أخرى ، فيجب على العضو الامتثال لطلب جهة الإصدار.

يجب أن يتضمن الإخطار جميع المعلومات المتاحة ذات الصلة ، مثل:

- معرف عضو المؤسسة التي ترسل الإخطار.
- اسم جهة الإصدار.
- رقم حساب حامل البطاقة.
- اسم وعنوان حامل البطاقة.
- رقم الهاتف والعنوان الذي يمكن من خلاله الوصول إلى حامل البطاقة.

وإذا لم يتمكن العضو من الوصول إلى جهة الإصدار على الفور عبر الهاتف، فيجب عليه القيام بمحاولة أخرى في أول فرصة ممكنة خلال ساعات العمل العادية لجهة الإصدار. ويجب أن تقبل جهات الإصدار جميع مكالمات التحصيل الموضوعة للإبلاغ عن البطاقة المفقودة أو المسروقة.

ملاحظة: ستكون جهة الإصدار مسؤولة عن التكاليف المعقولة لإرسال الإخطار.

يجوز للعضو الذي يتلقى التقرير وينقله، أن يقدم إلى جهة الإصدار طلبًا عبر رسالة مشغل شبكة الدفع المحلية لتحصيل الرسوم مع رمز سبب الرسالة لتحصيل XX دينار ليبي رسوم تقرير البطاقة المفقودة أو المسروقة بالإضافة إلى تكاليف النقل قد تتكبدها.

وإذا كان رقم الحساب غير معروف، فإنه يجوز للعضو المُبلغ استخدام نظام مشغل شبكة الدفع المحلية لطلب رسالة تحصيل الرسوم بملء حقل رقم الحساب صفرًا، وتقديم اسم وعنوان حامل البطاقة واسم جهة الإصدار أو علامة الخدمة في حقل نص البيانات.

استلام التقارير من قبل مشغل شبكة الدفع المحلية

سيساعد مشغل شبكة الدفع المحلية أعضائه من خلال تلقي تقارير البطاقة المفقودة أو المسروقة، وسيقوم (حسب خيار كل عضو) إما بأخذ التقرير وإخطار جهة الإصدار على الفور، أو إذا كان التقرير عن طريق الهاتف، بتوجيه المكالمات إلى جهة الإصدار (عندما تكون هذه الإمكانية متاحة). وسيقوم مشغل شبكة الدفع المحلية، بناءً على طلب كل جهة إصدار فقط، بتحديث ملف التفويض السلبي المستخدم في المعالجة الاحتياطية على الفور.

ويجوز لمشغل شبكة الدفع المحلية فرض رسوم على جهة الإصدار XX دينار ليبي لكل تقرير بالإضافة إلى تكاليف إرسال قد يتكبدها لاستلام التقرير وإرساله.

6.6.2 Fraud and Loss Database Reporting Requirements

The following reason codes must be used by Issuers to indicate the reason that the Issuer reported a fraudulent Transaction.

Table 6.5—Fraud Type Reason Codes Used by Issuers

(See appendix number 49)

6.6.2.1 Timely Fraud Reporting

POS Transactions

An Issuer must report at least 80% of lost, stolen, never received or issued, and counterfeit card fraud Transactions within 60 days from the Transaction date or 30 days from the Cardholder notification date or 60 days of the first chargeback date, unless the Standards require the Issuer to report the Transaction before a chargeback occurs.

An Issuer must report at least 65% of Card-not-present fraud Transactions within 60 days from the Transaction date or 30 days from the Cardholder notification date or 60 days of the first chargeback date, unless the Standards require the Issuer to report the Transaction before a chargeback occurs.

An Issuer must report fraudulent application, Account takeover, and bust-out collusive Merchant fraud Transactions within 30 days of the Cardholder notification date.

ATM Transactions

An Issuer must report at least 80% of all fraudulent ATM Transactions within 90 days from the date of discovery or 90 days from the Cardholder notification date, whichever occurs first.

Resubmission of Rejected or Suspended Records

An Issuer must correct and resubmit each rejected or suspended record within 60 days of notification.

6.6.2.2 Fraud Reporting Noncompliance

The National Scheme Operator, in its sole discretion, determines whether an Issuer is in compliance with these fraud reporting Standards. An Issuer that fails to timely report fraudulent Transactions is subject to noncompliance assessments.

After the first quarter of noncompliance, the National Scheme Operator will send an Issuer a warning letter (“First Notice”) informing such Issuer that it risks being assessed for noncompliance. The First Notice affords an Issuer the opportunity to remedy the noncompliance issue without being assessed. After two consecutive quarters of noncompliance, the National Scheme Operator will send an Issuer a noncompliance assessment letter (“Final Notice”) describing any applicable assessment amounts.

The National Scheme Operator, at Its”sole’discretion, may grant compliance variance to an Issuer for a limited period of time due to exigent circumstances. Throughout such variance period, said Issuer must take appropriate and timely action to resolve any outstanding noncompliance issues. If an Issuer fails to become compliant by the end of the stated variance period, an assessment may be reinstated for the variance period.

2.6.6. متطلبات الإبلاغ عن قاعدة بيانات الاحتيال والخسارة

يجب استخدام رموز الأسباب التالية من قبل جهات الإصدار للإشارة إلى سبب قيام جهة الإصدار بالإبلاغ عن معاملة احتيالية.

الجدول 6.5 - رموز سبب نوع الاحتيال المستخدمة من قبل جهات الإصدار
(انظر الملحق رقم 49)

1.2.6.6. الإخطار عن الاحتيال في الوقت المناسب

معاملات نقاط البيع

يجب على جهة الإصدار الإبلاغ عن 80% على الأقل من المعاملات المفقودة أو المسروقة أو التي لم يتم استلامها أو إصدارها، ومعاملات تزوير البطاقة خلال 60 يومًا من تاريخ المعاملة، أو 30 يومًا من تاريخ إخطار حامل البطاقة أو 60 يومًا من تاريخ رد المبالغ المدفوعة الأول، ما لم تطالب المعايير جهة الإصدار بالإبلاغ عن المعاملة قبل حدوث عملية رد المبالغ المدفوعة.

يجب على جهة الإصدار الإبلاغ عن 65% على الأقل من معاملات احتيال البطاقة غير الموجودة خلال 60 يومًا من تاريخ المعاملة أو 30 يومًا من تاريخ إخطار حامل البطاقة أو 60 يومًا من تاريخ رد المبالغ المدفوعة الأول، ما لم تطالب المعايير جهة الإصدار بالإخطار عن المعاملة قبل حدوث عملية رد المبالغ المدفوعة.

يجب على جهة الإصدار الإبلاغ عن الطلب الاحتيالي والاستيلاء على الحساب ومعاملات احتيال التاجر المتواطئ خلال 30 يومًا من تاريخ إخطار حامل البطاقة.

معاملات أجهزة الصراف الآلي

يجب على جهة الإصدار الإبلاغ عن 80% على الأقل من جميع معاملات أجهزة الصراف الآلي الاحتيالية خلال 90 يومًا من تاريخ الاكتشاف، أو 90 يومًا من تاريخ إخطار حامل البطاقة، أيهما اسبق. إعادة تقديم السجلات المرفوضة أو المعلقة يجب أن تصح جهة الإصدار كل سجل مرفوض، أو معلق ويعيد تقديمه خلال 60 يومًا من الإخطار.

2.2.6.6. عدم الامتثال للإبلاغ عن الاحتيال

وفقاً لسلطته التقديرية يحدد مشغل شبكة الدفع المحلية، ما إذا كانت جهة الإصدار ملتزمة بمعايير الإبلاغ عن المعاملات الاحتيالية. وجهة الإصدار التي تفشل في الإبلاغ عن المعاملات الاحتيالية في الوقت المناسب تخضع لتقييم عدم الامتثال.

بعد الربع الأول من عدم الامتثال، يرسل مشغل شبكة الدفع المحلية خطاب تحذير لجهة الإصدار (“الإخطار الأول”) لإبلاغها بأنها تخاطر بالتقييم لعدم الامتثال. يمنح الإخطار الأول جهة الإصدار الفرصة لمعالجة مشكلة عدم الامتثال دون أن يتم تقييمه. وبعد ربعين متتاليين من عدم الامتثال، يرسل مشغل شبكة الدفع المحلية إلى جهة الإصدار خطاب تقييم عدم الامتثال (“الإخطار النهائي”) يصف أي مبالغ تقييم قابلة للتطبيق.

وفقاً لسلطته التقديرية يحدد مشغل شبكة الدفع المحلية، قد يمنح تباين في تطبيق معايير الامتثال لأحدى جهات الإصدار لفترة زمنية محدودة بسبب ظروف طارئة. وخلال فترة التباين، يجب على جهة الإصدار المذكورة اتخاذ الإجراءات المناسبة وفي الوقت المناسب لمعالجة المشاكل المتعلقة بعدم الامتثال. وإذا فشلت جهة الإصدار في الالتزام بنهاية فترة التباين المحددة، فقد تتم إعادة التقييم لفترة التباين.

6.6.3 Criminal and Counterfeit Investigations

On request, each Member must provide other Members with reasonable investigative assistance. The investigating Member will be entitled to reimbursement from the requesting Member for both actual expenses and an hourly investigative fee as the National Scheme Operator may establish periodically. Procedures for requesting such assistance follow.

6.6.3.1 Initiating an Investigation

To initiate an investigation, the requesting Member must perform the following steps:

1. Complete part A of the Investigation Request and Report Form
2. Send the appropriate copies of the form to:
 - The Security Contact of the investigating Member, and
 - The National Scheme Operator.

In case of an emergency, the Member may initiate an investigation by phone or other means. However, the request must contain all pertinent information in the Investigation Request and Report Form. The Member must forward the appropriate copies of the form within 36 hours after making the request.

6.6.3.2 Providing a Progress Report

The investigating Member must acknowledge the receipt of the Investigation Request and Report Form within three business days. Within 15 business days of receiving the Investigation Request and Report Form, the investigating Member must furnish a progress report on the results of the investigation. If the investigation cannot be completed within 15 days, the investigating Member should complete the investigation as soon as viable. The investigating Member should use the same Investigation Request and Report Form to summarize the results of an investigation.

The form also serves as an invoice to the requesting Member for the personnel hours and expenses associated with the investigation. The Member conducting the investigation must complete part B of the form and route the copies according to the instructions on the Investigation Request and Report Form.

6.6.3.3 Requesting an Arrest and Criminal Prosecution

When a Member requests that another Member cause the arrest and subsequent criminal prosecution of an individual for misuse of a Card, the requesting Member must supply all necessary witnesses at the various criminal proceedings.

6.6.3.4 Fees and Reimbursement of Expenses

The investigating Member may collect from the requesting Member LYD XX for each half hour of investigative work performed. The Investigation Request and Report Form details all costs and expenses incurred by investigative personnel on behalf of the requesting Member, or the amount specifically authorized by the requesting Member to be used for investigation expenses.

3.6.6 التحقيقات الجنائية والاحتياطية

عند الطلب، يجب على كل عضو بذل الجهد المعقول، لمساعدة الأعضاء الآخرين في إجراءات التحقيق. ويحق للعضو المحقق أن يخصم من العضو الطالب، كل من النفقات الفعلية وأتعاب التحقيق المحسوبة بالساعة، كما قد يحددها مشغل شبكة الدفع المحلية بشكل دوري. فيما يلي إجراءات طلب هذه المساعدة.

1.3.6.6 بدء التحقيق

لبدء التحقيق، يجب على العضو الطالب القيام بالخطوات التالية:

1. استكمال الجزء من طلب التحقيق ونموذج التقرير.
2. إرسال النسخ المناسبة من النموذج إلى:
 - جهة الاتصال الأمنية للعضو المحقق.
 - مشغل شبكة الدفع المحلية.

وفي حالة الطوارئ، يجوز للعضو بدء التحقيق عبر الهاتف أو بأي وسيلة أخرى. ومع ذلك، يجب أن يحتوي الطلب على جميع المعلومات ذات الصلة في طلب التحقيق ونموذج التقرير. ويجب على العضو إرسال النسخ المناسبة من النموذج خلال 36 ساعة بعد تقديم الطلب.

2.3.6.6 تقديم تقرير مرحلي

- يجب أن يقر العضو الذي قام بالتحقيق، أنه قد استلم خلال ثلاثة أيام عمل، طلب التحقيق، ونموذج التقرير.
- يجب على العضو الذي قام بالتحقيق وخلال 15 يوم عمل، من استلام طلب التحقيق، ونموذج التقرير، تقديم تقرير مرحلي عن نتائج التحقيق.
- يجب على العضو، إذا تعذر استكمال التحقيق خلال 15 يومًا، استكمال التحقيق في أقرب وقت ممكن.
- يجب على العضو الذي قام بالتحقيق استخدام نفس طلب التحقيق ونموذج التقرير لتلخيص نتائج التحقيق. ويعمل النموذج أيضًا كفاتورة للعضو الطالب لساعات الموظفين والنفقات المرتبطة بالتحقيق.
- يجب على العضو الذي يجري التحقيق استكمال الجزء (ب) من النموذج، وتوجيه النسخ وفقًا للتعليمات الواردة في طلب التحقيق ونموذج التقرير.

3.3.6.6 طلب التوقيف والملاحقة جنائية

عندما يطلب أحد الأعضاء من عضو آخر، التسبب في توقيف شخص ما، ومقاضاته جنائيًا لاحقًا بسبب إساءة استخدام البطاقة، يجب على العضو الطالب تقديم مايمتلكه الأدلة اللازمة في الإجراءات الجنائية المختلفة.

4.3.6.6 الرسوم واسترداد المصاريف

يجوز للعضو الذي قام بالتحقيق أن يجمع من العضو الطالب XX دينار ليبي عن كل ساعة من ساعات عمل التحقيق الذي يتم إجراؤه. ويجب أن يبين طلب التحقيق ونموذج التقرير جميع التكاليف والنفقات التي يتكبدها المحققون نيابة عن العضو الطالب، أو المبلغ المصرح به تحديدًا من قبل العضو الطالب لاستخدامه في نفقات التحقيق.

When a Member requests that another Member cause the arrest and subsequent criminal prosecution of an individual for misuse of a Card, the requesting Member must pay all related expenses at the various criminal proceedings.

The National Scheme Operator can authorize the expenditure of any funds necessary to conduct a counterfeit or major criminal investigation, including reimbursement of a Member's expenses in any particular case that caused a hardship to that Member. To settle investigation fees and expenses.

6.6.3.5 Investigation of Counterfeits and Major Criminal Cases

The various regional the National Scheme Operator vice presidents of the Franchise Department have the authority to manage the investigation of a counterfeit or criminal case. When requested, Members are required to provide the regional vice president with any assistance necessary.

6.7 Merchant and Agent Screening and Monitoring Standards

This Rule may be of particular interest to Member personnel responsible for verification and monitoring Merchants and Agents.

6.7.1 Screening New Merchants and Agents.

A Member is responsible for verifying that a prospective Merchant or Agent is conducting bona fide business operations by performing these verification procedures.

The performance of these verification procedures does not relieve a Member from the responsibility of following good commercial banking practices. The review of a credit report, an annual report, or an audited statement, for example, might suggest the need for further inquiry, such as additional financial and background checks regarding the business, its principal owners, and officers.

6.7.1.1 Required Screening Procedures

The Acquirer of a prospective Merchant or ATM owner, and any Payment Facilitator of the Acquirer with respect to a prospective Agent, must ensure that the following verification procedures are performed:

- In accordance with the Acquirer's "know your customer" policies and, collect information about the entity and each of its principal owners as necessary or appropriate for identification and due diligence purposes; verify that the information collected is true and accurate; and comply with all NATIONAL DISTRIBUTOR OPERATOR sanction verification requirements; and
- Confirm that the entity is located and conducting legal business in Libya; and
- Ensure that an inquiry is submitted to the Terminated Merchants File with respect to a prospective high-risk Merchant or Agent. If sales will be conducted on a website or digital application, the inquiry must include the uniform resource locator (URL) address. An Acquirer must submit inquiries both for its own Merchants and for the Agents of its Payment Facilitators; and
- Establish fraud loss control measures appropriate for the business to be conducted, including but not limited to Transaction authorization and deposit activity monitoring parameters; and
- Assign a Card acceptor business code (MCC) that most accurately describes the nature of the business.

عندما يطلب أحد الأعضاء من عضو آخر التسبب توقيف شخص ما، ومقاضاته جنائياً لاحقاً بسبب إساءة استخدام البطاقة، ويجب على العضو الطالب دفع جميع النفقات ذات الصلة في الإجراءات الجنائية المختلفة.

لمشغل شبكة الدفع المحلية أن يصرح بإنفاق الأموال التي تعتبر ضرورية لإجراء تحقيق جنائي، بما في ذلك سداد نفقات العضو في حالة معينة تكون قد سببت في مشقة لذلك العضو. لتسوية أتعاب ومصاريف التحقيق.

5.3.6.6 التحقيق في التزوير والقضايا الجنائية الكبرى

يتمتع وكلاء مشغل شبكة الدفع المحلية بحق الإمتياز في المناطق الإقليمية المختلفة بسلطة إدارة التحقيق في قضايا التزوير وغيرها من القضايا الجنائية. وعند الطلب، يتعين على الأعضاء تزويد النائب الإقليمي بالمساعدة الضرورية.

7.6 معايير فحص ومراقبة التاجر والوكيل

قد تكون هذه القاعدة ذات أهمية خاصة للأشخاص الطبيعيين، الأعضاء المسؤولين عن التحقق ومراقبة التجار والوكلاء.

1.7.6 فحص التجار والوكلاء الجدد

العضو مسؤول عن التحقق من قيام التاجر أو الوكيل المحتمل بإجراء عمليات تجارية بحسن نية من خلال تنفيذ إجراءات التحقق.

إن تنفيذ الإجراءات المتعلقة بالتحقق لا يعفي العضو من مسؤولية اتباع الممارسات المصرفية التجارية الجيدة. وقد تشير مراجعة تقرير الائتمان أو التقرير السنوي أو البيان المدقق، على سبيل المثال، إلى الحاجة إلى مزيد من التحقيق، مثل الفحوصات المالية الإضافية، والخلفية المتعلقة بالعمل التجاري ومالكها الرئيسيين والمسؤولين.

1.1.7.6 إجراءات الفحص المطلوبة

يجب على جهة القبول (التاجر المحتمل) أو مالك جهاز الصراف الآلي، وأي ميسر دفع تابع لجهة القبول فيما يتعلق بالوكيل المحتمل، التحقق من تنفيذ إجراءات التحقق التالية:

- وفقاً لسياسات "اعرف عميلك" لدى جهة القبول، وجمع المعلومات حول الكيان وكل من مالكيها الرئيسيين حسب الضرورة أو المناسبة لأغراض التحديد والعناية الواجبة؛ التحقق من أن المعلومات التي تم جمعها صحيحة ودقيقة؛ والامتنال لجميع متطلبات التحقق من جزاءات مشغل شبكة الدفع المحلية.
- التحقق من أن الكيان موجود ويقوم بأعمال قانونية في ليبيا.
- تأكد من إرسال التحقيق إلى ملف التجار الذين تم إنهاء خدمتهم فيما يتعلق بالتاجر أو الوكيل المحتمل عالي الخطورة. وفي حالة إجراء المبيعات على موقع أو تطبيق رقمي، يجب أن يتضمن التحقيق عنوان محدد موقع الموارد الموحد. ويجب على جهة القبول تقديم تحقيقات لكل من تجاره و التجار ووكلاء ميسري الدفع التابعين له.
- وضع تدابير مكافحة خسائر الاحتيال مناسبة للأعمال التي سيتم إجراؤها، بما في ذلك على سبيل المثال لا الحصر، ترخيص المعاملات ومعايير مراقبة نشاط الإيداع ؛ و
- تعيين رمز عمل تقبل البطاقة (MCC) يصف طبيعة العمل بدقة أكبر.

- For a prospective high-risk negative option billing Merchant or Agent, identify any entity that provides service for the Merchant or Agent that would allow such entity to have access to Account data, and ensure that each such entity is registered with the National Scheme Operator as appropriate.

6.7.1.2 Retention of Investigative Records

The Acquirer must retain all records concerning the investigation of a Merchant, Agent, or ATM owner for a minimum of two years after the date that the Merchant Agreement or Agent Agreement as applicable, is terminated or expires.

Such records may include any of the following, when applicable:

- Signed Merchant or Agent Agreement
- With respect to the verification of a Merchant or Agent, a statement from the Merchant about previous Merchant Agreements, including the names of the entities where the Merchant has or had the agreements and the reasons for terminating the agreements, if applicable
- Corporate or personal banking statements
- Report from a credit bureau, or, if the credit bureau report is incomplete or unavailable, the written results of additional financial and background checks of the business, its principal owners, and officers
- Site inspection report, to include photographs of premises, inventory verification, and the name and signature of the inspector of record
- Merchant or Agent certificate of incorporation, licenses, or permits
- Verification of references, including personal, business, or financial
- Verification of the authenticity of the supplier relationship for the goods or services (invoice records) that a Merchant or Agent is offering the Cardholder for sale
- Date-stamped Terminated Merchant File inquiry and/or addition records, as applicable
- All Member correspondence with the Merchant, Agent, or ATM owner
- All correspondence relating to Issuer, Cardholder, or law enforcement inquiries concerning the Merchant, Agent, ATM owner, or any associated Service Provider
- Signed Service Provider contract, including the name of agents involved in the due diligence process
- Acquirer due diligence records concerning the Service Provider and its agents

NOTE: The National Scheme Operator recommends that the Acquirer retain all records, in the event that the National Scheme Operator conducts an audit as necessary to verify compliance with the verification procedures.

6.7.1.3 Assessments for Noncompliance with Screening Procedures

The National Scheme Operator may audit an Acquirer for compliance with these verification procedures, and each Member must comply with and assist any such audit. The National Scheme Operator will review the applicable records retained by the Acquirer to determine whether an Acquirer has complied with these verification procedures. If the National Scheme Operator determines that an Acquirer has not complied with these verification procedures, and if the Acquirer does not correct all deficiencies that gave rise to the violation to the satisfaction of the National Scheme Operator within 30 days of knowledge

- بالنسبة إلى التاجر أو الوكيل المحتمل لفواتير الخيار السلبي عالي الخطورة، تحديد الكيان الذي يقدم خدمة للتاجر أو الوكيل، من شأنه أن يسمح لمثل هذا الكيان بالوصول إلى بيانات الحساب، والتحقق من أن كل كيان مسجل لدى مشغل شبكة الدفع المحلية باعتباره كيان ملائم.

2.1.7.6. الاحتفاظ بسجلات التحقيق

يجب على جهة القبول أن تحتفظ بجميع السجلات المتعلقة بالتحقيق مع التاجر أو الوكيل أو مالك جهاز الصراف الآلي لمدة لا تقل عن عامين بعد تاريخ إنهاء اتفاقية التاجر أو اتفاقية الوكيل حسب الاقتضاء أو انتهاء صلاحيتها.

وعند الاقتضاء قد تتضمن هذه السجلات مما يلي:

- اتفاقية التاجر أو الوكيل الموقعة.
- فيما يتعلق بالتحقق من التاجر أو الوكيل، بيان من التاجر حول اتفاقيات التاجر السابقة، بما في ذلك أسماء الكيانات التي يمتلك التاجر فيها أو لديه اتفاقيات وأسباب إنهاء الاتفاقيات، إن أمكن ذلك.
- البيانات المصرفية للشركات أو الشخصيات.
- تقرير من مكتب الائتمان، غير أنه إذا كان تقرير مكتب الائتمان غير مكتمل أو غير متوفر، فيجب تقديم تقرير بالنتائج المكتوبة لفحوصات مالية وخلفية إضافية للشركة، ومالكها الرئيسيين، والمسؤولين
- تقرير معاينة الموقع، متضمنًا صورًا للمباني، والتحقق من المخزون، واسم وتوقيع مفتش السجل.
- شهادة التاجر أو الوكيل للتأسيس أو التراخيص أو التصاريح.
- التحقق من المراجع ، بما في ذلك الشخصية أو التجارية أو المالية.
- التحقق من صحة علاقة المورد بالسلع أو الخدمات (سجلات الفواتير) التي يعرضها التاجر أو الوكيل على حامل البطاقة للبيع.
- التحقيق عن ملف التاجر الذي أنتهت العلاقة معه، مختوم بالتاريخ و/أو إضافة السجلات، حسب الاقتضاء.
- جميع مراسلات الأعضاء مع التاجر أو الوكيل أو مالك جهاز الصراف الآلي.
- جميع المراسلات المتعلقة باستفسارات جهة الإصدار أو حامل البطاقة أو جهات إنفاذ القانون المتعلقة بالتاجر أو الوكيل أو مالك جهاز الصراف الآلي أو مقدم الخدمة المرتبط.
- عقد مقدم الخدمة موقع، بما في ذلك اسم الوكلاء المشاركين في عملية العناية الواجبة.
- سجلات العناية الواجبة لجهة القبول فيما يتعلق بمقدم الخدمة ووكلائه.

ملاحظة: يوصي مشغل شبكة الدفع المحلية بأنه يجب على جهة القبول أن تحتفظ بجميع السجلات، في حالة قيام مشغل شبكة الدفع المحلية بإجراء تدقيق حسب الضرورة للتحقق من الامتثال لإجراءات التحقق.

3.1.7.6. تقييمات عدم الامتثال لإجراءات الفحص

يجوز لمشغل شبكة الدفع المحلية تدقيق جهة القبول للتحقق من امتثالها لإجراءات التحقق، ويجب على كل عضو الامتثال والمساعدة في إجراء هذا التدقيق تدقيق. سيقوم مشغل شبكة الدفع المحلية بمراجعة السجلات المطبقة التي تحتفظ بها جهة القبول لتحديد ما إذا كانت قد امتثلت لإجراءات التحقق. وإذا قرر مشغل شبكة الدفع المحلية أن جهة القبول لم تمتثل لإجراءات التحقق، أو لم تقوم بتصحيح جميع أوجه القصور التي أدت إلى الانتهاك طبقا لما يقدره مشغل شبكة الدفع المحلية خلال 30 يومًا من العلم بالمخالفة، أو الإخطار بهذه العيوب، يجوز لمشغل شبكة الدفع المحلية تقييم جهة

or notice of such deficiencies, the National Scheme Operator may assess the Acquirer up to LYD XXXX for each 30-day period following the aforementioned period, with a maximum aggregate assessment of LYD XXXXX during any consecutive 12-month period. Any such assessment(s) will be in addition to any other financial responsibility that the Acquirer may incur, as set forth in the Standards. Violators will also be subject to chargebacks of fraudulent Transactions.

Failure to inquire to the Terminated Merchant File as described in this Rule with respect to prospective high-risk Merchants and Agents may result in an assessment of up to LYD XXXXX for each instance of noncompliance.

6.7.2 Terminated Merchant File

The Terminated Merchant File (TMF) is designed to provide Acquirers with the opportunity to develop and review enhanced or incremental risk information before entering into a Merchant Agreement. The TMF includes information about certain Merchants (and their owners) that an Acquirer has terminated.

When an Acquirer considers signing a Merchant, the TMF can help the Acquirer assess whether the Merchant was terminated by another Acquirer due to circumstances that could affect the decision whether to acquire for this Merchant and, if a decision is made to acquire, whether to implement specific action or conditions with respect to acquiring.

Legal Notice

The TMF and data stored therein are proprietary and confidential to the National Scheme Operator and its licensed Members.

A Member may use the TMF solely for the purpose of developing enhanced or incremental risk information before entering into a Merchant Agreement; any other use is prohibited.

The Standards set forth Member rights and obligations pertaining to access to and use of the TMF and require, among other things, that an Acquirer conduct an inquiry before acquiring high-risk Transactions from a Merchant and that an Acquirer report information pertaining to a Merchant that has been terminated for any one or more of a specified number of reasons. The Standards do not require an Acquirer to take any action or any specific action after receiving a response record and do not require that an Acquirer provide any information to or otherwise cooperate with any other Acquirer. The TMF may enable an Acquirer to develop enhanced or incremental risk information concerning a Merchant, but does not itself provide risk information. The Acquirer itself must determine whether the Merchant that is the subject of a “possible match” response is the same Merchant that the Acquirer conducted an inquiry about. A “possible match” response to an inquiry does not mean or suggest that a Merchant is a poor risk or greater risk than any other Merchant. A Member itself must determine whether a Merchant poses a risk and, if so, the nature of such risk.

The National Scheme Operator does not verify, otherwise confirm, or ask for confirmation of either the basis for or accuracy of any information that is reported to or listed in the TMF. The TMF may include incorrect, inaccurate, and incomplete information as well as information that should not have been reported. It is possible that facts and circumstances giving rise to a TMF report may be subject to interpretation and dispute.

القبول حتى XXXX دينار ليبي لكل فترة 30 يومًا بعد الفترة المذكورة أعلاه، مع أقصى تقدير إجمالي لـ XXXX دينار ليبي خلال أي فترة 12 شهرًا متتالية. سيكون أي تقييم (تقييمات) من هذا القبيل بالإضافة إلى أي مسؤولية مالية أخرى قد تتحملها الجهة القابلة، على النحو المنصوص عليه في المعايير. وسيخضع المخالفون أيضًا لرد المبالغ المدفوعة من المعاملات الاحتيالية.

قد يؤدي عدم التحقيق في ملف التاجر الذي فسخت العلاقة معه، كما هو موضح في هذه القاعدة فيما يتعلق بالتجار والوكلاء المحتملين ذوي المخاطر عالية إلى تقييم يصل إلى XXXXX دينار ليبي لكل حالة عدم امتثال.

2.7.6. ملف التاجر الذي فسخت العلاقة معه

تم إعداد ملف التاجر الذي فسخت العلاقة معه لتزويد جهات القبول بفرصة تطوير ومراجعة معلومات المخاطر المحسنة، أو المتزايدة قبل الدخول في اتفاقية التاجر. ويتضمن ملف التاجر الذي فسخت العلاقة معه معلومات حول تجار معينين (ومالكهم) فسخت جهة القبول العلاقة معهم.

عندما تفكر جهة القبول في التوقيع على التاجر، يمكن لملف التاجر الذي فسخت العلاقة معه مساعدة جهة القبول على تقييم ما إذا كان التاجر فسخت العلاقة معه من قبل جهة استحواذ أخرى بسبب الظروف التي قد تؤثر على قرار جهة القبول لهذا التاجر، وإذا تم اتخاذ قرار بالقبول، ما إذا كان سيتم تنفيذ إجراء أو شروط محددة فيما يتعلق بالقبول.

إخطار قانوني

ملف التاجر الذي فسخت العلاقة معه والبيانات المخزنة فيه مملوكة وسرية لمشغل شبكة الدفع المحلية والأعضاء المرخص لهم.

يجوز لأي عضو استخدام ملف التاجر الذي فسخت العلاقة معه، فقط لغرض تطوير معلومات المخاطر المحسنة أو المتزايدة قبل الدخول في اتفاقية التاجر؛ ولا يجوز استخدامه خارج هذا النطاق.

تحدد المعايير حقوق الأعضاء والالتزامات المتعلقة بالوصول إلى ملف التاجر الذي فسخت العلاقة معه، واستخدامها ومطابقتها، من بين أمور أخرى، ويجب على جهة القبول أن تقوم بإجراء تحقيق قبل الحصول على المعاملات عالية المخاطر من التاجر وأن تبلغ جهة القبول على المعلومات المتعلقة بالتاجر الذي فسخت العلاقة معه لأي سبب أو أكثر من العدد المحدد من الأسباب. لا تتطلب المعايير من جهة القبول اتخاذ أي إجراء أو أي إجراء محدد بعد تلقي سجل استجابة، ولا تتطلب أن تقدم جهة القبول أي معلومات أو تتعاون مع جهة استحواذ أخرى. وقد يمكن ملف التاجر التي فسخت العلاقة معه جهة القبول من تطوير معلومات مخاطر محسنة أو متزايدة تتعلق بالتاجر، لكنه لا يوفر معلومات مخاطر بحد ذاته. ويجب على جهة القبول بذاتها تحديد ما إذا كان التاجر موضوع استجابة “التطابق المحتمل” هو نفس التاجر الذي خضع للتحقيق من قبل جهة القبول. وإن رد “التطابق المحتمل” لا يعني أن التاجر يمثل مخاطرة ضعيفة أو مخاطرة أكبر من أي تاجر آخر. ويجب على العضو بذاته تحديد ما إذا كان التاجر يمثل خطرًا، وإذا كان الأمر كذلك، فطبيعة هذه المخاطر.

لا يتحقق مشغل شبكة الدفع المحلية أو يؤكد أو يطلب تحققاً على أساس أو دقة أي معلومات يتم الإبلاغ عنها أو إدراجها في ملف التاجر الذي فسخت العلاقة معه. وقد يتضمن ملف التاجر الذي فسخت العلاقة معه معلومات غير صحيحة وغير دقيقة وغير كاملة، بالإضافة إلى معلومات لا ينبغي الإبلاغ عنها. من الممكن أن الحقائق والظروف التي أدت إلى تقرير ملف التاجر الذي فسخت العلاقة معه قد تخضع للتفسير والنزاع.

6.7.3 Ongoing Monitoring

An Acquirer must monitor and confirm regularly that the Transaction activity of each of its Merchants (sales, credits, and chargebacks) is conducted in a legal and ethical manner and in full compliance with the Standards, and ensure that a Payment Facilitator conducts such monitoring with respect to each of its Agents, in an effort to deter fraud. Monitoring must focus on changes in activity over time, activity inconsistent with the Merchant's or Agent's business, or exceptional activity relating to the number of Transactions and Transaction amounts outside the normal fluctuation related to seasonal sales. Specifically for POS Transaction processing, ongoing monitoring includes, but is not limited to, Acquirer fraud loss controls relating to deposit (including credits) and authorization activity.

With respect to an electronic commerce (e-commerce) Merchant, the Acquirer regularly, as reasonably appropriate in light of all circumstances, must review and monitor the Merchant's website(s) and business activities to confirm and to reconfirm regularly that any activity related to or using a Mark is conducted in a legal and ethical manner and in full compliance with the Standards. The Acquirer must ensure that a Payment Facilitator conducts such monitoring with respect to each of its Agent's website(s). As a best practice, Acquirers should use a Merchant monitoring solution to review their e-commerce Merchants' and Agents' activity to avoid processing illegal or brand-damaging Transactions.

6.7.4 Merchant Education and Behavior

Once an acquiring relationship is established, an Acquirer must institute a fraud prevention program, including an education process consisting of periodic visits to Merchants, distribution of related educational literature, and participation in Merchant seminars. Instructions to Merchants must include Card acceptance procedures, use of the Electronic Warning Bulletin file or Warning Notice, authorization procedures including Code 10 procedures, proper completion of Transaction information documents (TIDs) (including primary account number [PAN] truncation), timely presentment of the Transaction to the Acquirer, and proper handling pursuant to Card capture requests. Members must thoroughly review with Merchants the Standards against the presentment of fraudulent Transactions. In addition, Members must review the data security procedures to ensure that only appropriate Card data is stored, magnetic stripe data never is stored, and any storage of data is done in accordance with the Standards for encryption, Transaction processing, and other prescribed practices. An Acquirer must also ensure that a Payment Facilitator conducts appropriate education activities for each of its Agents.

6.7.4.1 Requesting PIN and Authentication Data

An Acquirer or Merchant must not request or require that a Cardholder disclose his or her PIN. A PIN pad or Terminal must provide a means for the Cardholder to shield the keypad from view of others during PIN entry. If Card acceptance occurs via a web page, the Merchant must not design that web page in any way that might lead the Cardholder to believe that he or she must provide his or her PIN. Similarly, if the Cardholder is asked to complete a form in order to conduct a Transaction, the contents of that form must not lead the Cardholder to believe that he or she must provide his or her PIN.

3.7.6. المراقبة المستمرة

يجب أن تراقب جهة القبول، وتؤكد بطريقة منتظمة أن نشاط المعاملات لكل من تجاره (المبيعات والائتمانات وعمليات رد المبالغ المدفوعة) يتم بطريقة قانونية وأخلاقية وفي إطار الامتثال الكامل للمعايير، والتحقق من أن ميسر الدفع يجري مثل هذه المراقبة مع فيما يتعلق بكل من وكلائه، وفي محاولة لمكافحة المعاملات الاحتيالية. يجب أن تركز المراقبة على التغييرات في النشاط بمرور الوقت، أو النشاط غير المتوافق مع أعمال التاجر أو الوكيل، أو النشاط الاستثنائي المتعلق بعدد المعاملات ومبالغ المعاملات خارج التقلبات العادية المتعلقة بالمبيعات الموسمية. على وجه التحديد لمعالجة معاملات نقاط البيع، تشمل المراقبة المستمرة، على سبيل المثال، ضوابط مكافحة الاحتيال الخاصة بجهة القبول المتعلقة بالإيداع (بما في ذلك الاعتمادات) ونشاط التفويض.

فيما يتعلق بالتاجر الذي يمارس التجارة الإلكترونية، يجب على جهة القبول بشكل منتظم، وحسب الظروف، مراجعة ومراقبة موقع (مواقع) التاجر وأنشطته التجارية لتحقيق وإعادة التحقق بانتظام على أن أي نشاط متعلق بالعلامة أو استخدامها بطريقة قانونية وأخلاقية وبما يتفق تمامًا مع المعايير. يجب أن تتحقق جهة القبول من قيام ميسر الدفع بإجراء هذه المراقبة فيما يتعلق بكل موقع (مواقع) وكيله. كأفضل ممارسة، يجب على جهات القبول استخدام أسلوب مراقبة التاجر لمراجعة نشاط التاجر والوكلاء في التجارة الإلكترونية لتجنب معالجة المعاملات غير القانونية أو الضارة بالعلامة التجارية.

4.7.6. تعليم وسلوك التاجر

بمجرد إنشاء علاقة قبول، يجب على جهة القبول إنشاء برنامج لمنع المعاملات الاحتيالية، بما في ذلك عملية تعليمية تتكون من زيارات دورية للتجار وتوزيع المؤلفات التعليمية ذات الصلة والمشاركة في ندوات التاجر. يجب أن تتضمن التعليمات الموجهة إلى التجار إجراءات قبول البطاقة، واستخدام ملف نشرة التحذير الإلكترونية أو إخطار التحذير، وإجراءات التفويض بما في ذلك إجراءات الرمز 10، والإكمال الصحيح لوثائق معلومات المعاملة (بما في ذلك اقتطاع رقم الحساب الأساسي)، وتقديم المعاملة في الوقت المناسب إلى جهة القبول، والتعامل المناسب وفقًا لطلبات الحصول على البطاقة. يجب على الأعضاء مراجعة المعايير بدقة مع التجار مقابل تقديم المعاملات الاحتيالية. بالإضافة إلى ذلك، يجب على الأعضاء مراجعة إجراءات أمان البيانات لضمان تخزين بيانات البطاقة المناسبة فقط، وعدم تخزين بيانات الشريط المغناطيسي مطلقًا، وأي تخزين للبيانات يتم وفقًا لمعايير التشفير ومعالجة المعاملات والممارسات الأخرى المحددة. يجب على جهة القبول أيضًا التحقق من أن ميسر الدفع يجري أنشطة تعليمية مناسبة لكل من وكلائه.

1.4.7.6. طلب بيانات رقم التعريف الشخصي و المصادقة

يجب على جهة القبول، أو التاجر عدم طلب أو مطالبة حامل البطاقة بالكشف عن رقم التعريف الشخصي الخاص به. ويجب أن توفر لوحة رقم التعريف الشخصي أو المحطة وسيلة لحامل البطاقة لحماية لوحة المفاتيح من نظر الآخرين أثناء إدخال رقم التعريف الشخصي. إذا تم قبول البطاقة عبر صفحة الويب، يجب ألا يقوم التاجر بتصميم صفحة الويب هذه بطريقة قد تدفع حامل البطاقة للاعتقاد بأنه يجب عليه تقديم رقم التعريف الشخصي الخاص به. وبالمثل، إذا طلب من حامل البطاقة إكمال نموذج من أجل إجراء معاملة، يجب ألا تؤدي محتويات هذا النموذج إلى اعتقاد حامل البطاقة بأنه يجب عليه تقديم رقم التعريف الشخصي الخاص به.

A Merchant must not refuse to complete an e-commerce Transaction solely because the Cardholder does not have a digital certificate or other secured protocol, unless required by the National Scheme Operator. A Merchant is permitted and recommended to request that the Cardholder follow 3DS 1.0 or EMV 3DS authentication procedures, as applicable, prior to seeking the authorization of an Cardholder-initiated purchase Transaction or Payment Transaction.

The Acquirer must ensure that the Merchant is following these procedures. The National Scheme Operator will also, from time to time, perform audits on these Merchants to ensure that they are compliant with this and all other requirements.

6.7.5 High-Risk Merchants

An Acquirer of a non-face-to-face pharmaceutical, high-risk cyberlocker Merchant or Agent, cryptocurrency Merchant or Agent, high-risk negative option billing Merchant or Agent, and/or Merchant or Agent reported under the Excessive Chargeback Program (ECP) must comply with the registration and monitoring requirements set forth in this Rule for each such Merchant or Agent.

6.7.5.1 General Registration Requirements

The Member must provide all of the information requested for each Merchant, Agent, or other entity required to be registered through the MRP system. For each such entity, the requested information includes:

- The name, doing business as (DBA) name, and address
- The central access phone number or customer service phone number, website URL, or email address
- The name(s), address(es), and tax identification number(s) (or other relevant national identification number) of the principal owner(s)
- A detailed description of the service(s), product(s), or both that the entity will offer to Cardholders
- A description of payment processing procedures, Cardholder disclosures, and other practices including, but not limited to:
 - Data solicited from the Cardholder
 - Authorization process (including floor limits)
 - Member service return policies for card transactions
 - Disclosure made by the Merchant before soliciting payment information
 - Data storage and security practices
- The identity of any previous business relationship(s) involving the principal owner(s) of the entity
- A certification, by the officer of the Member with direct responsibility to ensure compliance of the registered entity with the Standards, stating that after conducting a diligent and good faith investigation, the Member believes that the information contained in the registration request is true and accurate.

Only the National Scheme Operator can modify or delete information about a registered entity. Members must submit any modification(s) about a registered entity in writing to the National Scheme Operator, with an explanation for the request. The National Scheme Operator reserves the right to deny a modification request.

يجب ألا يرفض التاجر إتمام معاملة التجارة الإلكترونية فقط لأن حامل البطاقة ليس لديه شهادة رقمية، أو بروتوكول آمن آخر، ما لم يطلب مشغل شبكة الدفع المحلية ذلك. ويُسمح للتاجر ويوصى له أن يطلب من حامل البطاقة اتباع إجراءات المصادقة DS3 1.0 أو 3DS EMV ، حسب الاقتضاء، قبل طلب التفويض لمعاملة الشراء أو معاملة الدفع التي بدأها حامل البطاقة.

يجب على جهة القبول التحقق من أن التاجر يتبع هذه الإجراءات. سيقوم مشغل شبكة الدفع المحلية أيضًا، من وقت لآخر، بإجراء عمليات تدقيق على هؤلاء التجار لضمان امتثالهم لهذا وجميع المتطلبات الأخرى.

5.7.6. التجار ذوي المخاطر العالية

يجب أن تمثل الجهة القابلة على تاجر أو وكيل صيدلاني غير مباشر وعالي الخطورة، وتاجر أو وكيل عملة مشفرة، وتاجر أو وكيل فاتورة خيار سلبي عالي المخاطر، أو تاجر أو وكيل تم الإبلاغ عنه بموجب برنامج رد التكاليف المفرط لشروط التسجيل والمراقبة المنصوص عليها في هذه القاعدة لكل تاجر أو وكيل من هذا القبيل.

1.5.7.6. متطلبات التسجيل العامة

يجب على العضو تقديم جميع المعلومات المطلوبة لكل تاجر أو وكيل أو كيان آخر مطلوب تسجيله من خلال نظام MRP لكل كيان، المعلومات المطلوبة تشمل:

- الاسم، وممارسة الأعمال التجارية باسم، والعنوان.
- رقم هاتف الوصول المركزي أو رقم هاتف خدمة العملاء أو عنوان URL لموقع الويب أو عنوان البريد الإلكتروني.
- الاسم (الأسماء) والعنوان (العناوين) ورقم (أرقام) التعريف الضريبي (أو أي رقم تعريف وطني آخر ذي صلة) للمالك (المالكين) الرئيسي.
- وصف تفصيلي للخدمة (الخدمات) أو المنتج (المنتجات) أو كليهما التي سيقدمها الكيان لحاملي البطاقات.
- وصف لإجراءات معالجة الدفع، وإفصاحات حامل البطاقة، وغيرها من الممارسات بما في ذلك، على سبيل المثال:
 - البيانات المطلوبة من حامل البطاقة.
 - عملية التفويض (بما في ذلك الحد الأدنى).
 - سياسات إرجاع خدمة الأعضاء لمعاملات البطاقة.
 - الإفصاح الذي يقدمه التاجر قبل طلب معلومات الدفع.
 - تخزين البيانات وممارسات الأمان.
- هوية أي علاقة (علاقات) عمل سابقة تشمل المالك (المالكين) الرئيسي للكيان.
- شهادة من مسؤول العضو المسؤول مباشرة عن ضمان امتثال الكيان المسجل للمعايير، تفيد بأنه بعد إجراء تحقيق دؤوب وحسن نية، يعتقد العضو أن المعلومات الواردة في طلب التسجيل صحيحة ودقيقة.

يمكن لمشغل شبكة الدفع المحلية فقط تعديل، أو حذف المعلومات حول كيان مسجل. ويجب على الأعضاء تقديم أي تعديل (تعديلات) حول الكيان المسجل كتابيًا إلى مشغل شبكة الدفع المحلية، مع توضيح للطلب. ولمشغل شبكة الدفع المحلية الموافقة على طلب التعديل، أو رفضه.

6.7.5.2 Merchant Registration Fees and Noncompliance Assessments

The National Scheme Operator assesses the Acquirer an annual LYDXXX registration fee for each high-risk Merchant and Agent, except Merchants reported under the Excessive Chargeback Program (ECP). The National Scheme Operator will collect the fee from the Acquirer through the Billing System.

The National Scheme Operator may assess a Member that acquires Transactions for any of these Merchant or Agent types without first registering the Merchant in accordance with the requirements of the MRP. A violation will result in an assessment of up to LYD XXX. If, after notice by the National Scheme Operator of the Acquirer’s failure to register a Merchant or Agent, that Acquirer fails to register its Merchant within 10 days of notice, the Acquirer will be subject to additional assessments of LYD XXXX per month for up to three months, and LYD XXXX per month thereafter, until the Acquirer satisfies the requirement. In addition, the Acquirer must ensure that the violation is corrected promptly. Such Merchant or Agent may also be deemed by the National Scheme Operator, in its sole discretion, to be in violation of the Illegal or Brand-damaging Transactions Rule.

6.7.5.3 General Monitoring Requirements

The monitoring requirements described in this Rule apply to Members that acquire non-face-to-face pharmaceutical and tobacco product Transactions, government-owned lottery Transactions, skill games Transactions, high-risk cyberlocker Transactions, recreational cannabis Transactions, cryptocurrency Transactions, high-risk negative option billing Transactions, or Transactions from Merchants reported under the ECP:

- The Acquirer must ensure that each such Merchant implements real-time and batch procedures to monitor continually all of the following:
 - Simultaneous multiple Transactions using the same Account number
 - Consecutive or excessive attempts using the same Account number

When attempted fraud is evident, a Merchant should implement temporary bank identification number (BIN) blocking as a fraud deterrent.

- The Acquirer must ensure that each such Merchant complies with the fraud control Standards in this chapter 10 and maintain a total chargeback-to-interchange sales volume ratio below the ECP thresholds.

6.7.5.4 Additional Requirements for Specific Merchant Categories

Before an Acquirer may process any of the high-risk Transaction types described in this Rule from a Merchant or Agent, it must register the Merchant with the National Scheme Operator.

At the time of registration, the Acquirer of such Merchant or Agent must have verified that the Merchant’s or Agent’s activity complies fully with all laws applicable to the National Scheme Operator, the Merchant or Agent, the Issuer, the Acquirer, and any prospective customer of the Merchant or Agent. Such verification may include, but is not limited to, a written opinion from independent, reputable, and qualified legal counsel or accreditation by a recognized third party.

By registering a Merchant or Agent, the Acquirer represents and warrants that the Acquirer has verified compliance with applicable law as described above. The Acquirer must maintain such verification for so long as it acquires Transactions from the Merchant or Agent that is subject to the afore described registration requirement and must, no less frequently

2.5.7.6. رسوم تسجيل التاجر وتقييمات عدم الامتثال

يقوم مشغل شبكة الدفع المحلية بتقييم جهة القبول رسم تسجيل XXX دينار ليبي سنويًا لكل تاجر ووكيل عالي الخطورة. باستثناء التجار المبلغين بموجب برنامج رد المبالغ المدفوعة المفراط. ويقوم مشغل شبكة الدفع المحلية بتحصيل الرسوم من جهة القبول من خلال نظام الفوترة.

يجوز لمشغل شبكة الدفع المحلية تقييم العضو الذي يكتسب معاملات لأي من أنواع هؤلاء التجار أوالوكلاء دون تسجيل التاجر أولًا وفقًا لمتطلبات MRP. سيؤدي الانتهاك إلى تقييم يصل إلى XXX دينار ليبي.

إذا فشلت جهة القبول في تسجيل تاجره، بعد إخطار من مشغل شبكة الدفع المحلية بفشل جهة القبول في تسجيل التاجر أو الوكيل، خلال 10 أيام من الإخطار، فإن جهة القبول تخضع إلى تقييمات إضافية بقيمة XXXX دينار ليبي شهريًا لمدة تصل إلى ثلاثة أشهر، و XXXX دينار ليبي شهريًا بعد ذلك، حتى تفي جهة القبول بالمتطلبات. بالإضافة إلى ذلك، يجب على جهة القبول التحقق من تصحيح المخالفة على الفور. يمكن أيضًا اعتبار هذا التاجر أو الوكيل من قبل مشغل شبكة الدفع المحلية، وفقًا لتقديره الخاص، مخالفًا لقاعدة المعاملات غير القانونية أو التي تضر بالعلامة التجارية.

3.5.7.6. متطلبات المراقبة العامة

تنطبق متطلبات المراقبة الموضحة في هذه القاعدة على الأعضاء الذين يكتسبون معاملات منتجات الأدوية والتبغ، غير المباشرة، ومعاملات ألعاب المهارة، والمعاملات الإلكترونية عالية الخطورة، ومعاملات القنب الترفيهية، ومعاملات العملات المشفرة، ومعاملات فواتير الخيارات السلبية عالية المخاطر، أو المعاملات من التاجر المبلغ عنها بموجب برنامج رد المبالغ المدفوعة المفراط:

- يجب عل جهة القبول أن تتحقق من أن كل تاجر من هذا القبيل ينفذ مجموعة إجراءات في الوقت الفعلي لمراقبة كل ما يلي باستمرار:
 - معاملات متعددة متزامنة باستخدام نفس رقم الحساب.
 - محاولات متتالية أو مفطرة باستخدام نفس رقم الحساب.

عندما تكون محاولة الاحتيال واضحة، يجب على التاجر تنفيذ حظر رقم التعريف المصرفي المؤقت كوسيلة لمكافحة الاحتيال.

- يجب على جهة القبول أن تتحقق من امتثال كل تاجر لمعايير مكافحة الاحتيال الواردة في هذا الفصل 10 والحفاظ على إجمالي نسبة حجم مبيعات رد المبالغ المدفوعة إلى التبادل أقل من مراحل ECP.

4.5.7.6.متطلبات إضافية لفئات تجار معينين

قبل أن تقوم جهة القبول بمعالجة أي من أنواع المعاملات عالية المخاطر الموضحة في هذه القاعدة من تاجر أو وكيل، يجب عليه تسجيل التاجر لدى مشغل شبكة الدفع المحلية.

يجب على جهة القبول، في وقت التسجيل، أن تتحقق من أن نشاط التاجر أو الوكيل يتوافق تمامًا مع جميع القوانين المطبقة على مشغل شبكة الدفع المحلية والتاجر أو الوكيل وجهة الإصدار وجهة القبول وأي عميل محتمل للتاجر أو الوكيل. قد يشمل هذا التحقق، على سبيل المثال، رأيًا مكتوبًا من مستشار قانوني مستقل وحسن السمعة ومؤهل أو اعتماد من قبل طرف ثالث معترف به.

بتسجيل التاجر أو الوكيل ، تقرر جهة القبول وتضمن أنه قد تحقق من الامتثال للقانون المعمول به كما هو موضح أعلاه. يجب على جهة القبول الاحتفاظ بهذا التحقق طالما أنه يكتسب المعاملات من التاجر أو الوكيل الذي يخضع لمتطلبات التسجيل الموصوفة أعلاه ويجب، على الأقل كل 12 شهرًا،

than every 12 months, confirm continued compliance with applicable law concerning the business of the registered Merchant or Agent. The Acquirer must furnish the National Scheme Operator with a copy of such documentation promptly upon request.

Pharmaceutical Product Merchants

A non-face-to-face pharmaceutical Transaction occurs in a Card-not-present environment when a consumer uses an Account to purchase prescription medicines from a Merchant whose primary business is non-face-to-face selling of prescription drugs.

An Acquirer must Identify all non-face-to-face pharmaceutical Transactions using MCC 5122 (Drugs, Drug Proprietors, and Druggists Sundries) and TCC T for wholesale purchases or MCC 5912 (Drug Stores, Pharmacies) and TCC T for retail purchases. An Acquirer must identify all non-face-to-face tobacco product Transactions using MCC 5993 (Cigar Stores and Stands) and TCC T.

High-Risk Cyberlocker Merchants

A non-face-to-face high-risk cyberlocker Transaction occurs in a Card-not-present environment when a consumer uses an Account to purchase access directly from a Merchant or Agent, or indirectly from an operator or entity that can provide access, to remote digital file storage and sharing services.

Any cyberlocker Merchant, Agent, or entity that provides access to or accepts payments on behalf of such Merchant's or Agent's contents and services that meets one or more of the following criteria must be registered by the Acquirer as a high-risk cyberlocker Merchant, and the National Scheme Operator will determine, in its sole discretion, if the Merchant, Agent, or entity is a high-risk cyberlocker Merchant:

- The cyberlocker Merchant provides rewards, cash payments, or other incentives to uploaders. Some incentives are based on the number of times that the uploader's files are downloaded or streamed by third parties. The Merchant's rewards programs also pay a higher commission for the distribution of file sizes consistent with long-form copyrighted content such as movies and television shows.
- The cyberlocker Merchant provides URL codes to uploaders to facilitate sharing and the incorporation of such links on third-party indexing or linking websites.
- Links to prohibited content stored in the cyberlocker are often found on third-party indexing or linking sites, or by search engine queries.
- Files stored within the cyberlocker Merchant may be purged if they are not accessed or unless the user purchases a premium membership.
- Incentives for premium cyberlocker memberships are based on faster download speed or removing ads, as opposed to storage space. Free access to stored files may otherwise be discouraged by long wait times, bandwidth throttling, download limits, online advertising, or other techniques.
- The cyberlocker Merchant provides a "link checker" that allows users to determine whether a link has been removed, and if so, allows the user to promptly re-upload that content.

تأكيد الامتثال المستمر للقانون المعمول به فيما يتعلق بأعمال الشركة التاجر أو الوكيل المسجل. ويجب على جهة القبول تزويد مشغل شبكة الدفع المحلية بنسخة من هذه المستندات على الفور عند الطلب.

تجار المنتجات الصيدلانية

تحدث المعاملة الصيدلانية غير المباشرة في بيئة البطاقة غير الموجودة عندما يستخدم المستهلك حسابًا لشراء الأدوية التي تستلزم وصفة طبية من تاجر يتمثل نشاطه الأساسي في البيع غير المباشر للعقاقير الطبية.

يجب على جهة القبول تحديد جميع المعاملات الصيدلانية غير المباشرة باستخدام MCC 5122 (الأدوية، ومالكي الأدوية، ومتخصصي الأدوية) و TCC T لعمليات الشراء بالجملة أو MCC 5912 (متاجر الأدوية، الصيدليات) و TCC T لمشتريات التجزئة. ويجب على جهة القبول تحديد جميع معاملات منتجات التبغ غير المباشرة باستخدام MCC 5993 (متاجر وأكشاك السيجار) و TCC T.

التجار Cyberlocker ذوو المخاطر العالية

تحدث معاملة Cyberlocker عالية الخطورة غير المباشرة في بيئة البطاقة غير الموجودة عندما يستخدم المستهلك حسابًا لشراء الوصول مباشرة من تاجر أو وكيل، أو بشكل غير مباشر من مشغل أو كيان يمكنه توفير الوصول، لتخزين الملفات الرقمية عن بعد وخدمات المشاركة.

أي تاجر أو وكيل أو كيان Cyberlocker يوفر الوصول إلى أو يقبل المدفوعات نيابة عن محتويات وخدمات هذا التاجر أو الوكيل الذي يستوفي واحدًا أو أكثر من المعايير التالية: يجب أن يتم تسجيله من قبل جهة القبول باعتباره تاجرًا Cyberlocker عالي الخطورة، وسيحدد مشغل شبكة الدفع المحلية، وفقًا لتقديره الخاص، ما إذا كان التاجر أو الوكيل أو الكيان تاجرًا Cyberlocker عالي الخطورة:

- يوفر تاجر Cyberlocker مكافآت أو مدفوعات نقدية أو حوافز أخرى للقائمين بالتحميل. وتعتمد بعض الحوافز على عدد المرات التي يتم فيها تنزيل ملفات القائم بالتحميل، أو بثها بواسطة جهات خارجية. تدفع برامج مكافآت التاجر أيضًا عمولة أعلى لتوزيع أحجام الملفات المتوافقة مع المحتوى الطويل المحمي بحقوق الطبع والنشر مثل الأفلام والبرامج التلفزيونية.
- يوفر تاجر Cyberlocker رموز عناوين URL للقائمين بالتحميل لتسهيل مشاركة ودمج هذه الروابط في فهرسة أو ربط مواقع تابعة لجهات خارجية.

- غالبًا ما يتم العثور على روابط المحتوى المحظور المخزن في Cyberlocker في فهرسة أو روابط مواقع تابعة لجهات خارجية، أو من خلال استعلامات محرك البحث.
- قد يتم حذف الملفات المخزنة في Cyberlocker التاجر إذا لم يتم الوصول إليها أو ما لم يشتري المستخدم عضوية مميزة.
- تستند حوافز عضويات Cyberlocker المتميزة إلى سرعة تنزيل أسرع أو إزالة الإعلانات، بدلًا من مساحة التخزين. قد يتم تشييط الوصول المجاني إلى الملفات المخزنة بسبب فترات الانتظار الطويلة، أو تقييد النطاق الترددي، أو حدود التنزيل، أو الإعلان عبر الإنترنت، أو غير ذلك من الأساليب.
- يوفر تاجر Cyberlocker "مدقق روابط" يسمح للمستخدمين بتحديد ما إذا كان الرابط قد تمت إزالته، وإذا كان الأمر كذلك، فإنه يسمح للمستخدم بإعادة تحميل هذا المحتوى على الفور.

- File owners are:
 - Typically anonymous,
 - Not required to provide any identifying information, and
 - Not aware of the identity of those users who have access to or view their files.
- File distribution and sharing are emphasized on the cyberlocker site.
- Storage or transfer of specific copyrighted file types such as movies, videos, or music is promoted on the cyberlocker site.
- Without the purchase of a premium membership, video playback includes frequent display advertisements.

An Acquirer must identify all non-face-to-face high-risk cyberlocker Transactions using MCC 4816 (Computer Network/Information Services) and TCC T.

To register a Merchant, Agent, or other entity, the Acquirer must demonstrate that an adequate due diligence review was conducted by providing the following items to the National Scheme Operator upon request as part of the registration process (herein, all references to a Merchant also apply to a Agent or other entity):

1. Evidence of legal authority

The Acquirer must obtain from the Merchant:

- a copy of the Merchant's license (or similar document), if any, issued by the appropriate governmental authority where the Merchant's cryptocurrency activity will occur or be offered to Cardholders, that expressly authorizes the Merchant to engage in such activity;
- a copy of the Merchant's registration, where required under applicable law, with a licensed exchange or licensed trading platform; and
- any law applicable to the Merchant that permits the cryptocurrency activity.
- The Acquirer must provide an updated license(s) to the National Scheme Operator prior to expiration. If an Acquirer is unable to obtain an updated license, then the Acquirer must cease processing applicable cryptocurrency Transactions from such Merchant until the Acquirer is able to provide an updated license to the National Scheme Operator.

2. Legal opinion

The Acquirer must obtain a reasoned legal opinion, addressed to the Acquirer, from a reputable law firm located in each country where cryptocurrency activity will occur or be offered to Cardholders. The legal opinion must:

- identify all relevant laws and other laws applicable to the Merchant;
- identify all relevant laws and other laws applicable to Cardholders that may transact with the Merchant; and
- demonstrate that the Merchant's and Cardholders' activities comply at all times with any laws identified above.

The legal opinion must be acceptable to the National Scheme Operator. Further, the Acquirer shall ensure that:

- the Merchant properly maintains its lawful status in any jurisdiction where such Merchant engages in cryptocurrency activities; and
- any relevant permits remain unexpired.

- أصحاب الملفات هم:
- مجهول عادةً.
- غير ملزم بتقديم معلومات التعريف.
- غير عالم بهوية هؤلاء المستخدمين الذين لديهم حق الوصول إلى ملفاتهم أو النظر إليها.
- يتم التأكيد على توزيع الملفات ومشاركتها على موقع Cyberlocker.
- تخزين أو نقل أنواع معينة من الملفات المحمية بحقوق الطبع والنشر مثل الأفلام أو مقاطع الفيديو أو الموسيقى على موقع Cyberlocker.
- بدون شراء عضوية متميزة، يتضمن تشغيل الفيديو إعلانات معروضة متكررة.

يجب على جهة القبول تحديد جميع المعاملات الإلكترونية عالية الخطورة غير المباشرة باستخدام MCC 4816 (شبكة الكمبيوتر/خدمات المعلومات) و TCC T.

لتسجيل تاجر أو وكيل أو كيان آخر، يجب على جهة الاستحواذ إثبات إجراء مراجعة كافية للعناية الواجبة من خلال توفير العناصر التالية لمشغل شبكة الدفع المحلية عند الطلب كجزء من عملية التسجيل (هنا، جميع الإشارات إلى التاجر تنطبق أيضًا على الوكيل أو أي كيان آخر):

1. دليل على السلطة القانونية

يجب على جهة القبول الحصول من التاجر على:

- نسخة من ترخيص التاجر (أو مستند مشابه)، إن وجد، صادر عن السلطة الرسمية المختصة حيث سيحدث نشاط التاجر في العملة المشفرة أو يُعرض على حاملي البطاقات، والذي يخول التاجر صراحةً الانخراط في مثل هذا النشاط.
- نسخة من تسجيل التاجر، عند الاقتضاء بموجب القانون المعمول به، في بورصة مرخصة أو منصة تداول مرخصة.
- أي قانون ينطبق على التاجر يسمح بنشاط العملة المشفرة.
- يجب على جهة القبول تقديم ترخيص (تراخيص) محدثة لمشغل شبكة الدفع المحلية قبل انتهاء الصلاحية. وإذا لم تتمكن جهة القبول من الحصول على ترخيص محدث، فيجب عليها التوقف عن معالجة معاملات العملة المشفرة المعمول بها من هذا التاجر حتى تتمكن من تقديم ترخيص محدث لمشغل شبكة الدفع المحلية.

2. رأي قانوني

يجب على جهة القبول الحصول على رأي قانوني مسبب، موجه إليها من شركة محاماة ذات سمعة طيبة تقع في كل بلد سيحدث فيه نشاط العملة المشفرة أو يُعرض على حاملي البطاقات. الرأي القانوني يجب أن:

- تحديد جميع القوانين ذات الصلة والقوانين الأخرى السارية على التاجر.
- تحديد جميع القوانين ذات الصلة والقوانين الأخرى السارية على حاملي البطاقات الذين قد يتعاملون مع التاجر.
- إثبات أن أنشطة التاجر وحملة البطاقات تمثل في جميع الأوقات لأي قوانين محددة أعلاه.
- يجب أن يكون الرأي القانوني مقبولًا لمشغل شبكة الدفع المحلية. علاوة على ذلك، يجب أن تضمن جهة القبول ما يلي:
- التاجر يحافظ بشكل صحيح على وضعه القانوني في دعوى قضائية يشارك فيها التاجر في أنشطة العملة المشفرة.
- تظل أي تصاريح ذات صلة غير منتهية الصلاحية.

3. Effective controls

The Acquirer must obtain certification from a qualified independent third party demonstrating that the Merchant's systems for operating its cryptocurrency business:

- include effective age and location verification; and
- are reasonably designed to ensure that the Merchant's cryptocurrency business will remain within legal limits (including in connection with cross-border Transactions).

4. Notification of changes

The Acquirer must certify that the Acquirer will notify the National Scheme Operator of any changes to the information that the Acquirer has provided to the National Scheme Operator, including changes in applicable law, Merchant activities, and Merchant systems. Such notification shall include any revisions or additions to the information provided to the National Scheme Operator (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten (10) days of any such change.

5. Acceptance of responsibilities

The Acquirer must specifically affirm that it will not submit restricted Transactions from the Merchant for authorization.

High-Risk Negative Option Billing Merchants

A non-face-to-face high-risk negative option billing Transaction occurs in a Card-not-present environment when a consumer uses an Account to purchase a subscription service to automatically receive one or more physical products (such as cosmetics, health-care products, or vitamins) on a recurring basis (such as weekly, monthly, semi-annually, or annually).

The subscription service may be initiated by an agreement between the consumer and the Merchant or Agent whereby the consumer (Cardholder) receives from the Merchant or Agent a sample of the product (either complimentary or at a nominal price) for a trial period. The sample may be larger, equal to, or smaller than the product provided by the Merchant or Agent during the subscription period. For the purposes of this Rule, a trial period means a preset length of time during which the Cardholder may evaluate the characteristics of the physical product such as its quality or usefulness to determine whether the Cardholder wants to either:

- Purchase the product on a one-time basis or recurring basis; or
- Return the product (if possible) to the high-risk negative option billing Merchant.

After the trial period has expired, a non-face-to-face high-risk negative option billing Transaction may occur on a recurring basis using Account information provided by the Cardholder to the Merchant or Agent each time that the product is shipped to the Cardholder.

The non-face-to-face high-risk negative option billing Transactions continue to occur on a recurring basis until either:

- The Cardholder takes action to terminate the agreement with the Merchant or Agent (for example, notifying the Merchant or Agent to cancel the subscription);
- The Merchant or Agent terminates the agreement; or
- The subscription expires.

3. ضوابط فعالة

يجب أن تحصل جهة القبول على شهادة من جهة خارجية مستقلة مؤهلة تثبت أن أنظمة التاجر لتشغيل أعمال العملة المشفرة:

- تشمل التحقق الفعال من العمر والموقع.
- مصممة بشكل معقول لضمان بقاء عمل التاجر للعمليات المشفرة ضمن الحدود القانونية (بما في ذلك ما يتعلق بالمعاملات عبر الحدود).

4. الإخطار بالتغييرات

يجب أن تتعهد جهة القبول بإنها سوف تخطر مشغل شبكة الدفع المحلية بأي تغييرات على المعلومات التي تقدمها جهة القبول إلى مشغل شبكة الدفع المحلية، بما في ذلك التغييرات في القانون المعمول به وأنشطة وأنظمة التاجر. ويجب أن يتضمن هذا الإخطار أي مراجعات أو إضافات للمعلومات المقدمة إلى مشغل شبكة الدفع المحلية (على سبيل المثال، الرأي القانوني، شهادة الطرف الثالث) لجعل المعلومات حديثة وكاملة. وتلتزم جهة القبول بتقديم هذا الإخطار خلال 10 أيام من حدوث التغيير.

5. قبول المسؤوليات

يجب على جهة القبول أن تؤكد على وجه التحديد أنها لن تقدم المعاملات المقيدة من التاجر للحصول على إذن.

تجار فواتير الخيارات السلبية عالية المخاطر

تحدث معاملة فوترة بخيار عالية الخطورة غير المباشرة في بيئة البطاقة غير الموجودة عندما يستخدم المستهلك حسابًا لشراء خدمة اشتراك لتلقي منتجًا ماديًا واحدًا أو أكثر تلقائيًا (مثل مستحضرات التجميل أو منتجات العناية أو الفيتامينات) بشكل متكرر (أسبوعيًا أو شهريًا أو نصف سنويًا أو سنويًا).

يمكن البدء في خدمة الاشتراك عن طريق عقد بين المستهلك والتاجر أو الوكيل حيث يتلقى المستهلك (حامل البطاقة) من التاجر أو الوكيل عينة من المنتج (إما مجانية أو بسعر رمزي) لفترة تجريبية. قد تكون العينة أكبر أو مساوية أو أصغر من المنتج المقدم من التاجر أو الوكيل خلال فترة الاشتراك. لأغراض تطبيق هذه القاعدة، تعني فترة التجربة، الفترة الزمنية المحددة مسبقًا، والتي يمكن خلالها لحامل البطاقة تقييم خصائص المنتج المادي مثل جودته أو فائدته، لتحديد ما إذا كان حامل البطاقة يريده، أم لا:

- شراء المنتج لمرة واحدة أو على أساس متكرر.
- إعادة المنتج (إن أمكن) إلى تاجر فواتير الخيار السلبي عالي الخطورة.

بعد انتهاء الفترة التجربة، قد تحدث معاملة فوترة بخيار سلبي عالية الخطورة غير المباشرة على أساس متكرر باستخدام معلومات الحساب التي يقدمها حامل البطاقة إلى التاجر أو الوكيل في كل مرة يتم فيها شحن المنتج إلى حامل البطاقة .

تستمر معاملات فوترة الخيار السلبي عالية الخطورة غير المباشرة في الحدوث على أساس متكرر حتى إما:

- يتخذ حامل البطاقة إجراء لإنهاء العقد مع التاجر أو الوكيل (على سبيل المثال، إخطار التاجر أو الوكيل بإلغاء الاشتراك).
- يقوم التاجر أو الوكيل بإنهاء العقد.
- ينتهي الاشتراك.

An Acquirer must use MCC 5968 (Direct Marketing—Continuity/Subscription Merchants) and TCC T to identify all non-face-to-face high-risk negative option billing Transactions. Registration is required not only for the Merchant or Agent, but also for any entities that provide service to such Merchant or Agent that allow access to Account data.

6.7.6 Reporting Suspected Merchant Fraud

A Merchant must submit to its Acquirer records of valid Transactions only between the Merchant and a bona fide Cardholder. A Merchant must not submit to its Acquirer a Transaction that the Merchant knows or should have known to be fraudulent or not authorized by the Cardholder, or that it knows or should have known to be authorized by a Cardholder colluding with the Merchant for a fraudulent purpose. For purposes of this Rule, the Merchant is deemed to be responsible for the conduct of its employees, agents, and representatives.

The following requirements relate to the reporting of Merchant activity suspected to be in violation of the foregoing Rule.

Acquirer Responsibilities

If an Acquirer has reason to believe that a Merchant with whom it has entered into a Merchant Agreement is engaging in collusive or otherwise fraudulent or inappropriate activity, the Acquirer must immediately notify the National Scheme Operator by sending an email message to [email address].

Issuer Responsibilities

If an Issuer becomes aware of any Merchant in violation of this Rule, through Cardholder complaints or otherwise, the Issuer immediately must notify the National Scheme Operator by sending an email message to [email address].

6.7.7 Chargeback Monitoring Program

The National Scheme Operator's Chargeback Monitoring Program is designed to encourage each Acquirer to closely monitor, on an ongoing basis, its chargeback performance at the Merchant level and to determine promptly when a Merchant has exceeded or is likely to exceed monthly chargeback thresholds.

Definitions

As used in this Rule, the following terms have the meanings set forth below.

Chargeback-to-Transaction Ratio (CTR)

The CTR is the number of chargebacks received by the Acquirer for a Merchant in a calendar month divided by the number of the Merchant's sales Transactions in the preceding month acquired by that Acquirer. (A CTR of 1% equals 100 basis points, and a CTR of 1.5% equals 150 basis points.)

Chargeback-Monitored Merchant (CMM)

A CMM is a Merchant that has a CTR in excess of 100 basis points and at least 100 chargebacks in a calendar month.

يجب على جهة القبول استخدام MCC 5968 (التسويق المباشر - تجار الاستمرارية/الاشتراك) و TCC T لتحديد جميع معاملات فواتير الخيارات السلبية عالية الخطورة وغير المباشرة. التسجيل مطلوب ليس فقط للتاجر أو الوكيل، ولكن أيضًا لأي كيانات تقدم خدمة لهذا التاجر أو الوكيل الذي يسمح بالوصول إلى بيانات الحساب.

6.7.6 الإبلاغ عن احتيال تاجر مشتبته به

يجب على التاجر أن يقدم إلى جهة القبول سجلات المعاملات الصالحة فقط بين التاجر وحامل البطاقة حسن النية. ويجب ألا يقدم التاجر إلى جهة القبول معاملة يعلم التاجر أو كان ينبغي أن يعلم أنها احتيالية، أو غير مصرح بها من قبل حامل البطاقة، أو أنه يعلم، أو كان ينبغي أن يعلم بأنه مصرح بها من قبل حامل البطاقة الذي يتواطأ مع التاجر لغرض احتيالي. لأغراض تطبيق هذه القاعدة، يعتبر التاجر مسؤولاً عن سلوك موظفيه ووكلائه وممثليه.

تتعلق المتطلبات التالية بالإبلاغ عن نشاط التاجر المشتبه في أنه ينتهك القاعدة السابقة.

مسؤوليات جهة القبول

إذا كان لدى جهة القبول سبب للاعتقاد بأن التاجر الذي أبرم معه اتفاقية تاجر ينخرط في نشاط تواطئي أو احتيالي أو غير مناسب، يجب على جهة القبول إخطار مشغل شبكة الدفع المحلية على الفور عن طريق إرسال رسالة بريد إلكتروني إلى [عنوان البريد الإلكتروني].

مسؤوليات جهة الإصدار

إذا علمت جهة الإصدار أن أي تاجر يخالف هذه القاعدة، من خلال شكاوى حامل البطاقة أو غير ذلك، يجب على جهة الإصدار إخطار مشغل شبكة الدفع المحلية على الفور عن طريق إرسال رسالة بريد إلكتروني إلى [عنوان البريد الإلكتروني].

7.7.6 برنامج مراقبة رد المبالغ المدفوعة

تم تصميم برنامج مراقبة رد المبالغ المدفوعة لمشغل شبكة الدفع المحلية لتشجيع جهات القبول على المراقبة عن كثب، على أساس مستمر، لأداء رد المبالغ المدفوعة على مستوى التاجر ولتحديد متى يتجاوز التاجر أو من المحتمل أن يتجاوز حدود رد المبالغ المدفوعة الشهرية.

تعريفات

كما هو مستخدم في هذه القاعدة، فإن المصطلحات التالية لها المعاني الموضحة أدناه.

نسبة رد المبالغ المدفوعة إلى معاملة (CTR)

نسبة رد المبالغ المدفوعة إلى معاملة (CTR) هي عدد عمليات رد المبالغ المدفوعة التي تتلقاها جهة القبول من التاجر في شهر تقويمياً مقسوماً على عدد معاملات مبيعات التاجر في الشهر السابق التي حصلت عليها جهة القبول. (نسبة 1% من نسبة رد المبالغ المدفوعة إلى معاملة (CTR) تساوي 100 نقاط أساسية، ونسبة 1.5% من نسبة رد المبالغ المدفوعة إلى معاملة (CTR) تساوي 150 نقاط أساسية).

التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM)

التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) هو تاجر لديه نسبة رد المبالغ المدفوعة إلى معاملة (CTR) تزيد عن 100 نقاط أساسية وما لا يقل عن 100 عملية رد مبالغ مدفوعة في شهر تقويمي.

Excessive Chargeback Merchant (ECM)

A Merchant is an ECM if in each of two consecutive calendar months (the “trigger months”), the Merchant has a minimum CTR of 150 basis points and at least 100 chargebacks in each month. This designation is maintained until the ECM’s CTR is below 150 basis points for two consecutive months.

6.7.7.1 Reporting Requirements

It is the Acquirer’s responsibility on an ongoing basis to monitor each of its Merchants in accordance with the Standards.

The program requires an Acquirer to calculate, for each calendar month, the CTR in basis points for each of its Merchants and report any Merchant that is a CMM or ECM. The National Scheme Operator will assess an Acquirer of an ECM the reporting fee.

Chargeback-Monitored Merchant Reporting Requirements

- Each calendar month, an Acquirer must submit a separate CMM report for each of its Merchant(s) that qualifies as a CMM for the previous calendar month. For the purpose of determining if an Acquirer is obligated to submit a CMM report,
- the Acquirer must calculate the CTR.
- The Acquirer must submit this report no later than 45 days from the end of the calendar month.
- The Acquirer must submit the CMM report in a form and manner required by the National Scheme Operator. The Acquirer also must provide a copy of the CMM report and these ECP Standards to the specific CMM.
- The Acquirer must continue to provide CMM reporting until the Merchant is no longer identified as a CMM for two consecutive months.

CMM Report Contents

The CMM report must include all of the following information:

- The name and location of the CMM
- The calendar month of CMM qualification being reported
- The Card acceptor business code/Merchant category code (MCC) assigned to the CMM and a description of the nature of the CMM’s business
- The number and gross dollar volume (GDV) of the CMM’s sales Transactions in the reported calendar month and in the preceding month
- The number and GDV of chargebacks of the CMM’s sales Transactions for the reported calendar month
- Any additional information as The National Scheme Operator may require

تاجر رد المبالغ المدفوعة المفرط (ECM)

يعد التاجر تاجرٍ لرد المبالغ المدفوعة المفرط (ECM) إذا كان لديه، في كل شهرين تقويميين متتاليين (“أشهر بدء التشغيل”) ، حد أدنى نسبة رد المبالغ المدفوعة إلى معاملة (CTR) يبلغ 150 نقاط أساسية و 100 عملية رد مبالغ مدفوعة على الأقل في كل شهر. ويتم الاحتفاظ بهذا التعيين حتى تقل نسبة رد المبالغ المدفوعة إلى المعاملة (CTR) الخاصة بالتاجر لرد المبالغ المدفوعة المفرط (ECM) عن 150 نقاط أساسية لمدة شهرين متتاليين.

1.7.7.6. متطلبات الإبلاغ

تقع على عاتق الجهة القابلة لمسؤولية مراقبة كل من التجار التابعين لها وفقًا للمعايير بشكل مستمر. يتطلب البرنامج من أحد جهات القبول أن تحسب، لكل شهر تقويمي، نسبة رد المبالغ المدفوعة إلى معاملة (CTR) في النقاط الأساسية لكل من التجار التابعين له والإبلاغ عن أي تاجر يمثل التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) أو تاجر لرد المبالغ المدفوعة المفرط (ECM). سيقوم مشغل شبكة الدفع المحلية بتقييم جهة القبول على التاجر لرد المبالغ المدفوعة المفرط (ECM) برسوم الإبلاغ.

متطلبات الإبلاغ عن التاجر الخاضعة لمراقبة رد المبالغ المدفوعة

- يجب على جهة القبول في كل شهر تقويمي، تقديم تقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) منفصل، لكل تاجر (تجار) مؤهل ليكون تاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) للشهر التقويمي السابق. لغرض تحديد ما إذا كانت جهة القبول ملزمة بتقديم تقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM)،
- يجب على جهة القبول حساب نسبة رد المبالغ المدفوعة إلى معاملة (CTR) .
- يجب على جهة القبول تقديم هذا التقرير في موعد لا يتجاوز 45 يومًا من نهاية الشهر التقويمي.
- يجب على جهة القبول تقديم تقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) بالشكل والطريقة التي يطلبها مشغل شبكة الدفع المحلية.
- يجب على جهة القبول أيضًا تقديم نسخة من تقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) ومعايير برنامج رد المبالغ المدفوعة المفرط (ECP) هذه إلى التاجر الخاضع لمراقبة لرد المبالغ المدفوعة (CMM) المحدد.
- يجب أن تستمر جهة القبول في تقديم تقارير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) حتى يتوقف تحديد التاجر على أنه تاجر خاضع لمراقبة رد المبالغ المدفوعة (CMM) لمدة شهرين متتاليين.

محتويات تقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM)

- يجب أن يتضمن تقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) جميع المعلومات التالية:
- اسم وموقع التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM).
- الشهر التقويمي الذي يتم فيه الإبلاغ عن مؤهلات التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM).
- رمز عمل متقبل البطاقة/رمز فئة التاجر (MCC) المعين إلى التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) ووصف طبيعة عمل التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM).
- العدد والحجم الإجمالي بالدولار (GVD) لمعاملات مبيعات التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) في الشهر التقويمي الذي تم الإبلاغ فيه وفي الشهر السابق.
- العدد والحجم الإجمالي بالدولار (GVD) لعمليات رد المبالغ المدفوعة لمعاملات مبيعات التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) للشهر التقويمي الذي تم الإبلاغ فيه.
- أي معلومات إضافية قد يطلبها مشغل شبكة الدفع المحلية.

Late CMM Report Submission Assessment

If the National Scheme Operator determines that a Merchant is a CMM and the Acquirer fails to submit a timely CMM report for that Merchant, the National Scheme Operator may assess the Acquirer up to LYD XXXX per month for each month that a specific monthly CMM report is overdue.

Excessive Chargeback Merchant Reporting Requirements

- Within 30 days of the end of the second trigger month, and on a monthly basis thereafter, the Acquirer must submit a separate ECM report for each of its ECMs (in lieu of a CMM report) until that ECM's CTR is below 150 basis points for two consecutive months.
- The Acquirer also must provide a copy of the ECM report and these ECP Standards to the specific ECM.

The National Scheme Operator will assess the Acquirer a reporting fee of LYD XXX for each ECM report submitted.

- The Acquirer must continue to provide monthly ECM reporting until the Merchant is no longer identified as an ECM for two consecutive months. If during those months the Merchant is identified as a CMM, then the CMM reporting requirements will apply.

ECM Report Contents

The ECM report must include all of the information required for the CMM report, and the following additional information:

- A completed ECM Action Plan form
- An electronic file that contains chargeback Transaction details for each chargeback received by the Acquirer for the ECM in the calendar month
- Any additional information as the National Scheme Operator may require from time to time.

The National Scheme Operator will assess the Acquirer a reporting fee of LYD XXX for each ECM report submitted.

Late ECM Report Submission Assessment

If the National Scheme Operator determines that a Merchant is an ECM and the Acquirer fails to submit a timely ECM report for that ECM, the National Scheme Operator may assess the Acquirer up to LYD XXX per day for each of the first 15 days that the ECM report for that ECM is overdue and up to LYD XXXX a day thereafter until the delinquent ECM report is submitted.

تقييم التقديم المتأخر لتقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM)

إذا قرر مشغل شبكة الدفع المحلية أن التاجر هو تاجر خاضع لمراقبة رد المبالغ المدفوعة (CMM) وفشلت جهة القبول في تقديم تقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) في الوقت المناسب لذلك التاجر، فيجوز لمشغل شبكة الدفع المحلية تقييم جهة القبول حتى XXXX دينار ليبي شهريًا لكل شهر تأخر فيه تقديم تقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) الشهري المحدد.

متطلبات الإبلاغ عن تاجر رد المبالغ المدفوعة المفراط

- خلال 30 يومًا من نهاية شهر التشغيل الثاني، وعلى أساس شهري بعد ذلك، يجب على جهة القبول تقديم تقرير تاجر رد المبالغ المدفوعة المفراط (ECM) منفصل لكل من تاجر رد المبالغ المدفوعة المفراط (sECM) التابعين له (بدلاً من تقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM) حتى تكون نسبة رد المبالغ المدفوعة إلى معاملة (CTR) الخاصة بتاجر رد المبالغ المدفوعة المفراط (ECM) أقل من 150 نقاط أساسية لشهرين متتاليين.
- يجب على جهة القبول أيضًا تقديم نسخة من تقرير تاجر رد المبالغ المدفوعة المفراط (ECM) ومعايير برنامج رد المبالغ المدفوعة المفراط (ECP) هذه إلى التاجر الخاضع لمراقبة رد المبالغ المدفوعة المحدد.

سيقوم مشغل شبكة الدفع المحلية بتقييم جهة القبول برسوم الإبلاغ البالغة XXX دينار ليبي لكل تقرير تاجر رد المبالغ المدفوعة المفراط (ECM) مقدم.

- يجب أن تستمر جهة القبول في تقديم تقارير تاجر رد المبالغ المدفوعة المفراط (ECM) الشهرية حتى يتوقف تحديد التاجر على أنه تاجر رد المبالغ المدفوعة المفراط (ECM) لمدة شهرين متتاليين. وإذا تم تحديد التاجر خلال تلك الأشهر على أنه تاجر خاضع لمراقبة رد المبالغ المدفوعة (CMM)، فسيتم تطبيق متطلبات إعداد تقارير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM).

محتويات تقرير تاجر رد المبالغ المدفوعة المفراط (ECM)

يجب أن يتضمن تقرير تاجر رد المبالغ المدفوعة المفراط (ECM) جميع المعلومات المطلوبة لتقرير التاجر الخاضع لمراقبة رد المبالغ المدفوعة (CMM)، والمعلومات الإضافية التالية:

- نموذج خطة عمل مكتملة لتاجر رد المبالغ المدفوعة المفراط (ECM)
 - ملف إلكتروني يحتوي على تفاصيل معاملة رد المبالغ المدفوعة لكل عملية رد مدفوعات تتلقاها جهة القبول من أجل تاجر رد المبالغ المدفوعة المفراط (ECM) في الشهر التقويمي
 - أي معلومات إضافية قد يطلبها مشغل شبكة الدفع المحلية من وقت لآخر.
- سيقوم مشغل شبكة الدفع المحلية بتقييم جهة القبول برسوم الإبلاغ البالغة XXX دينار ليبي لكل تقرير تاجر رد المبالغ المدفوعة المفراط (ECM) مقدم.

تقييم التقديم التأخر لتقرير تاجر رد المبالغ المدفوعة المفراط (ECM)

إذا قرر مشغل شبكة الدفع المحلية أن التاجر هو تاجر رد المبالغ المدفوعة المفراط (ECM) وفشلت جهة القبول في تقديم تقرير تاجر رد المبالغ المدفوعة المفراط (ECM) في الوقت المناسب لتاجر رد المبالغ المدفوعة المفراط (ECM) ذلك، فإنه يجوز لمشغل شبكة الدفع المحلية تقييم جهة القبول حتى XXX دينار ليبي في اليوم لكل يوم من الأيام الخمسة عشر الأولى التي يتم فيها تقديم تقرير تاجر رد المبالغ المدفوعة المفراط (ECM) متأخر لتاجر رد المبالغ المدفوعة المفراط (ECM) ذلك وما يصل إلى XXXX دينار ليبي في اليوم بعد ذلك حتى يتم تقديم تقرير تاجر رد المبالغ المدفوعة المفراط (ECM) المتأخر.

6.7.8 Reporting Terminated Merchants

If either the Acquirer or the Merchant acts to terminate the acquiring relationship (such as by giving notice of termination) and, at the time of that act, the Acquirer has reason to believe that a condition described below exists, then the Acquirer must add the required information to the TMF within five calendar days of the earlier of either:

1. A decision by the Acquirer to terminate the acquiring relationship, regardless of the effective date of the termination, or
2. Receipt by the Acquirer of notice by or on behalf of the Merchant of a decision to terminate the acquiring relationship, regardless of the effective date of the termination.

The conditions that require TMF reporting are:

- Account data compromise
- Common point of purchase
- Laundering
- Excessive chargebacks
- Excessive fraud
- Fraud conviction
- Bankruptcy/liquidation/insolvency
- Violation of Standards
- Merchant collusion
- PCI Data Security Standard noncompliance
- Illegal transactions
- Identity theft

Acquirers must act diligently, reasonably, and in good faith to comply with TMF requirements. Acquirers may not use or threaten to use the TMF as a collection tool for minor Merchant discretionary activity. One of the above conditions must be met or suspected (at decision to terminate) to justify a Merchant addition. Acquirers that use or threaten to use the TMF as a collection tool for minor Merchant discretionary activity are subject to noncompliance assessments. An Acquirer that fails to enter a Merchant into the TMF is subject to a noncompliance assessment, and may be subject to an unfavorable ruling in a compliance case filed by a subsequent Acquirer of that Merchant.

6.8 Card Validation Number and Service Code Data

This Rule contains requirements relating to Card validation value (CVV) and service code, which are Card features designed to detect counterfeiting and other fraudulent use of Cards and Accounts. Card retention at the point-of-sale (POS) or ATM, the reporting of lost, stolen, and counterfeit Cards, and criminal investigations relating to counterfeit Cards.

6.8.1 Card Validation Number (CVV)

The CVV is a security feature designed to make it more difficult for counterfeiters to alter Cards and reuse them for fraudulent purposes.

CVV 1 and CVV 2 are mandatory security features for all Cards.

8.7.6 الإبلاغ عن التجار الذين فسخت العلاقة معهم

إذا كانت جهة القبول أو التاجر، يعملوا على فسخ عقد القبول (مثل إرسال إشعار بالإلغاء)، وكان لدى جهة القبول سبب للاعتقاد بوجود شرط موصوف أدناه، فيجب عليها إضافة المعلومات المطلوبة إلى ملف التاجر الذي فسخت عقده TMF خلال خمسة أيام تقويمية من أي مما يلي:

1. قرار من قبل جهة القبول بفسخ عقد القبول ، بغض النظر عن التاريخ الفعلي للفسخ.
2. استلام جهة القبول إخطاراً من لتاجر أو نيابة عنه بقرارفسخ عقد القبول، بغض النظر عن التاريخ الفعلي للفسخ.

الشروط التي تتطلب الإبلاغ عن ملف التاجر التي تم إنهاؤه TMF هي:

- اختراق في بيانات الحساب.
- نقطة الشراء المشتركة.
- غسيل أموال.
- رد المبالغ المدفوعة المفرط.
- الاحتيال المفرط.
- حكم بالاحتيال.
- الإفلاس / التصفية / الإعسار.
- انتهاك المعايير.
- تواطؤ التاجر.
- عدم الامتثال لمعيار أمان بيانات PCI.
- المعاملات غير القانونية.
- سرقة الهوية.

يجب أن يتصرف جهات القبول بجدية وعقلانية وبحسن نية للامتثال لمتطلبات ملف التاجر الذي تم إنهاؤه TMF.

قد لا تستخدم جهات القبول، أو يهددوا باستخدام ملف التاجر الذي تم فسخ عقده TMF كأداة تحصيل للنشاط التاجر التقديري البسيط. يجب استيفاء أحد الشروط المذكورة أعلاه أو الشك فيه (عند اتخاذ قرار الإلغاء) لتبرير إضافة التاجر. وجهات القبول التي تستخدم أو تهدد باستخدام ملف التاجر الذي تم فسخ عقده كأداة تحصيل للنشاط التقديري البسيط للتاجر يخضعون لتقييمات عدم الامتثال. وتخضع جهة القبول التي تفشل في إدخال التاجر إلى ملف التاجر الذي تم فسخ عقده TMF لتقييم عدم الامتثال، وقد يخضع لحكم غير موافٍ في قضية الامتثال المرفوعة من قبل جهة القبول اللاحق لذلك التاجر.

8.6 رقم التحقق من البطاقة، وبيانات رمز الخدمة

تحتوي هذه القاعدة على متطلبات، تتعلق بقيمة التحقق من البطاقة (CVV) ورمز الخدمة، وهما من ميزات البطاقة المصممة لاكتشاف التزوير والاستخدام الاحتيالي الآخر للبطاقات والحسابات. ويحتفظ بالبطاقة في نقاط البيع (POS) أو أجهزة الصراف الآلي، والإبلاغ عن البطاقات المفقودة والمسروقة والمزورة، والتحقيقات الجنائية المتعلقة بالبطاقات المزورة.

1.8.6 رقم التحقق من البطاقة (CVV)

قيمة التحقق من البطاقة (CVV) هي ميزة أمنية مصممة لتجعل من الصعب على المزورين تغيير البطاقات وإعادة استخدامها لأغراض احتيالية.

تعد قيمة التحقق من البطاقة (1 CVV) و قيمة التحقق من البطاقة (2 CVV) من ميزات الأمان الإلزامية لجميع البطاقات.

CVV 1 must be encoded on Track 1 and Track 2 in three contiguous positions in the Discretionary Data field of the magnetic stripe.

Chip CVV must be encoded in the Track 2 Equivalent Data field in three contiguous positions within the Discretionary Data field of the chip on all Chip Cards and must be different than the CVV 1 value encoded on the magnetic stripe.

NOTE: Due to the pseudo-random method by which the three-digit values for CVV 1, CVV 2, and Chip CVV are generated, there is approximately a one in 1,000 chance that the CVV 1 and Chip CVV values for a new or reissued Card will be identical. If the CVV 1 and Chip CVV are identical values based solely on chance, then the use of these identical values for a new or reissued Card is acceptable.

The following applies to contactless-enabled Cards (“Contactless Cards”) and Contactless Payment Devices:

- All magnetic stripe profile Contactless Cards and Contactless Payment Devices must generate a dynamic CVV 3.

6.8.1.1 Issuer Requirements for CVV 1

Issuers must:

- Encode the CVV 1 on Tracks 1 and 2
- Verify the encoded CVV 1 when processing a magnetic stripe-read authorization request

The Issuer verifies the CVV 1 value from the magnetic stripe-read data as transmitted in the authorization request during the online authorization process. The Issuer’s host can perform the verification.

Certification is required for Issuers to validate the CVV 1 value during the authorization process and to signal CVV 1 validation errors.

NOTE: Certification is required for Issuers to validate the CVV 1 value during the authorization process and to signal CVV 1 validation errors.

When an Issuer is “timed out” or unavailable, the Stand-In Processing Service provides an authorization request response. If an Issuer is signed up for CVV 1 verification, the Stand-In Processing Service performs an additional test to verify that the CVV 1 value is valid.

The National Scheme Operator may mandate participation in the CVV 1 verification in the Stand-In Processing Service for an Issuer with both 35 basis points of Transactions authorized by means of Stand-In processing and significant counterfeit activity within a calendar quarter.

6.8.1.2 Issuer Requirements for CVV 2

An Issuer must verify the CVV 2 value when provided by the Merchant and transmitted by the Acquirer in the Authorization Request message.

The Issuer must verify the CVV 2 value by providing a valid response code in the appropriate field of the Authorization Request Response or Financial Transaction Request Response.

يجب ترميز قيمة التحقق من البطاقة (1 CVV) في المسار 1 والمسار 2 في ثلاثة مواضع متجاورة في حقل البيانات التقديرية للشريط المغناطيسي.

يجب ترميز شريحة قيمة التحقق من البطاقة (CVV) في حقل البيانات المكافئة للمسار 2 في ثلاثة مواضع متجاورة داخل حقل البيانات التقديرية للشريحة على جميع بطاقات الشريحة، ويجب أن تكون مختلفة عن قيمة قيمة التحقق من البطاقة (1 CVV) المشفرة على الشريط المغناطيسي.

ملاحظة: نظرًا للطريقة الشبه عشوائية التي يتم من خلالها إنشاء القيم المكونة من ثلاثة أرقام لقيمة التحقق من البطاقة 1 CVV و قيمة التحقق من البطاقة 2 CVV و شريحة قيمة التحقق من البطاقة CVV، هناك احتمال واحد من كل 1000 تقريبًا أن تكون قيم قيمة التحقق من البطاقة 1 CVV و شريحة قيمة التحقق من البطاقة CVV لبطاقة جديدة أو المعاد إصدارها ستكون متطابقة. إذا كانت قيم قيمة التحقق من البطاقة 1 CVV و شريحة قيمة التحقق من البطاقة CVV متطابقة بناءً على الصدفة فقط، فإن استخدام هذه القيم المتطابقة لبطاقة جديدة أو معاد إصدارها مقبول.

ينطبق ما يلي على البطاقات التي تعمل بتقنية عدم الاتصال (“البطاقات غير المتصلة”) وأجهزة الدفع الغير متصلة:

- يجب أن تولد جميع البطاقات غير المتصلة وأجهزة الدفع الغير متصلة ذات الشريط المغناطيسي الممغنطة رمز ديناميكي لقيمة التحقق من البطاقة 3 CVV.

6.8.1.1.6 متطلبات جهة الإصدار لقيمة التحقق من البطاقة 1 CVV

يجب على جهات الإصدار:

- تشفير قيمة التحقق من البطاقة 1 CVV في المسارين 1 و 2.
- التحقق من رمز قيمة التحقق من البطاقة 1 CVV المشفر عند معالجة طلب تفويض المقروء بالشريط المغناطيسي.

أن جهة الإصدار تتحقق من قيمة قيمة التحقق من البطاقة 1 CVV من البيانات المقروءة بالشريط المغناطيسي، كما تم إرسالها في طلب التفويض أثناء عملية التفويض عبر الإنترنت. ويمكن لمضيف جهة الإصدار إجراء هذا التحقق.

ملاحظة: يجب على جهات الإصدار الحصول على الشهادة المطلوبة للتحقق من قيمة قيمة التحقق من البطاقة 1 CVV أثناء عملية التفويض والإشارة إلى أخطاء التحقق من قيمة التحقق من البطاقة CVV 1.

عند “انتهاء مهلة” جهة الإصدار أو عدم وجود مهلة، توفر خدمة المعالجة الاحتياطية استجابة لطلب التفويض. وإذا تم تسجيل جهة الإصدار للتحقق من قيمة التحقق من البطاقة 1 CVV، تقوم خدمة المعالجة الاحتياطية بإجراء اختبار إضافي للتحقق من صلاحية قيمة قيمة التحقق من البطاقة 1 CVV.

يجوز لمشغل شبكة الدفع المحلية أن يفرض المشاركة في التحقق من قيمة التحقق من البطاقة CVV 1 في خدمة المعالجة الاحتياطية لجهة الإصدار مع كل من 35 نقاط أساسية للمعاملات المصرح بها عن طريق المعالجة الاحتياطية ونشاط التزوير الكبير خلال ربع سنة تقويمي.

6.8.1.2.6 متطلبات جهة الإصدار لقيمة التحقق من البطاقة 2 CVV

- يجب أن تتحقق جهة الإصدار من قيمة قيمة التحقق من البطاقة 2 CVV عندما يقدمها التاجر وترسلها جهة القبول في رسالة طلب التفويض.
- يجب أن تتحقق جهة الإصدار من قيمة قيمة التحقق من البطاقة 2 CVV من خلال توفير رمز استجابة صالح في الحقل المناسب لاستجابة طلب التفويض أو استجابة طلب المعاملة المالية.

6.8.1.3 Issuer Requirements for Dynamic CVV 3

- An Issuer must enable a dynamic CVV 3 on the contactless chip for all magnetic stripe profile Contactless Transactions performed by Contactless Chip Cards and Contactless Payment Devices.
- All Contactless Chip Cards and Contactless Payment Devices that are capable of performing magnetic stripe profile Contactless Transactions must generate a dynamic CVV 3.
- An Issuer must verify the CVV 3 value and provide the result in the response when processing the authorization received from a Contactless Transaction.

6.8.1.4 Acquirer Requirements for CVV 2

- When the Merchant provides the CVV 2 value, the Acquirer must include the CVV 2 value in DE 48, subelement 92 of the Authorization Request/0100 message or Financial Transaction Request/0200 message.
- The Acquirer is also responsible for ensuring that the Merchant receives the CVV 2 response code provided by the Issuer in DE 48, subelement 87 of the Authorization Request Response/0110 message or Financial Transaction Request Response/0210 message.

6.8.1.5 CVV Calculation Methods

The Issuer may calculate the CVV 1, CVV 2, and Chip CVV by one of two methods:

- Issuer proprietary calculation—which gives the Issuer the option to derive the CVV algorithmically.
- Data Encryption Standard (DES) software—where the Issuer can perform the calculation through a DES software application within a host system or through use of a tamper-resistant security module (TRSM).

Issuers that choose the DES software method must use the DES algorithm procedure to generate the CVV 1, CVV 2, and Chip CVV.

The DES algorithm procedure is described below and is also published in the following documents:

- ANSI X3.92-1981 American National Standard, Data Encryption Algorithm
- ISO/IEC 18033-3:2010, Information technology—Security techniques—Encryption algorithms—Part 3: Block ciphers (see Annex A)

The DES method algorithm generates the three-digit CVV 1 for the Discretionary Data field of Track 1 and Track 2. The Issuer also uses this method to develop the three-digit CVV 2 and Chip CVV. This algorithm procedure applies only to Issuers that implement the CVV generation process in their host systems.

3.1.8.6. متطلبات جهة الإصدار لقيمة التحقق من البطاقة CVV 3 الديناميكي

- يجب على جهة الإصدار تمكين قيمة التحقق من البطاقة CVV 3 الديناميكي على الشريحة غير المتصلة لجميع المعاملات الغير متصلة للشريط المغناطيسي التي يتم إجراؤها بواسطة بطاقات الشريحة غير المتصلة وأجهزة الدفع الغير متصلة.
- يجب أن تولد جميع بطاقات الشريحة غير المتصلة وأجهزة الدفع الغير متصلة القدرة على أداء المعاملات الغير متصلة للشريط المغناطيسي رمز قيمة التحقق من البطاقة CVV 3 ديناميكياً.
- يجب على جهة الإصدار التحقق من قيمة قيمة التحقق من البطاقة CVV 3 وتقديم النتيجة في الاستجابة عند معالجة التفويض المستلم من معاملة غير متصلة.

4.1.8.6. متطلبات جهة القبول لقيمة التحقق من البطاقة CVV 2

- يجب على جهة القبول عندما يقدم التاجر قيمة قيمة التحقق من البطاقة CVV 2، تضمين قيمة قيمة التحقق من البطاقة CVV 2 في DE 48، أو العنصر الفرعي 92 من رسالة طلب التفويض / 0100 أو رسالة طلب المعاملة المالية / 0200.
- جهة القبول هي المسؤولة أيضاً على ضمان استلام التاجر لرمز استجابة قيمة التحقق من البطاقة CVV 2 المقدم من جهة الإصدار في DE 48، أو العنصر الفرعي 87 من رسالة استجابة طلب التفويض / 0110 أو رسالة استجابة طلب المعاملة المالية / 0210.

5.1.8.6. طرق حساب قيمة التحقق من البطاقة CVV

- يجوز لجهة الإصدار حساب قيمة التحقق من البطاقة CVV 1 و قيمة التحقق من البطاقة CVV 2 و شريحة قيمة التحقق من البطاقة بإحدى طريقتين:
- حساب ملكية جهة الإصدار - والذي يمنح جهة الإصدار خيار اشتقاق رمز التحقق من البطاقة CVV بطريقة حسابية.
- من خلال برنامج معيار تشفير البيانات (DES) - حيث يمكن لجهة الإصدار إجراء الحساب من خلال تطبيق برنامج معيار تشفير البيانات ضمن نظام مضيف أو من خلال استخدام وحدة أمان مقاومة للعبث (TRSM).

يجب أن تستخدم جهات الإصدار التي تختار طريقة برنامج معيار تشفير البيانات (DES) إجراء خوارزمية معيار تشفير البيانات (DES)، لإنشاء قيمة التحقق من البطاقة CVV 1 و قيمة التحقق من البطاقة CVV 2 و شريحة قيمة التحقق من البطاقة CVV.

يتم وصف إجراء خوارزمية معيار تشفير البيانات (DES) أدناه ويتم نشره أيضاً في المستندات التالية:

- ANSI X3.92-1981 المعيار الوطني الأمريكي، خوارزمية تشفير البيانات
- ISO / IEC 18033-3: 2010، تكنولوجيا المعلومات - تقنيات الأمن - خوارزميات التشفير - الجزء 3: الأصفار الكتلية (انظر الملحق أ)

تقوم خوارزمية طريقة معيار تشفير البيانات (DES) بتوليد قيمة التحقق من البطاقة CVV 1 المكون من ثلاثة أرقام لحقل البيانات التقديرية للمسار 1 والمسار 2. كما تستخدم جهة الإصدار هذه الطريقة لتطوير قيمة التحقق من البطاقة CVV 2 المكون من ثلاثة أرقام وشريحة قيمة التحقق من البطاقة CVV. وينطبق إجراء الخوارزمية هذا، فقط على جهات الإصدار التي تنفذ عملية إنشاء رمز التحقق من البطاقة CVV في أنظمتهم المضيفة.

Two 64-bit cryptographic DES keys must be used in the generation process. An Issuer is permitted to use the same two 64-bit DES keys for generating the CVV 1, CVV 2, and Chip CVV (but not the dynamic CVV 3), provided that separate service codes are used. The same keys should not be shared among multiple Issuers, such as when Issuers use a common Service Provider for CVV 1, CVV 2, and Chip CVV processing.

Issuers are strongly discouraged from using a CVV 2 value of “000.”

The DES algorithm procedure is performed by following the eight steps below:

1. If the primary account number (PAN) is longer than 16 digits, extract the last 16 digits of the PAN.
2. Construct a string of bits by concatenating (left to right) the sequence of 4-bit values (or nibbles), each of which is the binary representation of a numeric digit in the CVV Data Elements, in the order indicated in Table 6.6:

NOTE: The Issuer must perform independent calculations to produce each CVV value.

Table 6.6—CVV Data Elements

(See appendix number 50)

3. Apply ISO/IEC 9797-1 (Information technology—Security techniques—Message Authentication Codes [MACs]—Part 1: Mechanisms using a block cipher) “MAC Algorithm 3”, “Padding Method 1” to the string created in Step 2, using two independent DES keys, to produce an 8-byte result.
4. From the result of Step 3, going from left to right, a nibble at a time, extract all nibbles that correspond to numeric digits (0-9); left-justify these digits in a 16-position field.
5. From the result of Step 3, going from left to right, a nibble at a time, extract all nibbles that correspond to hexadecimal characters (A-F). To compensate for hexadecimal, subtract 10 from each extracted hexadecimal digit.
6. Concatenate the resulting digits from Step 5 to the right of the digits extracted in Step 4.
7. Set the CVV to the first three left-most digits of the decimal string created in Step 6.
8. Run the program three times, once for each CVV, using the CVV data elements indicated in Table 3.1.

The output from Step 1 is 16 digits long. The resulting string reflects 23 digits (16+4+3) and is 92 bits long.

يجب استخدام مفتاحي معيار تشفير البيانات (64 DES) بت المشفرين في عملية الإنشاء. يُسمح لجهة الإصدار باستخدام نفس مفتاحي معيار تشفير البيانات 64 بت لإنشاء قيمة التحقق من البطاقة CVV 1 و قيمة التحقق من البطاقة CVV 2 و شريحة قيمة التحقق من البطاقة CVV (لكن ليس قيمة التحقق من البطاقة CVV 3 الديناميكي)، وبشرط استخدام رموز خدمة منفصلة. ولا ينبغي مشاركة نفس المفاتيح بين عدة جهات إصدار، كما هو الحال عندما تستخدم جهات الإصدار مقدم خدمة مشتركًا لمعالجة قيمة التحقق من البطاقة CVV 1 و قيمة التحقق من البطاقة CVV2 و شريحة قيمة التحقق من البطاقة CVV.

لا يُنصح جهات الإصدار باستخدام قيمة التحقق من البطاقة CVV 2 لقيمة “000.”

يتم تنفيذ إجراء خوارزمية معيار تشفير البيانات DES باتباع الخطوات الثمانية أدناه:

1. إذا كان رقم الحساب الأساسي أطول من 16 رقمًا، يتم استخراج آخر 16 رقمًا من رقم الحساب الأساسي.
2. يتم بناء سلسلة من البتات عن طريق تسلسل (من اليسار إلى اليمين) تسلسل قيم 4 بت (أو العايب)، كل منها يمثل التمثيل الثنائي لرقم رقمي في عناصر بيانات قيمة التحقق من البطاقة CVV ، وبالترتيب الموضح في الجدول 6.6:

ملاحظة: يجب على جهة الإصدار إجراء حسابات مستقلة لإنتاج كل قيمة لقيمة التحقق من البطاقة CVV

الجدول 6.6 - عناصر بيانات قيمة التحقق من البطاقة CVV

(انظر الملحق رقم 50)

3. تطبيق ISO / IEC 9797-1 (تقنية المعلومات - تقنيات الأمان - رموز مصادقة الرسائل [MACs]- الجزء 1: الآليات التي تستخدم تشفير الكتلة) “خوارزمية MAC 3”، “طريقة الحشو 1” على السلسلة التي تم إنشاؤها في الخطوة 2، باستخدام مفتاحي معيار تشفير البيانات DES مستقلين، لإنتاج نتيجة 8 بايت.
4. من نتيجة الخطوة 3، الانتقال من اليسار إلى اليمين، عاب في كل مرة ، يتم استخراج كل العايب الذي يتوافق مع الأرقام الرقمية (0-9) ؛ اليسار - ضبط هذه الأرقام في حقل ذي 16 موضعًا.
5. من نتيجة الخطوة 3، بالانتقال من اليسار إلى اليمين، عاب في كل مرة، يتم استخراج جميع العايب الذي يتوافق مع الأحرف السداسية العشرية (A – F). للتعويض عن النظام الست عشري، يتم طرح 10 من كل رقم سداسي عشري مستخرج.
6. يتم ربط الأرقام الناتجة من الخطوة 5 إلى يمين الأرقام المستخرجة في الخطوة 4.
7. يتم تعيين رمز التحقق من البطاقة CVV على أول ثلاثة أرقام في أقصى اليسار من السلسلة العشرية التي تم إنشاؤها في الخطوة 6.
8. يتم تشغيل البرنامج ثلاث مرات، مرة واحدة لكل قيمة التحقق من البطاقة CVV، باستخدام عناصر بيانات قيمة التحقق من البطاقة CVV الموضحة في الجدول 3.1.

طول الإخراج من الخطوة 1 يبلغ 16 رقمًا. تعكس السلسلة الناتجة 23 رقمًا (3 + 4 + 16) ويبلغ طولها 92 بتًا.

6.8.2 Service Codes

The service code, a three-digit number that complies with ISO/IEC 7813, is encoded on Track 1 and Track 2 of the magnetic stripe of a Card and indicates to a magnetic stripe-reading terminal the Transaction acceptance parameters of the Card. Each digit of the service code represents a distinct element of the Issuer's Transaction acceptance policy. However, not all combinations of valid digits form a valid service code, nor are all service code combinations valid for all Card Programs. Issuers must encode only one service code on Cards, and the same value must be encoded on both Track 1 and Track 2 in their respective, designated positions.

Service codes provide Issuers with flexibility in defining Card acceptance parameters, and provide Acquirers with the ability to interpret Issuers' Card acceptance preferences for all POI conditions.

Service codes apply to magnetic stripe-read Transactions only. In the case of Chip Cards used in Hybrid Terminals, the Hybrid Terminal uses the data encoded in the chip to complete the Transaction. (A Hybrid Terminal is a Terminal that accepts both magnetic stripe and Chip Cards.)

NOTE: A value of 2 or 6 in position 1 of the service code indicates that a chip is present on a Card, which contains the same payment application as is present on the magnetic stripe.

6.8.2.1 Issuer Information

Issuers are recommended to use one of the following service code values for most Cards:

- For magnetic stripe Cards—501 (national use only Card, normal authorization, normal Cardholder verification, no restrictions); or
- For Chip Cards—601 (national use only integrated circuit Card, normal authorization, normal Cardholder verification, no restrictions).

Issuers are permitted to use a different value in position 3 of the service code to support PIN requirements, as follows:

- A value of 0 to indicate PIN is always required;
- A value of 3 to indicate the Card is an ATM-only Card and PIN is always required;
- A value of 6 to indicate that if the Terminal has a PIN pad, the Cardholder should be prompted to provide a PIN.

6.8.2.2 Acquirer Information

Acquirers must ensure that their Hybrid Terminals do not reject or otherwise decline to complete a Transaction solely because of the service code encoded on the magnetic stripe. Acquirers are not required to act on the service codes at this time unless a value of 2 or 6 is present in position 1 of the service code. The Hybrid Terminal must first attempt to process the Transaction as a Chip Transaction.

6.9 Card Recovery and Return

The following sections address Member responsibilities associated with Card retention and return, rewards for Card capture, reporting of lost and stolen Cards, and criminal and counterfeit investigations.

2.8.6. رموز الخدمة

رمز الخدمة هو رقم مكون من ثلاثة أرقام يتوافق مع ISO / IEC 7813، يتم ترميزه على المسار 1 والمسار 2 من الشريط المغناطيسي للبطاقة، ويشير إلى محطة مقروءة بالشريط مغناطيسي إلى معايير قبول المعاملة الخاصة بالبطاقة. ويمثل كل رقم من رموز الخدمة عنصرًا مميزًا في سياسة قبول المعاملات الخاصة بجهة الإصدار. ومع ذلك، لا تشكل جميع مجموعات الأرقام الصالحة رمز خدمة صالحًا، كما أن جميع مجموعات رموز الخدمة ليست صالحة لجميع برامج البطاقات. ويجب أن تقوم جهات الإصدار بترميز رمز خدمة واحد فقط على البطاقات، ويجب عليها تشفير نفس القيمة على كل من المسار 1 والمسار 2 في المواضع المخصصة لكل منهما.

توفر رموز الخدمة لجهات الإصدار مرونة في تحديد معايير قبول البطاقة، وتزود جهات القبول بالقدرة على تفسير تفضيلات قبول بطاقات جهات الإصدار لجميع شروط نقاط البيع.

تنطبق رموز الخدمة على المعاملات المقروءة بالشريط المغناطيسي فقط. وفي حالة بطاقات الشريحة المستخدمة في المحطات الهجينة، تستخدم المحطة الهجينة البيانات المشفرة في الشريحة لإكمال المعاملة. (المحطة الهجينة هي محطة تقبل كل من الشريط المغناطيسي وبطاقات الشريحة).

ملاحظة: تشير القيمة 2 أو 6 في الموضع 1 من رمز الخدمة إلى وجود شريحة على البطاقة، والتي تحتوي على نفس تطبيق الدفع الموجود على الشريط المغناطيسي.

1.2.8.6. معلومات جهة الإصدار

يُنصح جهات الإصدار باستخدام إحدى قيم رمز الخدمة التالية لإغلب البطاقات:

- بالنسبة للبطاقات ذات الشريط المغناطيسي - 501 (بطاقة الاستخدام المحلي فقط، التفويض العادي، التحقق العادي من حامل البطاقة، بلا قيود).
- بالنسبة للبطاقات ذات الشريحة- 601 (بطاقة الدوائر المتكاملة للاستخدام المحلي فقط، التفويض العادي، التحقق العادي من حامل البطاقة، بلا قيود).
- يُسمح لجهات الإصدار باستخدام قيمة مختلفة في الموضع 3 من رمز الخدمة لدعم متطلبات رقم التعريف الشخصي، على النحو التالي:
 - قيمة 0 للإشارة إلى رقم التعريف الشخصي مطلوبة دائمًا.
 - قيمة 3 للإشارة إلى أن البطاقة هي بطاقة جهاز صراف آلي فقط، ودائمًا ما يلزم إدخال رقم التعريف الشخصي.
 - القيمة 6 للإشارة إلى أنه إذا كانت المحطة تحتوي على لوحة رقم التعريف الشخصي، فيجب أن يُطلب من حامل البطاقة فوراً تقديم رقم التعريف الشخصي.

2.2.8.6. معلومات جهة القبول

يجب على جهات القبول أن تتحقق من أن المحطات الهجينة الخاصة بهم لا تقبل أو ترفض إتمام المعاملة فقط بسبب رمز الخدمة المشفر على الشريط المغناطيسي. لا يُطلب من جهات القبول التصرف وفقًا لرموز الخدمة في هذا الوقت ما لم تكن القيمة 2 أو 6 موجودة في الموضع 1 من رمز الخدمة. ويجب أن تحاول المحطة الهجينة أولاً معالجة المعاملة كمعاملة شريحة.

6.9.1 Merchant Card Retention and Return

Acquirers and Merchants should use their best efforts to recover a Card by reasonable and peaceful means if:

- The Issuer advises the Acquirer or Merchant to recover the Card in response to an authorization request.
 - The Electronic Warning Bulletin file or Warning Notice lists the account number.
- After recovering a Card, the recovering Acquirer or Merchant must notify its authorization center or its Acquirer and receive instructions for returning the Card. If mailing the Card, the recovering Acquirer or Merchant first should cut the Card in half through the magnetic stripe.

6.9.1.1 Returning Recovered Cards

The Acquirer must follow these procedures when returning a recovered Card to the Issuer:

1. If the Merchant has not already done so, the Acquirer must render the Card unusable by cutting it in half vertically through the magnetic stripe.
2. The Acquirer must forward the recovered Card to the Issuer within five calendar days of receiving the Card along with the required Card recovery form. A recovered Card must be returned to the Security Contact of the Issuer.

A Merchant may return a Card inadvertently left at the Merchant location if the Cardholder claims the Card before the end of the next business day and presents positive identification. With respect to unclaimed Cards, a Merchant must follow the Acquirer's requirements as set forth in the Merchant Agreement.

6.9.1.2 Returning Counterfeit Cards

The Acquirer or Merchant must return counterfeit Cards to the Issuer by following the instructions provided by its authorization center. The following information identifies an Issuer:

- The Issuer's name and/or logo on the Card front
- The Licensee Acknowledgement Statement

In the absence of an Issuer's name/logo or Licensee Acknowledgement Statement, the Acquirer should attempt to identify the Issuer by other means, such as the Issuer's bank identification number (BIN) printed on the front or back of the Card or the magnetic stripe. If the Issuer is still unidentifiable, the Acquirer should return the Card to the National Scheme Operator.

NOTE: The above method of identifying the Issuer applies only to the return of a counterfeit Card, not to determining the Member responsible for the counterfeit losses associated with such Cards.

9.6. استرداد وإعادة البطاقة

تتناول الأقسام التالية مسؤوليات الأعضاء المرتبطة بالاحتفاظ بالبطاقة وإعادتها، ومكافآت الاستيلاء على البطاقة، والإبلاغ عن البطاقات المفقودة والمسرقة، والتحقيقات الجنائية والتزوير.

1.9.6. الاحتفاظ وإعادة بطاقة التاجر

يجب على جهات القبول، والتجار أن يبذلوا قصارى جهدهم لاسترداد البطاقة بالوسائل المعقولة والسلمية إذا:

- تنصح جهة الإصدار الجهة القابلة أو التاجر باسترداد البطاقة استجابةً لطلب التفويض.
 - يسرد ملف نشرة التحذير الإلكترونية أو إخطار التحذير رقم الحساب.
- يجب على جهة القبول، أو التاجر بعد استرداد البطاقة، إخطار مركز التفويض الخاص به أو القابل التابع له، وتلقي تعليمات لإعادة البطاقة. وفي حالة إرسال البطاقة بالبريد، يجب على جهة القبول أو التاجر الذي قام بالاسترداد أولاً قطع البطاقة إلى نصفين من خلال الشريط المغناطيسي.

1.1.9.6. إعادة البطاقات المستردة

- يجب على جهة القبول اتباع هذه الإجراءات عند إعادة البطاقة المستردة إلى جهة الإصدار:
1. إذا لم يقم التاجر بذلك بالفعل، فيجب على جهة القبول أن تجعل البطاقة غير صالحة للاستعمال عن طريق قصها إلى نصفين عمودياً عبر الشريط المغناطيسي.
 2. يجب على جهة القبول إرسال البطاقة المستردة إلى جهة الإصدار خلال خمسة أيام تقويمية من استلام البطاقة مع نموذج استرداد البطاقة المطلوب. ويجب إعادة البطاقة المستردة إلى جهة اتصال الآمنة الخاصة بجهة الإصدار.

يجوز للتاجر إعادة البطاقة التي تركت عن غير قصد في موقع التاجر إذا طالب حامل البطاقة بالبطاقة قبل نهاية يوم العمل التالي وقدم هوية إيجابية.

وفيما يتعلق بالبطاقات التي لم تتم المطالبة بها، يجب على التاجر اتباع متطلبات جهة القبول على النحو المنصوص عليه في اتفاقية التاجر.

2.1.9.6. إعادة البطاقات المزورة

يجب على جهة القبول أو التاجر إعادة البطاقات المزورة إلى جهة الإصدار باتباع الإرشادات المقدمة من مركز التفويض الخاص به. تحدد المعلومات التالية جهة الإصدار:

- اسم و شعار جهة الإصدار على واجهة البطاقة.
- بيان إقرار المرخص له.

في حالة عدم وجود اسم، وشعار جهة الإصدار أو بيان إقرار المرخص له، يجب على جهة القبول محاولة تحديد هوية جهة الإصدار بوسائل أخرى، مثل رقم تعريف المصرفي الخاص بجهة الإصدار المطبوع على الجزء الأمامي أو الخلفي من البطاقة أو الشريط المغناطيسي. إذا كانت جهة الإصدار غير معروفة، يجب على جهة القبول إعادة البطاقة إلى مشغل شبكة الدفع المحلية.

ملاحظة: الطريقة المذكورة أعلاه لتحديد هوية جهة الإصدار تنطبق فقط على إعادة البطاقة المزورة، وليس لتحديد العضو المسؤول عن الخسائر المزورة المرتبطة بهذه البطاقات.

6.9.1.3 Liability for Loss, Costs, and Damages

Neither the National Scheme Operator nor any Member shall be liable for loss, costs, or other damages for claims declared against them by an Issuer for requested actions in the listing of an account or a Group or Series listing on the Electronic Warning Bulletin file or in the applicable regional Warning Notice by the Issuer.

If an Acquirer erroneously uses these procedures without the Issuer's guidance and authorizes Merchant recovery of a Card not listed on the Electronic Warning Bulletin file or Warning Notice, neither The National Scheme Operator or its Members shall be liable for loss, costs, or other damages if a claim is made against them.

No Member is liable under this section for any claim unless the Member has:

- Written notice of the assertion of a claim within 120 days of the assertion of the claim, and
- Adequate opportunity to control the defense or settlement of any litigation concerning the claim.

6.9.2 ATM Card Retention and Return

Card retention must occur only at the Issuer's command. Cards captured because of ATM Terminal malfunction or Cardholder error, over which the ATM Terminal owner has no control, are the only allowable exceptions. If the ATM Acquirer cannot determine within two business days if a Card was captured because of a machine malfunction, Cardholder error, or a command sent by the Issuer, the Card will be deemed to be a Card captured on command of the Issuer.

An ATM Terminal Acquirer that as an Issuer sends Card capture commands must honor the commands sent by other Issuers at all of its ATMs that are capable of Card capture.

6.9.2.1 Handling ATM-Retained Cards

An ATM Terminal Acquirer must handle retained Cards in accordance with the following requirements:

1. Log all retained Cards under dual control immediately upon removal from the ATM.
2. Destroy retained Cards by cutting them in half vertically through the magnetic stripe, if the Card is captured on command of the Issuer or if an Acquirer's procedures do not include returning retained Cards to Cardholders.

When a captured card appears to be fraudulent (for example, a plain white plastic or cardboard card), the Acquirer may (at its option) retain, preserve, and release such card to appropriate law enforcement authorities.

6.9.2.2 Returning ATM-Retained Cards to Cardholders

Cards retained at the request of an Issuer must never be returned to the Cardholder without the permission of the Issuer. However, Cards erroneously retained by the Acquirer because of a machine malfunction, system failure, or Cardholder error may be held at the ATM location, in a secure place, for two business days following capture and released to the Cardholder subsequent to all of the following:

3.1.9.6. المسؤولية عن الخسائر والتكاليف والأضرار

لا يتحمل مشغل شبكة الدفع المحلية، ولا أي عضو المسؤولية عن الخسائر أو التكاليف أو الأضرار الأخرى للمطالبات المعلنة ضدهم من قبل جهة الإصدار عن الإجراءات المطلوبة في إدراج حساب أو مجموعة أو سلسلة قائمة في ملف نشرة التحذير الإلكترونية أو في إخطار التحذير المحلي المعمول به من قبل جهة الإصدار.

إذا استخدمت جهة القبول هذه الإجراءات عن طريق الخطأ، دون توجيهات جهة الإصدار، وأذن للتاجر باسترداد بطاقة غير مدرجة في ملف نشرة التحذير الإلكترونية أو إخطار التحذير، فلن يكون مشغل شبكة الدفع المحلية أو أعضائه مسؤولين عن الخسائر أو التكاليف أو الأضرار الأخرى إذا تم تقديم مطالبة ضدهم.

لا يتحمل أي عضو بموجب هذا القسم مسؤولية أي مطالبة ما لم يكن لدى العضو:

- إخطار مكتوب بتأكيد المطالبة خلال 120 يومًا من تأكيد المطالبة.
- فرصة كافية للسيطرة على الدفاع أو تسوية أي دعوى قضائية تتعلق بالمطالبة.

2.9.6. الاحتفاظ وإعادة بطاقة جهاز الصراف الآلي

يجب أن يتم الاحتفاظ بالبطاقة، فقط بأمر من جهة الإصدار. تعتبر البطاقات التي تم الاستيلاء عليها بسبب عطل في جهاز الصراف الآلي أو بخطأ حامل البطاقة، والتي لا يتحكم فيها مالك جهاز الصراف الآلي، هي الاستثناءات الوحيدة المسموح بها. إذا لم تتمكن الجهة القابلة على جهاز الصراف الآلي من تحديد ما إذا تم الاستيلاء على البطاقة خلال يومي عمل بسبب عطل في الجهاز أو خطأ حامل البطاقة أو أمر أرسله جهة الإصدار، فسيتم اعتبار البطاقة على أنها بطاقة تم الاستيلاء عليها بأمر من جهة الإصدار.

يجب على الجهة القابلة على جهاز الصراف الآلي الذي يرسل أوامر الاستيلاء على البطاقة، بصفته جهة الإصدار، أن تلتزم بالأوامر التي ترسلها جهات الإصدار الأخرى في جميع أجهزة الصراف الآلي الخاصة بها القادرة على الاستيلاء البطاقة.

1.2.9.6. التعامل مع بطاقات الصراف الآلي المحتفظ بها

يجب على على الجهة القابلة على أجهزة الصراف الآلي التعامل مع البطاقات المحتفظ بها وفقًا للمتطلبات التالية:

1. تسجيل جميع البطاقات المحتفظ بها تحت تحكم مزدوج فور إخراجها من جهاز الصراف الآلي.
2. إتلاف البطاقات المحتفظ بها عن طريق قصها إلى نصفين عموديًا من خلال الشريط المغناطيسي، إذا تم التقاط البطاقة بأمر من جهة الإصدار، أو إذا كانت إجراءات الجهة القابلة لا تتضمن إعادة البطاقات المحتفظ بها إلى حاملي البطاقات.

عندما تكون البطاقة التي تم الاستيلاء عليها مزورة (على سبيل المثال ، بطاقة بلاستيكية بيضاء عادية أو كرتونية)، يجوز لجهة القبول (حسب اختيارها) الاحتفاظ بهذه البطاقة وحفظها وتسليمها للسلطات المختصة بتطبيق القانون.

2.2.9.6. إعادة بطاقات الصراف الآلي إلى حاملي البطاقات

يجب عدم إعادة البطاقات المحتفظ بها بناءً على طلب جهة الإصدار إلى حامل البطاقة دون الحصول على إذن من جهة الإصدار. ومع ذلك، قد يتم الاحتفاظ بالبطاقات التي تحتفظ بها جهة القبول عن طريق الخطأ بسبب عطل في الجهاز أو فشل النظام أو خطأ حامل البطاقة في موقع جهاز الصراف الآلي، في مكان آمن، لمدة يومين عمل بعد الاستيلاء عليها وإصدارها إلى حامل البطاقة بعد كل ما يلي:

1. The Acquirer checks the Electronic Warning Bulletin file or Warning Notice.
2. The Cardholder presents reasonable identification (for example, a current driver's license, passport, or similar identification with a picture or descriptive data and a signature that is comparable to the signature on the captured Card, if applicable).
3. The Cardholder signs a disposition log or receipt, or the Acquirer otherwise maintains a record of the action taken.

The Acquirer then must notify the Issuer and explain that the Card was retained, the circumstances of the retention, and that the Card was returned to the Cardholder.

If the Cardholder does not return to claim the Card before the end of the second business day following Card capture, the Card's magnetic stripe must be destroyed.

An Acquirer will not incur liability for fraudulent or unauthorized Transactions initiated with a Card that such Acquirer has returned to a Cardholder following the Card's capture at an ATM Terminal, provided that the Acquirer complied with the requirements described in this section.

6.9.2.3 Fees for ATM Card Retention and Return

The Acquirer must not charge the Issuer any fee for the ATM retention or return of a Card.

6.9.3 Payment of Rewards

The Acquirer may, at its option, pay the Merchant or financial institution teller a reward for capturing a Card in accordance with local practice. The person capturing the Card receives the reward.

The Acquirer must follow these Standards when paying a reward:

1. Pay no less than LYD XXX to the Merchant capturing a Card listed on the Electronic Warning Bulletin file or Warning Notice;
2. Pay the Merchant LYD XXX, if a Merchant initiates an authorization call because of a suspicious Transaction or captures a Card not listed on the Electronic Warning Bulletin file or Warning Notice.
3. Pay a reward to a financial institution teller for the capture of another Member's Card if it is the Acquirer's practice to pay its tellers rewards for picking up its own Cards. The amount of the reward should be the same amount paid for the capture of the Acquirer's own Cards as described in Table 6.8.

6.9.3.1 Reward Amounts

The Acquirer should follow these guidelines for determining reward amounts.

Table 6.8—Reward Amount Determinations

(See appendix number 51)

The stipulation that the person capturing the recovered Card receives the reward does not prevent Members from making mutually acceptable agreements between themselves regarding rewards.

The recovering Member may collect an administrative fee of LYD XX for expenses incurred in processing the captured Card. The capturing Member may add this fee to the amount of the reward reimbursement or collect the fee independently, using the Fee Collection message through the National Scheme Operator system.

1. تحقق جهة القبول من ملف نشرة التحذير الإلكترونية أو إخطار التحذير.
2. يقدم حامل البطاقة هوية معقولة (على سبيل المثال، رخصة القيادة الحالية، أو جواز السفر أو تعريف مماثل مع صورة أو بيانات وصفية وتوقيع مشابه للتوقيع على البطاقة المحتفظ بها، إن أمكن).

3. يوقع حامل البطاقة على سجل التصرف أو الإيصال، أو تحتفظ جهة القبول بسجل للإجراء المتخذ. يجب على جهة القبول بعد ذلك إخطار جهة الإصدار وتوضيح أنه تم الاحتفاظ بالبطاقة وظروف الاحتفاظ بها وأن البطاقة قد أعيدت إلى حامل البطاقة.

وإذا لم يعد حامل البطاقة للمطالبة بالبطاقة قبل نهاية يوم العمل الثاني بعد الاحتفاظ بالبطاقة، فيجب إتلاف الشريط المغناطيسي للبطاقة.

جهة القبول لا تتحمل المسؤولية عن المعاملات الاحتيالية أو غير المصرح بها، والتي بدأت ببطاقة أعادتها جهة القبول إلى حامل البطاقة بعد الاستيلاء على البطاقة في جهاز الصراف الآلي، شريطة أن تلتزم جهة القبول بالمتطلبات الموضحة في هذا القسم.

3.2.9.6 رسوم الاحتفاظ ببطاقة الصراف الآلي وإعادتها

يجب ألا تفرض جهة القبول على جهة الإصدار أي رسوم مقابل الاحتفاظ بأجهزة الصراف الآلي أو إرجاع البطاقة.

3.9.6 دفع المكافآت

يجوز لجهة القبول وحسب اختيارها، أن تدفع للتاجر أو صراف المؤسسة المالية مكافأة مقابل الاستيلاء على البطاقة وفقًا للممارسات المحلية. يتلقى الشخص الذي يستولي على البطاقة المكافأة. يجب على جهة القبول اتباع هذه المعايير عند دفع المكافأة:

1. دفع ما لا يقل عن XXX دينار ليبي للتاجر الذي يستولي على بطاقة مدرجة في ملف نشرة التحذير الإلكترونية أو إخطار التحذير.
2. دفع التاجر XXX دينار ليبي، إذا بدأ التاجر مكاملة تفويض بسبب معاملة مشبوهة أو استولى على بطاقة غير مدرجة في ملف نشرة التحذير الإلكترونية أو إخطار التحذير.
3. دفع مكافأة لصراف مؤسسة مالية مقابل الاستيلاء على بطاقة عضو آخر، إذا كانت ممارسة جهة القبول هي دفع مكافآت لصرافيه مقابل الحصول على البطاقات الخاصة به. ويجب أن يكون مبلغ المكافأة هو نفس المبلغ المدفوع للاستيلاء على بطاقات جهة القبول الخاصة بها كما هو موضح في الجدول 6.8.

1.3.9.6 قيم مبالغ المكافأة

يجب على على جهة القبول اتباع هذه الإرشادات لتحديد مبالغ المكافأة.

الجدول 6.8 - تحديد قيمة مبلغ المكافأة

(انظر الملحق رقم 51)

ولا يمنع اشتراط حصول الشخص الذي يستولي على البطاقة المستردة على المكافأة، الأعضاء من إبرام عقود فيما بينهم تتعلق بالمكافآت.

يجوز للعضو الذي قام بالاسترداد تحصيل رسوم إدارية بقيمة XX دينار ليبي للمصاريف المتكبدة في معالجة البطاقة التي تم الاستيلاء عليها. ويجوز للعضو الذي قام بالاستيلاء إضافة هذه الرسوم إلى مبلغ تعويض المكافأة أو تحصيل الرسوم بشكل مستقل، باستخدام رسالة تحصيل الرسوم من خلال نظام مشغل شبكة الدفع المحلية.

6.9.3.2 Reimbursement of Rewards

The following specifications apply to reward reimbursement:

- Upon dispatching the Card to the Issuer, the Acquirer will obtain reimbursement for the reward paid and the LYD XX fee by processing the Fee Collection message through the National Scheme Operator System.
- If a Member returns a Card to an Issuer and a reward is not paid, the recovering Member may, at its discretion, collect a LYD XX fee by processing a Fee Collection message record.
- Upon receipt of the Interchange Card Recovery Form, the Issuer should match it to the Fee Collection message record based on the Acquirer Member ID, account number, and recovery date comparisons.
- If an exempt Member has an electronic reward payment processed, clearing receives the record by an information slip. The Transaction is part of the Net Settlement System for settlement purposes.

6.9.3.3 Reward Payment Chargebacks

A reward reimbursement draft may be charged back only when the incorrect Member is charged. The senior vice president of the Franchise Department will resolve any dispute concerning reward reimbursement.

6.10 PIN Security Standards

All Members and their agents performing PIN encipherment or any other aspect of PIN processing must comply with the applicable PIN security-related requirements in the latest editions of the following documents, available at www.pcisecuritystandards.org:

- Payment Card Industry (PCI) PIN Security Requirements
- PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements
- PCI PTS Hardware Security Module (HSM) Security Requirements
- PCI Software-based PIN Entry on COTS (SPoC) Security Requirements

Cardholder PIN entry at a Terminal must only be performed by means of one of the following:

1. A PIN entry device (PED) or an encrypting PIN pad (EPP) approved pursuant to the PCI PIN Transaction Security (PTS) program; or
2. On the touchscreen of a consumer device (such as a smartphone or tablet) using a solution for software-based PIN entry on a commercial off-the-shelf (COTS) consumer device (SPoC Solution) and incorporating a PIN Cardholder Verification Method (CVM) Application approved pursuant to the PCI SPoC program.

2.3.9.6. تعويض المكافآت

تنطبق المواصفات التالية على تعويض المكافآت:

- عند إرسال البطاقة إلى جهة الإصدار، ستحصل جهة القبول على تعويض عن المكافأة المدفوعة ورسوم XX دينار ليبي عن طريق معالجة رسالة تحصيل الرسوم من خلال نظام مشغل شبكة الدفع المحلية.
- إذا أعاد أحد الأعضاء بطاقة إلى جهة إصدار ولم يتم دفع مكافأة، يجوز للعضو الذي قام بالاسترداد، وفقاً لتقديره، تحصيل رسوم XX دينار ليبي عن طريق معالجة سجل رسالة تحصيل الرسوم.
- عند استلام نموذج استرداد بطاقة التبادل، يجب على جهة الإصدار مطابقته مع سجل رسالة تحصيل الرسوم بناءً على معرف عضو جهة القبول ورقم الحساب ومقارنات تاريخ الاسترداد.
- إذا تمت معالجة مدفوعات مكافأة إلكترونية لعضو معفى، فإن المقاصة تتلقى السجل عن طريق قسيمة معلومات. المعاملة هي جزء من صافي نظام التسوية لأغراض التسوية.

3.3.9.6. عمليات رد المبالغ المدفوعة على مدفوعات المكافآت

قد يتم خصم مسودة استرداد المكافأة فقط عندما يتم تحصيل رسوم من العضو غير الصحيح. سيقوم النائب الأول لرئيس قسم الامتياز بتسوية النزاع الذي يتعلق باسترداد المكافأة.

10.6. معايير أمان رقم التعريف الشخصي

يجب على جميع الأعضاء ووكلائهم الذين يقومون بتشفير رقم التعريف الشخصي، أو أي جانب آخر من جوانب معالجة رقم التعريف الشخصي، الامتثال للمتطلبات المتعلقة بأمان رقم التعريف الشخصي المعمول بها في أحدث إصدارات المستندات التالية: المتوفرة على www.pcisecuritystandards.org:

- متطلبات أمان رقم التعريف الشخصي لصناعة بطاقات الدفع (PCI).
- متطلبات الأمان المعيارية لنقطة التفاعل (POI) الخاصة بأمان معاملات رقم التعريف الشخصي لصناعة بطاقات الدفع (PTS) (PCI).
- متطلبات أمان وحدة أمان الأجهزة (HSM) الخاصة بأمان معاملات رقم التعريف الشخصي لصناعة بطاقات الدفع (PTS) (PCI).
- متطلبات أمان إدخال رقم التعريف الشخصي المستند على البرامج لصناعة بطاقات الدفع PCI إلى (COTS) (SPoC).

يجب أن يتم إدخال رقم التعريف الشخصي لحامل البطاقة في المحطة فقط، عن طريق أحد الإجراءات التالية:

1. جهاز إدخال رقم التعريف الشخصي (PED) أو لوحة رقم تعريف شخصي مشفرة (EPP) معتمدة وفقاً لبرنامج بأمان معاملات رقم التعريف الشخصي لصناعة بطاقات الدفع (PTS).
2. على شاشة اللمس لجهاز المستهلك (مثل الهاتف الذكي أو الجهاز اللوحي) باستخدام معالج لإدخال رقم التعريف الشخصي المستند إلى البرامج على جهاز المستهلك التجاري (COTS) (معالج SPoC)، ودمج تطبيق طريقة التحقق من رقم التعريف الشخصي لحامل البطاقة (CVM) تمت الموافقة عليه وفقاً لبرنامج صناعة بطاقات الدفع SPoC.

As used in this Rule, the following terms have the meanings set forth in the PCI Software-based PIN Entry on COTS (SPoC)™ Program Guide:

- Monitoring/Attestation System
- PIN Cardholder Verification Method (CVM) Application
- SPoC Solution

NOTE: All documents referenced in this section are available at www.pcisecuritystandards.org.

6.10.1 PIN Entry Devices (PEDs) and Encrypting PIN Pads (EPPs)

PEDs and EPPs are the security hardware and software modules for PIN entry at any type of Terminal, ensuring the confidentiality of the PIN immediately upon entry by the Cardholder. PEDs and EPPs use physical security mechanisms (hardware) as the first line of defense to protect PINs and any other Cardholder data that may be captured by the PED or EPP.

The PCI PTS program for PED and EPP device testing and approval is described in the Payment Card Industry (PCI) PIN Transaction Security (PTS) Device Testing and Approval Program Guide. Approved PEDs and EPPs may be found in the PCI Approved PTS Devices list.

Secure Deployment and Management of PEDs and EPPs

As attackers' security capabilities evolve, the PCI PTS POI specifications for PED and EPP vendors are updated periodically. Acquires should use the latest security version possible of PED and EPP models as such devices offer more robust protections against current threats.

An Acquirer must ensure that all PEDs and EPPs meet the following requirements:

1. Each newly installed PED and EPP must have its model listed in the PCI Approved PTS Devices list. Such devices may continue to be used after the expiration of the PCI PTS approval; however, an Acquirer should plan to upgrade or replace the PED or EPP before the expiration of the PCI PTS approval.

كما هو مستخدم في هذه القاعدة ، فإن المصطلحات التالية لها المعاني الموضحة في دليل برنامج إدخال رقم التعريف الشخصي المستند إلى برنامج صناعة بطاقات الدفع PCI على COTS (SPoC) (TM):

- نظام المراقبة/ التصديق.
 - تطبيق طريقة التحقق من رقم التعريف الشخصي لحامل البطاقة.
 - معالج SPoC.
- ملاحظة: جميع الوثائق المشار إليها في هذا القسم متاحة على www.pcisecuritystandards.org.

1.10.6. أجهزة إدخال أرقام التعريف الشخصية (PEDs) ولوحات تشفير أرقام التعريف الشخصية (EPPs)

أجهزة إدخال أرقام التعريف الشخصية (PEDs)، ولوحات تشفير أرقام التعريف الشخصية (EPPs) هي الأجهزة الأمنية، ووحدات البرامج لإدخال رقم التعريف الشخصي في أي نوع من الأجهزة، مما يضمن سرية رقم التعريف الشخصي فور إدخاله من قبل حامل البطاقة. وتستخدم أجهزة إدخال أرقام التعريف الشخصية (PEDs) ولوحات تشفير أرقام التعريف الشخصية (EPPs) آليات الأمان المادية (الأجهزة) كخط دفاع أول لحماية أرقام التعريف الشخصية و البيانات الأخرى لحامل البطاقة والتي قد يتم التقاطها بواسطة جهاز إدخال رقم التعريف الشخصي (PED) ولوحة تشفير رقم التعريف الشخصي (EPP).

تم وصف برنامج أمان معاملات رقم التعريف الشخصي PTS لصناعة بطاقات الدفع PCI، لاختبار جهاز إدخال رقم التعريف الشخصي (PED) ولوحة تشفير رقم التعريف الشخصي (EPP) واعتماده في دليل برنامج جهاز اختبار واعتماد أمان معاملات رقم التعريف الشخصي (PTS) (لصناعة بطاقات الدفع PCI. ويمكن العثور على جهاز إدخال رقم التعريف الشخصي ولوحة تشفير رقم التعريف الشخصي (EPPs) المعتمدة في قائمة أجهزة صناعة بطاقات الدفع PCI المعتمدة وأمان معاملات رقم التعريف الشخصي PTS.

النشر الآمن، وإدارة أجهزة إدخال أرقام التعريف الشخصية (PEDs)، ولوحات تشفير أرقام التعريف الشخصية (EPPs)

مع تطور قدرات المهاجمين الأمنية، يتم تحديث مواصفات نقاط الاهتمام POI صناعة بطاقات الدفع PCI لأمان معاملات رقم التعريف الشخصي PTS لبائعي جهاز إدخال رقم التعريف الشخصي PED ولوحة تشفير رقم التعريف الشخصي EPP بشكل دوري. ويجب على جهات القبول استخدام أحدث إصدار أمان ممكن من نماذج جهاز إدخال رقم التعريف الشخصي PED ولوحة تشفير رقم التعريف الشخصي EPP حيث توفر هذه الأجهزة حماية أكثر قوة ضد التهديدات الحالية.

يجب على على جهة القبول التحقق من أن جميع أجهزة إدخال أرقام التعريف الشخصية ولوحات تشفير أرقام التعريف الشخصية تفي بالمتطلبات التالية:

1. يجب أن يكون طراز كل جهاز من أجهزة إدخال أرقام التعريف الشخصية PED ولوحات تشفير أرقام التعريف الشخصية EPP مثبتين حديثًا، ومدرجًا في قائمة أجهزة أمان معاملات رقم التعريف الشخصي PTS المعتمدة من صناعة بطاقات الدفع PCI . ويمكن الاستمرار في استخدام هذه الأجهزة بعد انتهاء صلاحية اعتماد أمان معاملات رقم التعريف الشخصي PTS لصناعة بطاقات الدفع PCI؛ ومع ذلك ، يجب على جهة القبول أن تخطط لترقية أو استبدال جهاز إدخال رقم التعريف الشخصي PED ولوحة تشفير رقم التعريف الشخصي EPP قبل انتهاء صلاحية اعتماد أمان معاملات رقم التعريف الشخصي PTS لصناعة بطاقات الدفع الخاص بها PCI.

2. In limited cases as required by system or business conditions (for example, device replacements or refurbishments), Acquirers may newly install devices from device sets whose PCI PTS approval has expired, if either of the following conditions apply:
 - The device set is in inventory when the PCI PTS approval expired
 Device models that reach approval expiration are moved from the PCI Approved PTS Devices list to the PIN Transaction Security Devices With Expired Approvals list.
 - The device set is under a device management system.
 Such system must ensure that devices are able to both receive software security patches when made available by the device vendor and are physically managed (for example, maintaining a list of devices and periodically inspecting devices to look for tampering or substitution).
3. An Acquirer must properly manage its PED and EPP inventory. Such management must include:
 - Identifying the type and location of each deployed device; and
 - Having trained staff to conduct periodic visual inspections for signs of tampering or device substitution.
4. In exceptional circumstances, such as widespread successful attacks to a specific model of PED or EPP, The National Scheme Operator may, at any point in time, require Acquirers to follow specific risk management actions that may include the sunseting of that model. Should the National Scheme Operator announce a sunset date for a given model, devices of that model, then as of the specified sunset date, the device must no longer be used to process Transactions.

6.10.2 Software-based PIN Entry using PIN CVM Applications

PIN CVM Applications are elements of SPoC Solutions that must be validated pursuant to the PCI SPoC program, as described in the Payment Card Industry (PCI) Software-based PIN Entry on COTS (SPoC)™ Program Guide.

PIN CVM Applications ensure the confidentiality of the PIN immediately upon entry by the Cardholder in MPOS Terminals based on COTS devices. PIN CVM Applications (and the COTS device operating platforms on which they run) are continuously monitored and security-attested by the SPoC Solution's back-end Monitoring/Attestation System.

Permitted PIN CVM applications and supported Card and Contactless Payment Device readers (external to the COTS device) are listed in each SPoC Solution's documentation. A list of SPoC Solutions validated pursuant to the PCI SPoC program is available at www.pcisecuritystandards.org.

2. في حالات محدودة، ووفقًا لمتطلبات النظام أو ظروف العمل (على سبيل المثال، استبدال الأجهزة أو تجديدها)، يجوز لجهات القبول تثبيت الأجهزة الاحداث من مجموعات الأجهزة التي انتهت صلاحية اعتماد أمان معاملات رقم التعريف الشخصي PTS لصناعة بطاقات الدفع PCI الخاص بها، إذا تم تطبيق أي من الشروط التالية:
 - يكون الجهاز في المخزون عندما تنتهي صلاحية اعتماد أمان معاملات رقم التعريف الشخصي PTS لصناعة بطاقات الدفع PCI الخاص به.
 - يتم نقل طرازات الأجهزة التي وصلت إلى الموافقة منتهية صلاحية من قائمة أجهزة أمان معاملات رقم التعريف الشخصي PTS المعتمدة من صناعة بطاقات الدفع PCI إلى قائمة أجهزة أمان معاملات رقم التعريف الشخصي ذات الموافقات منتهية الصلاحية.
 - الجهاز خاضع لنظام إدارة الجهاز.
 يجب أن يضمن هذا النظام أن الأجهزة قادرة على تلقي تصحيحات أمان البرامج عند إتاحتها بواسطة بائع الجهاز وإدارتها فعليًا (على سبيل المثال، الاحتفاظ بقائمة من الأجهزة وفحص الأجهزة بشكل دوري للبحث عن التلاعب أو الاستبدال).
3. يجب على جهات القبول إدارة مخزون جهاز إدخال رقم التعريف الشخصي PED ولوحة تشفير رقم التعريف الشخصي EPP بشكل صحيح. يجب أن تشمل هذه الإدارة:
 - تحديد نوع وموقع كل جهاز تم نشره.
 - وجود موظفين مدربين لإجراء فحوصات بصرية دورية بحثًا عن علامات العبث أو استبدال الجهاز.
4. في ظروف استثنائية، مثل الهجمات الناجمة على نطاق واسع لنموذج معين من جهاز إدخال رقم التعريف الشخصي PED ولوحة تشفير رقم التعريف الشخصي EPP، قد يطلب مشغل شبكة الدفع المحلية، في أي وقت، من جهات القبول اتباع إجراءات إدارة مخاطر محددة قد تشمل إنهاء هذا النموذج. وإذا أعلن مشغل شبكة الدفع المحلية، عن تاريخ انتهاء العمل لطراز معين من الأجهزة، فابتداءً من تاريخ انتهاء الصلاحية المحدد، يجب ألا يتم استخدام الجهاز لمعالجة المعاملات.

2.10.6 إدخال رقم التعريف الشخصي المستند إلى البرامج باستخدام تطبيقات أرقام التعريف الشخصية و طريقة التحقق من البطاقة PIN CVM

تطبيقات أرقام التعريف الشخصية و طريقة التحقق من البطاقة PIN CVM هي عناصر من طول SPoC التي يجب التحقق من صحتها وفقًا لبرنامج صناعة بطاقات الدفع PCI، كما هو موضح في دليل برنامج صناعة بطاقات الدفع (PCI) المستند إلى برنامج رقم التعريف الشخصي على COTS (SPoC).

وتضمن تطبيقات أرقام التعريف الشخصية، و طريقة التحقق من البطاقة PIN CVM سرية رقم التعريف الشخصي فور إدخاله من قبل حامل البطاقة في محطات MPOS استنادًا إلى أجهزة COTS. تخضع تطبيقات أرقام التعريف الشخصية و طريقة التحقق من البطاقة PIN CVM (وأنظمة تشغيل أجهزة COTS التي تعمل عليها) للمراقبة المستمرة والتصديق على الأمان من خلال نظام المراقبة/التصديق الخلفي الخاص بمعالج SPoC.

يتم سرد تطبيقات أرقام التعريف الشخصية و طريقة التحقق من البطاقة PIN CVM المسموح بها وقارئات البطاقات وأجهزة الدفع غير المتصلة المدعومة (خارج جهاز COTS) في كل وثائق معالج SPoC.

تتوفر قائمة معالجات SPoC التي تم التحقق من صحتها وفقًا لبرنامج صناعة بطاقات الدفع PCI SPoC على www.pcisecuritystandards.org.

Secure Deployment and Management of PIN CVM Applications

An Acquirer must ensure that all PIN CVM Applications used by its Merchants and any Agents of a Payment Facilitator of the Acquirer meet the following requirements:

1. Each PIN CVM Application is listed as a valid element of a SPoC Solution in good standing;
2. Each PIN CVM Application is used only with those Card or Contactless Payment Device readers supported by its specific approved SPoC Solution;
3. The PIN CVM Application is the only scheme acceptance application active in the COTS device during the Transaction; and
4. Each Merchant and Agent using the PIN CVM Application has acknowledged and follows the SPoC Solution's Merchant Guidance and Acceptable Use Policy.

The Monitoring/Attestation System of a SPoC Solution continuously ensures that the overall protection of PIN and Cardholder data in a SPoC Solution is commensurate with current mobile security threat levels.

As attackers' security skills evolve, the Monitoring/Attestation System of a SPoC Solution may determine that a given PIN CVM Application or COTS device operating platform is no longer suitable to support secure PIN entry, and may impose Transaction processing restrictions. These restrictions may include halting the full Transaction capability of the PIN CVM Application.

6.10.3 PIN Verification

An Issuer must be capable of verifying PINs based on a maximum of six characters. The Issuer may use the PIN verification algorithm of its choice.

If a Card is encoded with a PIN Verification Value (PVV), then the Issuer may use the National Scheme Operator's PIN verification service for authorization processing. If a proprietary algorithm is used for the PVV calculation or the PVV is not encoded on the Card, then PIN verification will not be performed on a Transaction authorized by means of the Stand-In Processing Service.

The National Scheme Operator provides a PIN verification service for all purchase transactions that contain a PIN.

To request PIN verification service, the issuer must provide the PIN verification key(s) and PIN processing parameters to the National Scheme Operator. This is achieved by completing the PIN Processing Profile Form and by sending the PIN verification keys using the Hard Copy Key Exchange Form.

النشر الآمن، وإدارة تطبيقات أرقام التعريف الشخصية و طريقة التحقق من البطاقة PIN CVM

يجب على جهة القبول التحقق من أن جميع تطبيقات أرقام التعريف الشخصية و طريقة التحقق من البطاقة PIN CVM التي يستخدمها التجار، ووكلاء ميسر الدفع التابع لجهة القبول أن تفي بالمتطلبات التالية:

1. يتم إدراج كل تطبيق رقم التعريف الشخصي و طريقة التحقق من البطاقة PIN CVM كعنصر صالح لحل SPoC في وضع جيد.
2. يتم استخدام كل تطبيق رقم التعريف الشخصي و طريقة التحقق من البطاقة PIN CVM فقط مع أجهزة قارئ البطاقات أو أجهزة الدفع غير المتصلة المدعومة بحل SPoC المعتمد.
3. تطبيق رقم التعريف الشخصي و طريقة التحقق من البطاقة PIN CVM هو تطبيق قبول النظام الوحيد النشط في جهاز COTS أثناء المعاملة.

4. أقر كل تاجر، ووكيل يستخدم تطبيق رقم التعريف الشخصي و طريقة التحقق من البطاقة PIN CVM بإرشادات التاجر وسياسة الاستخدام المقبول الخاصة بمعالجات SPoC وأنه يتبعهما.

يضمن نظام المراقبة/ التصديق الخاص بمعالج SPoC باستمرار أن الحماية الشاملة لبيانات رقم التعريف الشخصي وحامل البطاقة في معالج SPoC تتناسب مع مستويات تهديد أمان الهاتف المحمول الحالية. غير أنه مع تطور المهارات الأمنية للمهاجمين، قد يحدد نظام المراقبة/ المصادقة الخاص بمعالج SPoC أن تطبيق رقم التعريف الشخصي و طريقة التحقق من البطاقة PIN CVM أو نظام تشغيل جهاز COTS لم يعد مناسبًا لدعم إدخال رقم التعريف الشخصي الآمن، وقد يفرض قيودًا على معالجة المعاملات. وقد تشمل هذه القيود وقف القدرة الكاملة لمعاملة تطبيق رقم التعريف الشخصي و طريقة التحقق من البطاقة PIN CVM.

3.10.6. التحقق من رقم التعريف الشخصي

يجب أن تكون جهة الإصدار قادرة على التحقق من أرقام التعريف الشخصية، استنادًا إلى ستة أحرف كحد أقصى. وقد تستخدم جهة الإصدار خوارزمية التحقق من رقم التعريف الشخصي التي تختارها. إذا تم تشفير البطاقة بقيمة التحقق من رقم التعريف الشخصي (PVV)، فيجوز لجهة الإصدار استخدام خدمة التحقق من رقم التعريف الشخصي لمشغل شبكة الدفع المحلية لمعالجة التفويض. وإذا تم استخدام خوارزمية الملكية لحساب قيمة التحقق من رقم التعريف الشخصي PVV أو لم يتم تشفير قيمة التحقق من رقم التعريف الشخصي PVV على البطاقة، فلن يتم إجراء التحقق من رقم التعريف الشخصي على معاملة مرسلة من خلال خدمة المعالجة الاحتياطية.

يوفر مشغل شبكة الدفع المحلية خدمة التحقق من رقم التعريف الشخصي لجميع معاملات الشراء التي تحتوي على رقم تعريف شخصي.

لطلب خدمة التحقق من رقم التعريف الشخصي، يجب على جهة الإصدار تقديم مفتاح (مفاتيح) التحقق من رقم التعريف الشخصي وظوابط معالجة رقم التعريف الشخصي لمشغل شبكة الدفع المحلية. ويتم تحقيق ذلك من خلال استكمال نموذج ملف تعريف معالجة رقم التعريف الشخصي وإرسال مفاتيح التحقق من رقم التعريف الشخصي باستخدام نموذج تبادل مفتاح النسخ الورقي .

The Single Message System supports the American Bankers Association (ABA) method of PIN generation verification. The PIN verification service is an optional service. To generate PINs using the ABA method, the institution must determine the following.

- Validation data
- PVKI (PIN verification key index)
- Key left
- Key right
- PIN (customer-selected)

This generation process will produce a PIN verification value (PVV), which is encoded on Track 2 of the card's magnetic stripe or provided by the customer in a file. The validation data is the last 11 digits of the PAN, excluding the check digit. The PVKI is appended to the validation data, which is in turn appended by the PIN to complete the 16-digit block.

This block along with the 16-digit key left is sent through the DES algorithm to produce another 16-digit block. The resultant block is sent through DES using the 16-digit key right, producing a new 16-digit resulting block. This new block is sent through DES with the key left to produce the final block called the generated PIN block.

The PVV is determined by taking the first four numeric digits of the natural PIN block. If there are not four numeric digits, the A-F are mapped to 0-5 starting from the beginning of the natural PIN block, and the remaining digits of the PVV are completed.

For example:
47CAD278C8674359 = 4727
EFACECB4B9C4EEAF = 494E = 4944
BDBACF4FCDF33ABE = 433B = 4331
BFDCCA4FBFBFAADF = 4BFD = 4153
EFAAFAFFEEDFBFCE = EFAA = 4500

يدعم نظام الرسالة الواحدة طريقة جمعية المصرفيين الأمريكيين ABA للتحقق من إنشاء رقم التعريف الشخصي.

خدمة التحقق من رقم التعريف الشخصي هي خدمة اختيارية. لإنشاء أرقام تعريف شخصية باستخدام طريقة جمعية المصرفيين الأمريكيين (ABA)، يجب على المؤسسة تحديد ما يلي.

- بيانات التحقق.
- فهرس مفتاح التحقق من رقم التعريف الشخصي PVKI.
- المفتاح الأيسر.
- المفتاح الأيمن.
- رقم التعريف الشخصي (من اختيار العميل).

ستنتج عملية الإصدار هذه، قيمة التحقق من رقم التعريف الشخصي (PVV)، والتي يتم ترميزها على المسار 2 للشريط المغناطيسي للبطاقة أو التي يوفرها العميل في ملف. بيانات التحقق هي آخر 11 رقمًا من رقم التعريف الشخصي، باستثناء رقم التحقق. ويرفق فهرس مفتاح التحقق من رقم التعريف الشخصي PVKI ببيانات التحقق، والتي ترفقها بدورها بواسطة رقم التعريف الشخصي لإكمال الكتلة المكونة من 16 رقمًا.

يتم إرسال هذه الكتلة مع المفتاح الأيسر المكون من 16 رقمًا عبر خوارزمية معيار تشفير البيانات DES لإنتاج كتلة أخرى مكونة من 16 رقمًا. يتم إرسال الكتلة الناتجة من خلال معيار تشفير البيانات DES باستخدام المفتاح الأيمن المكون من 16 رقمًا، مما ينتج عنه كتلة ناتجة جديدة مكونة من 16 رقمًا. يتم إرسال هذه الكتلة الجديدة من خلال معيار تشفير البيانات DES مع ترك المفتاح لإنتاج الكتلة النهائية التي تسمى كتلة رقم التعريف الشخصي التي تم إنشاؤها.

يتم تحديد قيمة التحقق من رقم التعريف الشخصي PVV، بأخذ أول أربعة أرقام رقمية من كتلة رقم التعريف الشخصي الطبيعية. وإذا لم يكن هناك أربعة أرقام رقمية، يتم تعيين A-F إلى 0-5 بدءًا من بداية كتلة رقم التعريف الشخصي الطبيعية، ويتم إكمال الأرقام المتبقية من قيمة التحقق من رقم التعريف الشخصي PVV.

على سبيل المثال:

47CAD278C8674359 = 4727
EFACECB4B9C4EEAF = 494E = 4944
BDBACF4FCDF33ABE = 433B = 4331
BFDCCA4FBFBFAADF = 4BFD = 4153
EFAAFAFFEEDFBFCE = EFAA = 4500

6.10.4 PIN Encipherment

All Members and their agents performing PIN Transaction processing must comply with the security requirements for PIN encipherment specified in the Payment Card Industry PIN Security Requirements.

An Acquirer must ensure that PIN entry devices (PEDs) and encrypting PIN pads (EPPs) comply with the following requirements:

- For secure transmission of the PIN from the PED or EPP to the Issuer host system, the PED or EPP must encrypt the PIN using the approved algorithm(s) for PIN encipherment listed in ISO/IEC 9564-2 (Financial services—PIN management and security—Part 2: Approved algorithms for PIN encipherment) and the appropriate PIN block format as provided in ISO/IEC 9564-1 (Financial services—PIN management and security—Part 1: Basic principles and requirements for PINs in card-based systems); and
- If the PIN pad and the secure component of the PED are not integrated into a single tamper-evident device, then for secure transmission of the PIN from the PIN pad to the secure component, the PIN pad must encrypt the PIN using the approved algorithm(s) for PIN encipherment listed in ISO/IEC 9564-2.

6.10.5 PIN Key Management

Key management is the process of creating, distributing, maintaining, storing, and destroying cryptographic keys, including the associated policies and procedures used by processing entities.

All Acquirers and their agents performing PIN Transaction processing must comply with the security requirements for PIN and key management specified in the Payment Card Industry PIN Security Requirements.

In addition, all Acquirers and their agents must adhere to the following Standards for PIN encryption:

1. Perform all PIN encryption, translation, and decryption for the network using hardware encryption.
2. Do not perform PIN encryption, translation, or decryption using software routines.

The Interchange System and Members exchange PIN encryption keys (PEKs) in two manners: statically and dynamically. Directly connected Members that are processing Transactions that contain a PIN may use either static or dynamic key encryption to encipher the PIN. The National Scheme Operator strongly recommends using dynamic PEKs.

4.10.6. تشفير رقم التعريف الشخصي

يجب أن يلتزم جميع الأعضاء ووكلائهم الذين يقومون بمعالجة معاملات رقم التعريف الشخصي بمتطلبات الأمان لتشفير رقم التعريف الشخصي المحدد في متطلبات أمان رقم التعريف الشخصي الخاصة بصناعة بطاقات الدفع.

يجب على جهة القبول التحقق من أن أجهزة إدخال رقم التعريف الشخصي (PEDs) ولوحات رقم التعريف الشخصي المشفرة (EPPs) تتوافق مع المتطلبات التالية:

- لنقل آمن لرقم التعريف الشخصي من جهاز إدخال رقم التعريف الشخصي PED أو لوحة رقم التعريف الشخصي المشفرة EPP إلى نظام مضيف جهة الإصدار، يجب أن يقوم جهاز إدخال رقم التعريف الشخصي PED أو لوحة رقم التعريف الشخصي المشفرة EPP بتشفير رقم التعريف الشخصي باستخدام الخوارزمية (الخوارزميات) المعتمدة لتشفير رقم التعريف الشخصي المدرج في ISO / IEC 9564-2 (الخدمات المالية - إدارة و أمن رقم التعريف الشخصي - الجزء 2: الخوارزميات المعتمدة لتشفير رقم التعريف الشخصي) وتنسيق كتلة رقم التعريف الشخصي المناسبة على النحو المنصوص عليه في ISO / IEC 9564-1 (الخدمات المالية - إدارة وأمن رقم التعريف الشخصي - الجزء 1: المبادئ والمتطلبات الأساسية لأرقام التعريف الشخصية في الأنظمة القائمة على البطاقة).
- إذا لم يتم دمج لوحة رقم التعريف الشخصي، والمكون الآمن لجهاز إدخال رقم التعريف الشخصي PED في جهاز واحد واضح للعبث، ثم من أجل النقل الآمن لرقم التعريف الشخصي من لوحة رقم التعريف الشخصي إلى المكون الآمن، يجب أن تقوم لوحة رقم التعريف الشخصي بتشفير رقم التعريف الشخصي باستخدام الخوارزمية (خوارزميات) المعتمدة لتشفير رقم التعريف الشخصي المدرج في ISO / IEC 9564-2.

5.10.6. إدارة مفتاح رقم التعريف الشخصي

إدارة المفاتيح هي عملية إنشاء مفاتيح التشفير، وتوزيعها وصيانتها وتخزينها وإتلافها، بما في ذلك السياسات والإجراءات المرتبطة التي تستخدمها كيانات المعالجة.

يجب أن تلتزم جهات القبول ووكلائها الذين يقومون بمعالجة معاملات رقم التعريف الشخصي بمتطلبات الأمان الخاصة برقم التعريف الشخصي وإدارة المفاتيح المحددة في متطلبات أمان رقم التعريف الشخصي الخاصة بصناعة بطاقات الدفع .

بالإضافة إلى ذلك، يجب على جميع جهات القبول ووكلائها الالتزام بالمعايير التالية لتشفير رقم التعريف الشخصي:

1. تنفيذ جميع عمليات تشفير رقم التعريف الشخصي والترجمة وفك التشفير للشبكة باستخدام تشفير الأجهزة.
2. عدم القيام بإجراء تشفير رقم التعريف الشخصي أو الترجمة أو فك التشفير باستخدام إجراءات البرامج.

يقوم نظام التبادل والأعضاء بتبادل مفاتيح تشفير رقم التعريف الشخصي (PEKs) بطريقتين: بشكل ثابت وديناميكي. ويجوز للأعضاء المتصلين مباشرة والذين يقومون بمعالجة المعاملات التي تحتوي على رقم تعريف شخصي، استخدام تشفير مفتاح ثابت أو ديناميكي لتشفير رقم التعريف الشخصي. يوصي مشغل شبكة الدفع المحلية استخدام مفاتيح تشفير رقم التعريف الشخصي SPEK الديناميكية.

6.11 Terminal Security Standards

The Acquirer must ensure that each Terminal:

1. Has a magnetic stripe reader capable of reading Track 2 data and transmitting such data to the Issuer for authorization;
2. Permits the Cardholder to enter PIN data in a private manner;
3. Prevents a new Transaction from being initiated before the prior Transaction is completed; and
4. Validates the authenticity of the Card or Access Device.

For magnetic stripe Transactions, the following checks must be performed by the Acquirer (either in the Terminal or the Acquirer host system), before the authorization request is forwarded:

- Longitudinal Redundancy Check (LRC)—The magnetic stripe must be read without LRC error.
- Track Layout—The track layout must conform to ISO specifications.

With respect to the electronic functions performed by a Terminal, the following requirements apply:

1. A Transaction may not be declined due to bank identification number (BIN)/Issuer identification number (IIN) validation.
2. A Transaction may not be declined as a result of edits or validations performed on the primary account number (PAN) length, expiration date, service code, discretionary data, or check digit data of the Access Device.
3. Tests or edits on Track 1 must not be performed for the purpose of disqualifying a Card from eligibility for Interchange System processing.

6.11.1 Hybrid Terminal Security Standards

The Acquirer must ensure that a Hybrid Terminal deployed at a location where NUMO is accepted complies with all of the following Standards:

- Each Hybrid Terminal that reads and processes EMV-compliant payment applications must read and process EMV-compliant NUMO-branded Payment Applications.
- Each Dual Interface Hybrid Terminal must read and process the same NUMO-branded Payment Applications on both the contact and contactless interfaces.
- Each Hybrid Terminal must perform a Chip Transaction when a Chip Card or Access Device is presented in compliance with all applicable Standards.

6.11.2 Triple DES Standards

Triple Data Encryption Standard (DES), minimum double key length (hereafter referred to as Triple DES), must be implemented as follows:

- All newly installed PEDs, including replacement and refurbished PEDs that are part of POS Terminals, must be Triple DES capable. This requirement applies to POS Terminals owned by Members and non-Members.
- All Member and processor host systems must support Triple DES.
- It is strongly recommended that all PEDs that are part of POS Terminals be Triple DES compliant and chip-capable.

11.6. معايير أمن الطرفيات

يجب على جهة القبول التحقق من أن كل محطة طرفية:

1. لديها قارئ شريط مغناطيسي قادر على قراءة بيانات المسار 2 ونقل هذه البيانات إلى جهة الإصدار للحصول على تفويض.
 2. تسمح لحامل البطاقة بإدخال بيانات رقم التعريف الشخصي بطريقة خاصة.
 3. تمنع بدء معاملة جديدة قبل إتمام المعاملة السابقة.
 4. تتحقق من صحة البطاقة أو جهاز الوصول.
- بالنسبة لمعاملات الشريط المغناطيسي، يجب إجراء الفحوصات التالية بواسطة جهة القبول (سواء في المحطة أو نظام القابل المضيف) ، قبل إعادة توجيه طلب التفويض:
- فحص التكرار الطولي (LRC)- يجب قراءة الشريط المغناطيسي بدون خطأ فحص التكرار الطولي (L-RC).
 - تخطيط المسار —يجب أن يتوافق تخطيط المسار مع مواصفات ISO.

فيما يتعلق بالوظائف الإلكترونية التي تؤديها المحطة، تنطبق المتطلبات التالية:

1. لا يجوز رفض المعاملة بسبب التحقق من رقم تعريف المصرفي / رقم تعريف جهة الإصدار (IIN).
2. لا يجوز رفض المعاملة نتيجة لعمليات التحرير أو التحقق التي يتم إجراؤها على طول رقم الحساب الأساسي أو تاريخ انتهاء الصلاحية أو رمز الخدمة أو البيانات التقديرية أو بيانات التحقق من رقم جهاز الوصول.
3. يجب عدم إجراء الاختبارات أو التعديلات على المسار 1 لغرض استبعاد البطاقة من القدرة لمعالجة نظام التبادل.

1.11.6. معايير أمن الطرفيات الهجينة

يجب على جهة القبول التحقق من أن المحطة الطرفية الهجينة المنتشرة في موقع يُقبل فيه نمو تتوافق مع جميع المعايير التالية:

- يجب على كل محطة هجينة تقرأ وتعالج تطبيقات الدفع المتوافقة مع معيار EMV قراءة ومعالجة تطبيقات الدفع التي تحمل علامة نمو التجارية المتوافقة مع معيار EMV.
- يجب على كل محطة هجينة ذات واجهة مزدوجة، أن تقرأ وتعالج نفس تطبيقات الدفع التي تحمل علامة نمو التجارية على كل من واجهات الاتصال وعدم الاتصال.
- يجب أن تقوم كل محطة هجينة بإجراء معاملة شريحة عندما يتم تقديم بطاقة شريحة أو جهاز وصول وفقاً لجميع المعايير المعمول بها.

2.11.6. معايير تشفير البيانات الثلاثي DES

يجب تنفيذ معيار تشفير البيانات الثلاثي (DES)، الحد الأدنى لطول المفتاح المزدوج (المشار إليه فيما يلي باسم معيار تشفير البيانات الثلاثي (DES) على النحو التالي:

- يجب أن تكون جميع أجهزة إدخال أرقام التعريف الشخصية PEDs المثبتة حديثاً، بما في ذلك أجهزة إدخال أرقام التعريف الشخصية PEDs التي تم استبدالها وتجديدها، والتي تعد جزءاً من محطات نقاط البيع POS، قادرة على الوصول إلى معيار تشفير البيانات الثلاثي. وينطبق هذا الشرط على محطات نقاط البيع المملوكة للأعضاء وغير الأعضاء.
- يجب أن تدعم جميع أنظمة مضيف الأعضاء والمعالج معيار تشفير البيانات الثلاثي DES .
- يوصى أن تكون جميع أجهزة إدخال أرقام التعريف الشخصية PEDs التي تعد جزءاً من محطات نقاط البيع POS متوافقة مع معيار تشفير البيانات الثلاثي DES وقادرة على الشريحة.

- All EPPs that are part of ATM Terminals must be Triple DES compliant.
- All Transactions routed to the Interchange System must be Triple DES compliant.

The National Scheme Operator recognizes that Members may elect to use other public key encryption methods between their POS Terminals or ATMs and their host(s). In such instances, the National Scheme Operator must approve the alternate method chosen in advance of its implementation and use. Approval will be dependent, in part, on whether the National Scheme Operator deems the alternate method to be as secure as or more secure than Triple DES. Approval is required before implementation can begin.

- يجب أن تكون جميع لوحات أرقام التعريف الشخصية EPPs المشفرة التي تعد جزءًا من أجهزة الصراف الآلي متوافقة مع معيار تشفير البيانات الثلاثي DES.
- يجب أن تكون جميع المعاملات الموجهة إلى نظام التبادل متوافقة مع معيار تشفير البيانات الثلاثي DES.

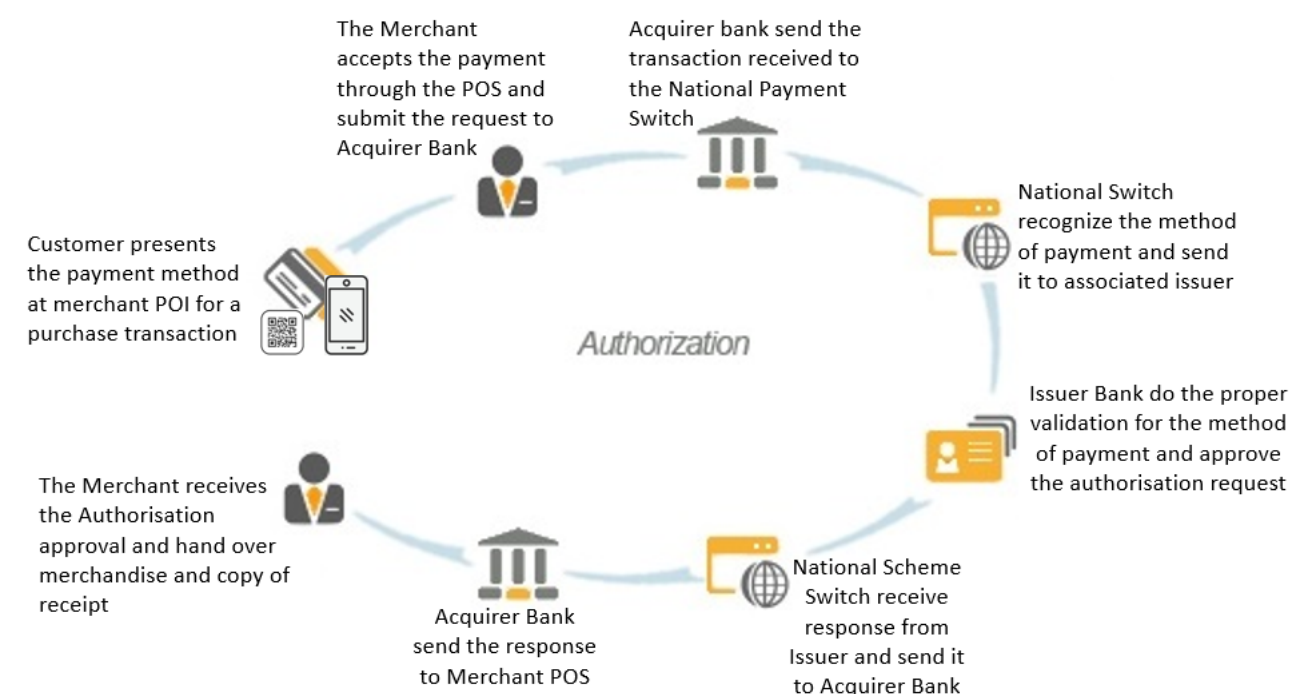
يدرك مشغل شبكة الدفع المحلية أنه يجوز للأعضاء اختيار استخدام طرق تشفير المفتاح العامة الأخرى بين محطات نقاط البيع POS أو أجهزة الصراف الآلي ومضيفهم (مضيفهم). وفي مثل هذه الحالات، يجب على مشغل شبكة الدفع المحلية الموافقة على الطريقة البديلة المختارة مسبقًا من تنفيذها واستخدامها. وتعتمد الموافقة، جزئيًا، على ما إذا كان مشغل شبكة الدفع المحلية يقدر أن الطريقة البديلة آمنة مثل معيار تشفير البيانات الثلاثي DES أو أكثر أمانًا منه. الحصول على هذه الموافقة مطلوبًا قبل أن يتم البدء في التنفيذ.

Book 1: Appendix number 52 Quarterly Statistics Report

الكتاب 1 : الملحق رقم 52 تقرير احصائي ربع سنوي

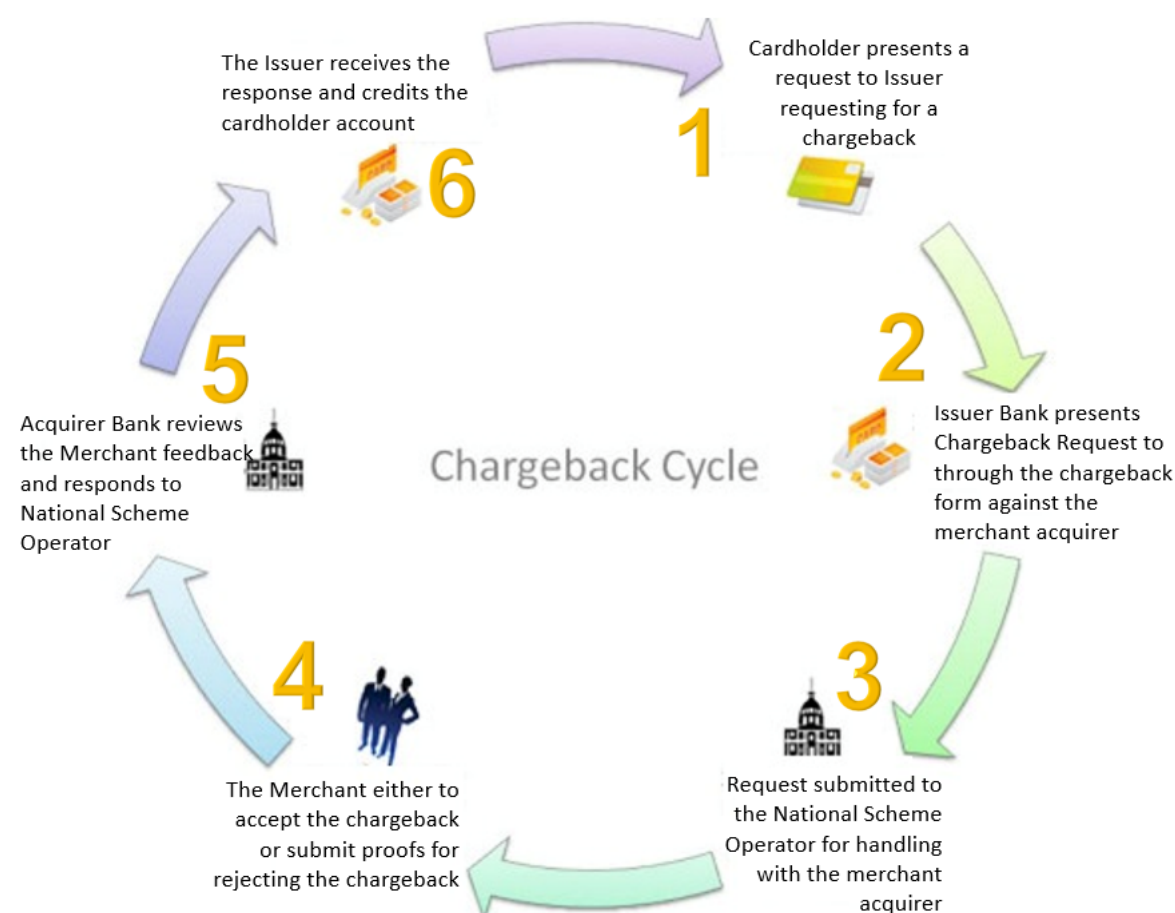
Appendix Number 1

(الملحق رقم 1)



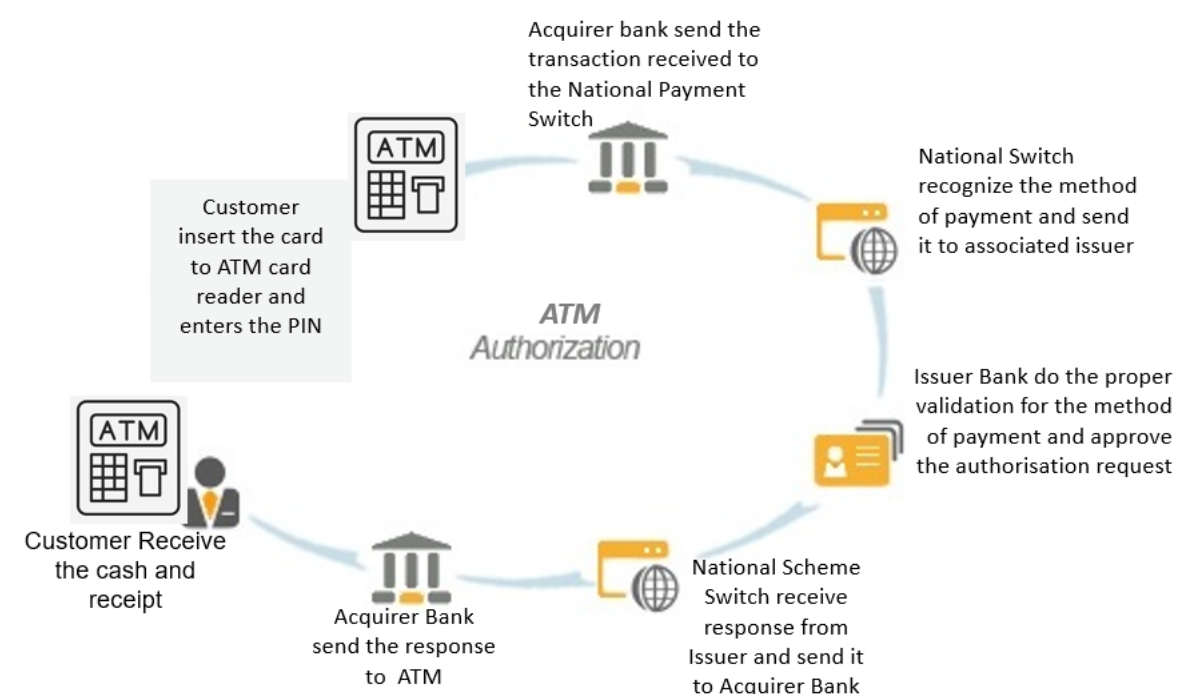
Appendix Number 4

(الملحق رقم 4)



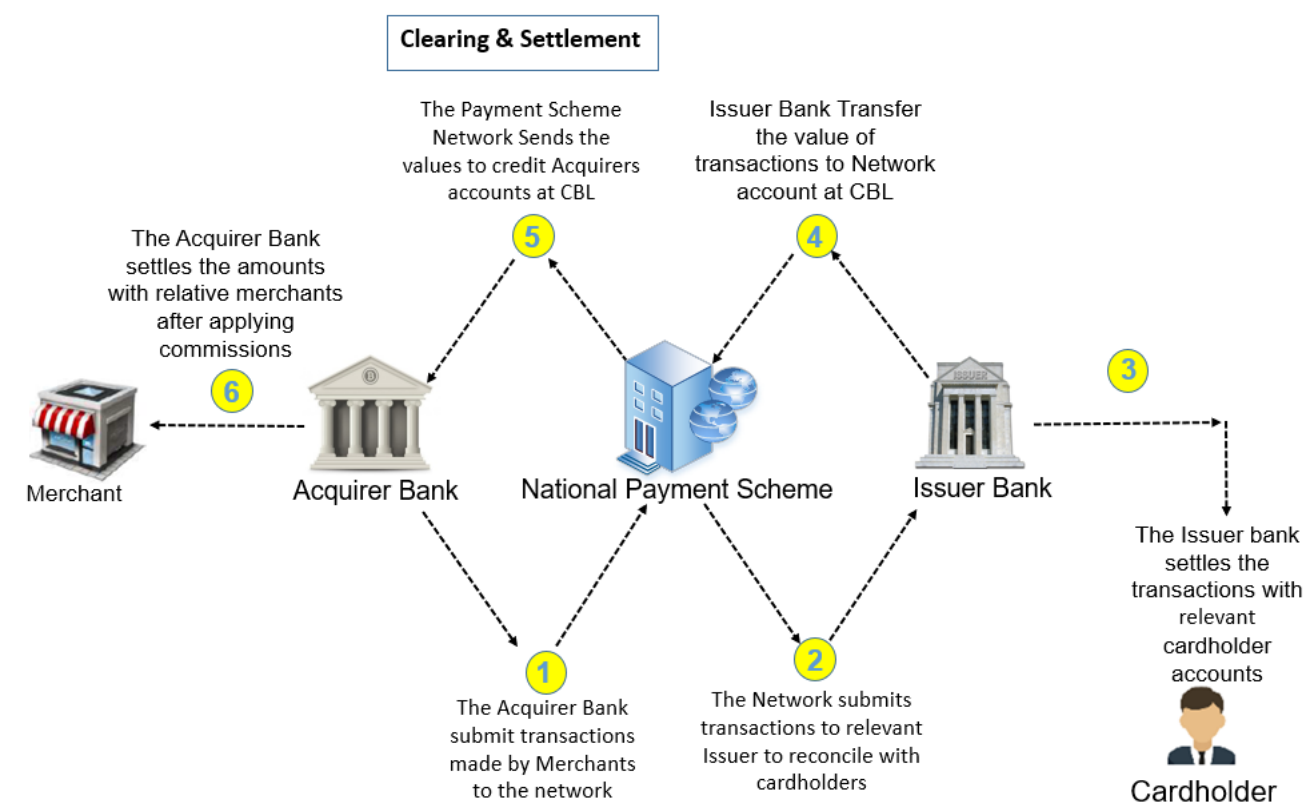
Appendix Number 2

(الملحق رقم 2)



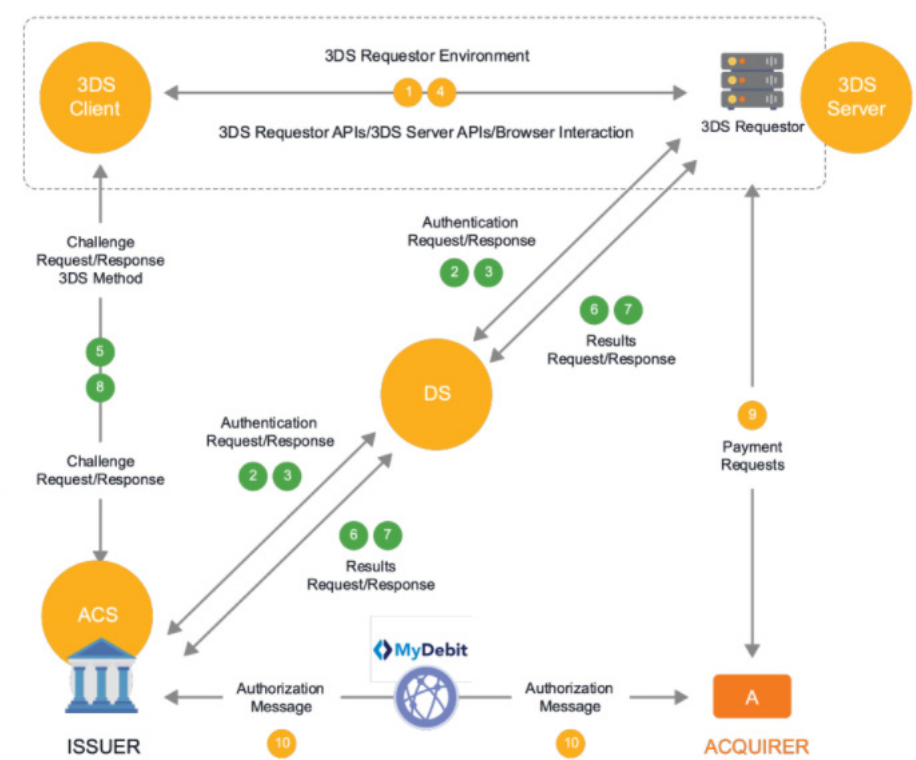
Appendix Number 3

(الملحق رقم 3)



Appendix Number 5

(الملحق رقم 5)



Appendix Number 6

(الملحق رقم 6)

Compliance Category	Assessment Type	Assessment Description
A	Per violation	Up to LDY xxx for the first violation Up to LDY xxx for the second violation within 12 months Up to LDY xxx for the third violation within 12 months Up to LDY xxx per violation for the fourth and subsequent violations within 12 months
	Variable occurrence (by device or Transaction)	Up to LDY xxx per occurrence for the first 30 days Up to LDY xxx per occurrence for days 31-60 Up to LDY xxx per occurrence for days 61-90 Up to LDY xxx per occurrence for subsequent violations
	Variable occurrence (by number of Cards)	Up to LDY xx per Card Minimum LDY xxx per month per Portfolio No maximum per month per Portfolio or per all Portfolios
B	Per violation	Up to LDY xxx for the first violation Up to LDY xxx for the second violation within 12 months Up to LDY xxx for the third violation within 12 months Up to LDY xxx per violation for the fourth and subsequent violations within 12 months
	Variable occurrence (by device or Transaction)	Up to LDY xxx per occurrence for the first 30 days Up to LDY xxx per occurrence for days 31-60 Up to LDY xxx per occurrence for days 61-90 Up to LDY xxx per occurrence for subsequent violations
	Variable occurrence (by number of Cards)	Up to LDY xx per Card Minimum LDY xxx per month per Portfolio Maximum LDY xxx per month per Portfolio Maximum LDY xxx per month per all Portfolios
C	Per violation	Up to LDY xxx for the first violation Up to LDY xxx for the second violation within 12 months Up to LDY xxx for the third violation within 12 months Up to LDY xxx per violation for the fourth and subsequent violations within 12 months
	Variable occurrence (by device or Transaction)	Up to LDY xxx per occurrence for the first 30 days Up to LDY xxx per occurrence for days 31-60 Up to LDY xxx per occurrence for days 61-90 Up to LDY xxx per occurrence for subsequent violations
	Variable occurrence (by number of Cards)	Up to LDY xx per Card Minimum LDY xxx per month per Portfolio Maximum LDY xxx month per Portfolio Maximum LDY xxx per month per all Portfolios

فئة الامتثال	نوع التقييم	وصف التقييم
أ.	لكل مخالفة	حتى xxx دينار ليبي عن المخالفة الأولى حتى xxx دينار ليبي عن المخالفة الثانية في غضون 12 شهرًا حتى xxx دينار ليبي عن المخالفة الثالثة في غضون 12 شهرًا حتى xxx دينار ليبي عن المخالفة الرابعة والمخالفات اللاحقة في غضون 12 شهرًا
ب.	أحداث متغيرة (حسب الجهاز أو المعاملة)	حتى xxx دينار ليبي لكل حدث في أول 30 يومًا حتى xxx دينار ليبي لكل حدث في الأيام من 31 إلى 60 حتى xxx دينار ليبي لكل حدث في الأيام من 61-90 حتى xxx دينار ليبي لكل حدث في المخالفات اللاحقة
	أحداث متغيرة (حسب عدد البطاقات)	حتى xxx دينار ليبي لكل بطاقة xxx دينار ليبي كحد أدنى في الشهر لكل محفظة لا يوجد حد أقصى في الشهر لكل محفظة أو لكل المحافظ
	لكل مخالفة	حتى xxx دينار ليبي عن المخالفة الأولى حتى xxx دينار ليبي عن المخالفة الثانية في غضون 12 شهرًا حتى xxx دينار ليبي عن المخالفة الثالثة في غضون 12 شهرًا حتى xxx دينار ليبي عن المخالفة الرابعة والمخالفات اللاحقة في غضون 12 شهرًا
ج.	أحداث متغيرة (حسب الجهاز أو المعاملة)	حتى xxx دينار ليبي لكل حدث في أول 30 يومًا حتى xxx دينار ليبي لكل حدث في الأيام من 31 إلى 60 حتى xxx دينار ليبي لكل حدث في الأيام من 61-90 حتى xxx دينار ليبي لكل حدث في المخالفات اللاحقة
	أحداث متغيرة (حسب عدد البطاقات)	حتى xxx دينار ليبي لكل بطاقة xxx دينار ليبي كحد أدنى في الشهر لكل محفظة xxx دينار ليبي كحد أقصى في الشهر لكل محفظة xxx دينار ليبي كحد أقصى في الشهر لكل المحافظ
	لكل مخالفة	حتى xxx دينار ليبي عن المخالفة الأولى حتى xxx دينار ليبي عن المخالفة الثانية في غضون 12 شهرًا حتى xxx دينار ليبي عن المخالفة الثالثة في غضون 12 شهرًا حتى xxx دينار ليبي عن المخالفة الرابعة والمخالفات اللاحقة في غضون 12 شهرًا
	أحداث متغيرة (حسب الجهاز أو المعاملة)	حتى xxx دينار ليبي لكل حدث في أول 30 يومًا حتى xxx دينار ليبي لكل حدث في الأيام من 31 إلى 60 حتى xxx دينار ليبي لكل حدث في الأيام من 61-90 حتى xxx دينار ليبي لكل حدث في المخالفات اللاحقة
	أحداث متغيرة (حسب عدد البطاقات)	حتى xxx دينار ليبي لكل بطاقة xxx دينار ليبي كحد أدنى في الشهر لكل محفظة xxx دينار ليبي كحد أقصى في الشهر لكل محفظة xxx دينار ليبي كحد أقصى في الشهر لكل المحافظ
	لكل مخالفة	حتى xxx دينار ليبي عن المخالفة الأولى حتى xxx دينار ليبي عن المخالفة الثانية في غضون 12 شهرًا حتى xxx دينار ليبي عن المخالفة الثالثة في غضون 12 شهرًا حتى xxx دينار ليبي عن المخالفة الرابعة والمخالفات اللاحقة في غضون 12 شهرًا

Appendix Number 7

For CVV 1	For CVV 2	For Chip CVV	(Length (all
Output from Step 1	Output from Step 1	Output from Step 1	16
Card expiration date (as presented in Track 2 encoding)	Card expiration date (as presented on the Card)	Card expiration date (as presented in Track 2 Equivalent Data Encoding)	¹ 4
Service code value must NOT be “000”	Service code value must be “000”	Service code value must be “999”	3
Total			² 4

Appendix 8

Definition	Position 2	Position 2	Position 3
International Card	1		
International Card—Integrated Circuit Card	2		
National Use Only	5		
National Use Only—Integrated Circuit Card	6		
Private Label or Proprietary Card	7		
Normal Authorization		0	
Positive Online Authorization Required		2	
PIN Required			0
Normal Cardholder Verification, No Restrictions			1
Normal Cardholder Verification—Goods and services only at Point of Sale (no cash back)			2
ATM Only, PIN Required			3
PIN Required—Goods and services only at Point of Sale (no) (cash back)			5
Prompt for PIN if PIN Pad Present			6
Prompt for PIN if PIN Pad Present—Goods and services only at Point of Sale (no cash back)			7

(الملحق رقم 7)

لقيمة التحقق من البطاقة 1	لقيمة التحقق من البطاقة 2	لقيمة التحقق من شريحة البطاقة	الطول (الكل)
الإخراج من الخطوة 1	الإخراج من الخطوة 1	الإخراج من الخطوة 1	16
تاريخ انتهاء صلاحية البطاقة (كما هو معروض في ترميز المسار 2)	تاريخ انتهاء صلاحية البطاقة (كما هو معروض في المسار 2 لتشفير البيانات المكافئ)	تاريخ انتهاء صلاحية البطاقة (كما هو معروض في البطاقة)	¹ 4
يجب ألا تكون قيمة رمز الخدمة "000"	يجب أن تكون قيمة رمز الخدمة "999"	يجب أن تكون قيمة رمز الخدمة "999"	3
المجموع			² 4

(الملحق رقم 8)

قيم رمز الخدمة

التعريف	موضع 2	موضع 2	موضع 3
البطاقة الدولية	1		
البطاقة الدولية - بطاقة الدائرة المتكاملة	2		
الاستخدام الوطني فقط	5		
الاستخدام الوطني فقط - بطاقة الدائرة المتكاملة	6		
العلامة الخاصة أو بطاقة الملكية	7		
التفويض العادي	0		
مطلوب ترخيص عبر الإنترنت	2		
يلزم إدخال رقم التعريف الشخصي	0		
التحقق العادي من حامل البطاقة، لا قيود	1		
التحقق العادي من حامل البطاقة - السلع والخدمات فقط في نقاط البيع (بدون استرداد نقدي).	2		
ماكينة الصراف الآلي فقط، يلزم إدخال رقم التعريف الشخصي	3		
يلزم إدخال رقم التعريف الشخصي - السلع والخدمات فقط في نقطة البيع (لا استرداد نقدي).	5		
المطالبة برقم التعريف الشخصي في حالة وجود لوحة رقم التعريف الشخصي	6		
المطالبة برقم التعريف الشخصي في حالة وجود لوحة رقم التعريف الشخصي - السلع والخدمات فقط في نقطة البيع (بدون استرداد نقدي)	7		

1 For OBKM, the format of the Card expiration date may be as presented as either YYMM or MMY¹.
2 The output from Step 1 is 16 digits long. The resulting string reflects 23 digits (3+4+16) and is 92 bits long.

1 بالنسبة إلى OBKM، قد يتم عرض تنسيق تاريخ انتهاء صلاحية البطاقة على أنه YYMM أو MMY¹.
2 يبلغ طول الإخراج من الخطوة (1) 16 رقماً. تعكس السلسلة الناتجة 23 رقماً (3 + 4 + 16) ويبلغ طولها 92 بتًا.

Appendix Number 9

Acceptance Environment	Display Requirements
Face-to-face Transactions	At physical Merchant locations, the preferred way to communicate acceptance is to display the Mark on a main entry door or on a nearby window. If these locations are not available, the Mark must be displayed so that it is seen easily from outside the premises.
	When a Cardholder-facing POS Terminal is present at a Merchant location, the Mark must be displayed on the POS Terminal at parity (in terms of size, frequency, and location) with all other acceptance marks of any type shown.
ATMs and POS Terminals	The Mark must be displayed on the ATM or POS Terminal or on its screen, or in both locations.
E-commerce, mail order, telephone order, recurring payment and other CNP Transactions	For e-commerce, mail order, phone order, recurring payment and other CNP Transactions, the Mark must be displayed where payment options are presented.
Agent locations	The same requirements apply as for Merchant locations.

Appendix 10

Type	Interactive
Routing	- From an Acquirer processing system (APS) to the Authorization Platform. - From the Authorization Platform to an IPS.
Response	An Authorization Request Response/0110 message is required.

Appendix 11

Type	Interactive
Routing	From an IPS to the Authorization Platform. From the Authorization Platform to an Acquirer processing system APS.
Response	The Acquirer processing system APS may provide an Authorization Acknowledgement/0180 – 1180 message to the Authorization Platform to acknowledge positive receipt of the Authorization Request Response/0110 – 1110 message from the Authorization Platform. The Authorization Acknowledgement/0180 – 1180 message is optional for an Acquirer processing system APS.

Appendix 12

Type	Non-Interactive
Routing	From the Acquirer processing system APS to an Issuer processing system IPS.
Response	An Authorization Advice Response/0130—Issuer-generated message is required.

Appendix 13

Type	Non-Interactive
Routing	From the IPS to the Authorization Platform.
Response	An Authorization Advice Response/0130—System-generated message is required.

(الملحق رقم 9)

بيئة القبول	متطلبات العرض
المعاملات التي تتم وجها لوجه	في مواقع التاجر الفعلية، تتمثل الطريقة المفضلة للإبلاغ عن القبول في عرض العلامة على بوابة الدخول الرئيسية أو على الأبواب الداخلية أو على النوافذ القريبة. وفي حالة عدم توفر هذه المواقع، يجب عرض العلامة بشكل يسمح برؤيتها بسهولة من خارج المبنى.
	عند وجود محطة نقطة بيع مواجهة لحامل البطاقة في موقع التاجر، يجب عرض العلامة على محطة نقاط البيع على قدم المساواة (من حيث الحجم والتكرار والموقع) مع جميع علامات القبول الأخرى من أي نوع معروضة.
أجهزة الصراف الآلي ومحطات نقاط البيع	يجب عرض العلامة على جهاز الصراف الآلي أو محطة نقاط البيع أو على شاشتها أو في كلا الموقعين.
التجارة الإلكترونية والطلب عبر البريد والطلب عبر الهاتف والدفع المتكرر والدفع المتكرر ومعاملات البطاقة غير الموجودة الأخرى	بالنسبة للتجارة الإلكترونية والطلب عبر البريد والطلب عبر الهاتف والدفع المتكرر ومعاملات البطاقة غير الموجودة الأخرى، يجب عرض العلامة حيث يتم تقديم خيارات الدفع.
مواقع الوكلاء	تنطبق نفس المتطلبات على مواقع التجار.

(الملحق رقم 10)

النوع	تفاعلي
التوجيه	- من نظام معالجة القابل (APS) إلى منصة التفويض. - من منصة التفويض إلى IPS.
الاستجابة	استجابة طلب التفويض / 0110 مطلوبة.

(الملحق رقم 11)

النوع	تفاعلي
التوجيه	- من IPS إلى منصة التفويض. - من منصة التفويض إلى نظام معالجة القابل APS.
الاستجابة	قد يقدم نظام معالجة القابل APS رسالة إقرار تفويض / 0180-1180 إلى منصة التفويض للإقرار بالاستلام الإيجابي لرسالة استجابة طلب التفويض / 0110 - 1110 من منصة التفويض. تعتبر رسالة إقرار التفويض / 0180-1180 اختيارية لنظام معالجة القابل APS.

(الملحق رقم 12)

النوع	غير تفاعلي
التوجيه	من نظام معالجة القابل APS لنظام معالجة جهة الإصدار IPS.
الاستجابة	استجابة نصيحة التفويض / 0130 — الرسالة التي تنشئها جهة الإصدار مطلوبة.

(الملحق رقم 13)

النوع	غير تفاعلي
التوجيه	من IPS إلى منصة التفويض.
الاستجابة	استجابة نصيحة التفويض / 0130 —الرسالة التي ينشئها النظام مطلوبة.

Appendix 14

Type	Non-Interactive
Routing	From the Authorization Platform to an IPS.
Response	An Authorization Advice Response/0130 - 1130—Issuer-generated message is required.

Appendix 15

Type	Non-Interactive
Routing	From the Issuer processing system IPS to the Acquirer processing system APS when responding to the Authorization Advice/0120 - 1120—Acquirer-generated message.
Response	None.

Appendix 16

Type	Non-Interactive
Routing	From the IPS to the Authorization Platform when responding to the Authorization Advice/0120 - 1120—System-generated message.
Response	None.

Appendix 17

Type	Non-Interactive
Routing	From the Authorization Platform to the Acquirer processing system APS to the Issuer processing system IPS.
Response	None.

Appendix 18

Type	Interactive
Routing	From an Acquirer processing system APS to the Authorization Platform.
Response	None.

Appendix 19

Type	Interactive
Routing	From an Acquirer processing system APS to the Authorization Platform.
Response	None.

(الملحق رقم 14)

النوع	غير تفاعلي
التوجيه	من منصة التفويض إلى IPS.
الاستجابة	مطلوب استجابة نصيحة التفويض / -0130 1130—الرسالة التي تنشئها جهة الإصدار مطلوبة.

(الملحق رقم 15)

النوع	غير تفاعلي
التوجيه	من نظام معالجة جهة الإصدار IPS إلى نظام معالجة القابل APS عند الاستجابة لإشعارالتفويض / -0120 1120 — الرسالة التي أنشأتها جهة القبول.
الاستجابة	لا توجد.

(الملحق رقم 16)

النوع	غير تفاعلي
التوجيه	التوجيه من IPS إلى منصة التفويض عند الاستجابة لإشعارالتفويض / 0120 - 1120 — رسالة من إنشاء النظام.
الاستجابة	لا توجد.

(الملحق رقم 17)

النوع	غير تفاعلي
التوجيه	من منصة التفويض إلى نظام معالجة جهة القبول APS إلى نظام معالجة جهة الامدار IPS.
الاستجابة	لا توجد.

(الملحق رقم 18)

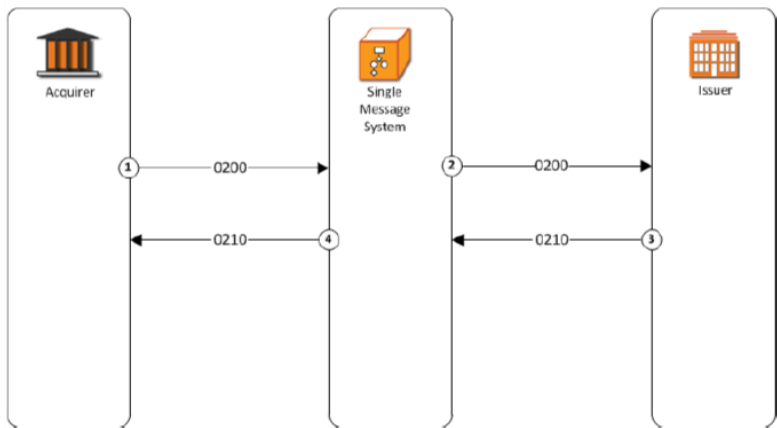
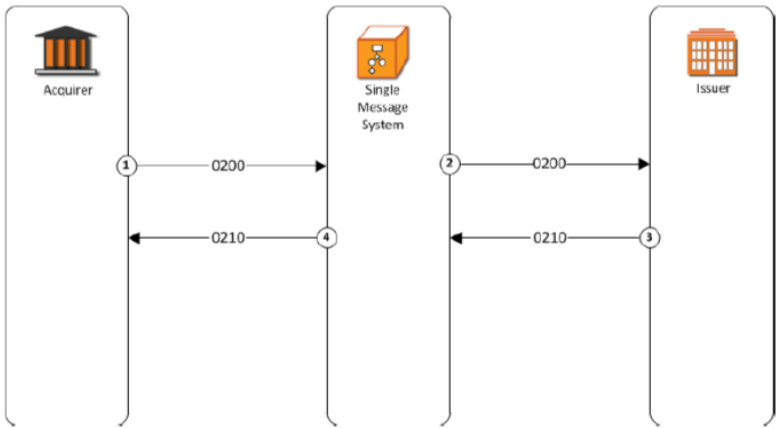
النوع	تفاعلي
التوجيه	من APS لنظام معالجة جهة القبول إلى منصة التفويض.
الاستجابة	لا توجد.

(الملحق رقم 19)

النوع	تفاعلي
التوجيه	من منصة التفويض إلى IPS.
الاستجابة	لا توجد.

Appendix 20

(الملحق رقم 20)



Appendix 21

(الملحق رقم 21)

Type	Interactive
Routing	From an Acquirer to the network and from the network to an Issuer.
Response	A Financial Transaction Request Response/0210 message is required.

النوع	تفاعلي
التوجيه	من جهة القبول إلى الشبكة ومن الشبكة إلى جهة الإصدار.
الإستجابة	استجابة طلب معاملة مالية/ 0210 مطلوبة

Appendix 22

(الملحق رقم 22)

Type	Non-Interactive
Routing	From an Issuer to the network and from the network to an Acquirer.
Response	The Single Message System will provide an Acquirer Reversal Advice/0420 message to an Issuer when the Issuer processing system responds with a late Financial Transaction Re-sponse/0210 message to a Financial Transaction Request/0200 message.

النوع	تفاعلي
التوجيه	من جهة الإصدار إلى الشبكة ومن الشبكة إلى جهة القبول.
الإستجابة	سيوفر نظام الرسالة الفردية رسالة إشعار عكس المستلم/ 0420 إلى جهة الإصدار عندما يستجيب نظام معالجة جهة الاعداد برسالة استجابة معاملة مالية متأخرة/ 0210 إلى رسالة طلب معاملة مالية/ 0200.

Appendix 23

(الملحق رقم 23)

Type	Non-Interactive
Routing	From an Acquirer to the network and from the network to an Issuer.
Response	A Financial Transaction Advice Response/0230 message is required.

النوع	غير تفاعلي
التوجيه	من جهة القبول إلى الشبكة ومن الشبكة إلى جهة الإصدار.
الإستجابة	استجابة إشعار المعاملات المالية/ 0230 مطلوبة.

Appendix 24

(الملحق رقم 24)

Type	Non-Interactive
Routing	From the network to an Acquirer and from an Issuer to the network.
Response	None.

النوع	غير تفاعلي
التوجيه	من الشبكة إلى جهة القبول ومن جهة الإصدار إلى الشبكة.
الإستجابة	لا توجد.

Appendix 25

(الملحق رقم 25)

Type	Interactive
Routing	From an IPS to the Authorization Platform.
Response	An Issuer File Update Request Response/0312 message is required.

النوع	تفاعلي
التوجيه	من IPS إلى منصة التفويض.
الإستجابة	استجابة طلب تحديث ملف جهة الإصدار/ 0312 مطلوبة.

Appendix 26

Type	Interactive
Routing	From the Authorization Platform to an IPS.
Response	None

Appendix 27

Type	Interactive
Routing	From the Acquirer to the Issuer or intermediate network facility
Response	A Reversal Request Response/0410 message is required

Appendix 28

Type	Interactive
Routing	From the Issuer to the Acquirer
Response	None

Appendix 29

Type	Non-Interactive
Routing	From the Authorization Platform to an IPS.
Response	A Reversal Advice Response/0430 message is required.

Appendix 30

Type	Non-Interactive
Routing	From an IPS to the Authorization Platform.
Response	None

Appendix 31

Type	Non-Interactive
Routing	From an acquirer to the Single Message System
Response	An Acquirer Reversal Advice Response/0430 message is required.

Appendix 32

Type	Interactive
Routing	Between the Authorization Platform and any other party (such as CPS, APS, IPS, INF) communicating directly with the Authorization Platform. May be originated by either party.
Response	A Network Management Request Response/0810 message is required.

(الملحق رقم 26)

النوع	تفاعلي
التوجيه	من منصة التفويض إلى IPS.
الاستجابة	لا توجد.

(الملحق رقم 27)

النوع	تفاعلي
التوجيه	من الجهة القابلة إلى جهة الإصدار أو منشأة الشبكة الوسيطة.
الاستجابة	رد طلب الإلغاء/ 0410 مطلوب

(الملحق رقم 28)

النوع	تفاعلي
التوجيه	من جهة الإصدار إلى جهة القبول.
الاستجابة	لا توجد.

(الملحق رقم 29)

النوع	غير تفاعلي
التوجيه	من منصة التفويض إلى IPS.
الاستجابة	رسالة استجابة إشعارالإلغاء/ 0430 مطلوبة.

(الملحق رقم 30)

النوع	غير تفاعلي
التوجيه	من IPS إلى منصة التفويض.
الاستجابة	لا توجد.

(الملحق رقم 31)

النوع	غير تفاعلي
التوجيه	من القابل إلى نظام الرسالة الواحدة. من نظام الرسائل الفردية إلى جهة الإصدار.
الاستجابة	مطلوب رسالة "رد الإشعار عكسي لجهة القبول"/ 0430.

(الملحق رقم 32)

النوع	تفاعلي
التوجيه	بين منصة التفويض وأي طرف آخر (مثل CPS و APS و IPS و INF) يتواصل مباشرة مع منصة التفويض. ويمكن أن يكون قد تم إنشاؤه من قبل أي من الطرفين.
الاستجابة	استجابة طلب إدارة الشبكة / 0810 مطلوبة.

Appendix 33

(الملحق رقم 33)

Type	Interactive
Routing	From “receiver” to “originator” of the related Network Management Request/0800.
Response	None

Appendix 34

(الملحق رقم 34)

Type	Non-Interactive
Routing	From the Authorization Platform to any other party (such as CPS, APS, IPS, INF) communicating directly with the Authorization Platform. NOTE: May not be originated by any party other than the Authorization Platform.
Response	None

Appendix 35

(الملحق رقم 35)

Product and Transaction Type	Issuer Response Time (in seconds)	Alternate Authorization Provider (if applicable)	Acquirer Minimum Wait Time (in seconds)
Point-of-Sale (POS)	9	3	12
ATM	12	6	18

Appendix 35

(الملحق رقم 36)

Message Type Identifier	Function Code	Description
	200	First Presentment
	696	Financial Detail Addendum
	450	First Chargeback (Full)
	451	Arbitration Chargeback (Full)
	453	First Chargeback (Partial)
	454	Arbitration Chargeback (Partial)
	205	Second Presentment (Full)
	282	Second Presentment (Partial)
	603	Retrieval Request
	605	Retrieval Request Acknowledgement
	700	Fee Collection (Member-generated)
	780	Fee Collection Return (Member-generated)
	781	Fee Collection Resubmission (Member-generated)
	782	Fee Collection Arbitration Return (Member-generated)
	783	Fee Collection (Clearing System-generated)

النوع	تفاعلي
التوجيه	من "المتلقي" إلى "المنشئ" لطلب إدارة الشبكة ذي الصلة / 0800.
الإستجابة	لا توجد.

النوع	غير مفعّل
التوجيه	من منصة التفويض إلى أي طرف آخر (مثل CPS و APS و IPS و INF) يتواصل مباشرة مع منصة التفويض. ملاحظة: قد لا يتم إنشاؤها من قبل أي طرف آخر غير منصة التفويض.
الإجابة	لا شيء.

نوع المنتج والمعاملات	وقت استجابة جهة الإصدار (بالثواني)	توفر تفويض بديل (إن وجد)	الحد الأدنى لمهلة انتظار جهة القبول (بالثواني)
نقاط البيع (POS)	9	3	12
جهاز الصراف الآلي	12	6	18

مُعرّف نوع الرسالة	رمز الوظيفة	الوصف
	200	التقديم الأول
	696	ملحق التفاصيل المالية
	450	عملية رد المبالغ المدفوعة (كاملة)
	451	رد مبالغ التحكيم المدفوعة (كاملة)
	453	رد المبالغ المدفوعة الأولى (جزئي)
	454	رد مبالغ التحكيم المدفوعة (جزئي)
	205	التقديم الثاني (كامل)
	282	التقديم الثاني (جزئي)
	603	طلب استرداد
	605	إقرار طلب الاسترداد
	700	تحصيل الرسوم (من إنشاء الأعضاء)
	780	عائد تحصيل الرسوم (من إنشاء الأعضاء)
	781	إعادة تقديم تحصيل الرسوم (من إنشاء الأعضاء)
	782	إرجاع تحصيل رسوم التحكيم (من الأعضاء)
	783	تحصيل الرسوم (المقاصة التي تم إنشاؤها بواسطة النظام)

Appendix 37

(الملحق رقم 37)

Type	Interactive
Interbank Settlement System (for example, High Value [RTGS] and Low Value [ACH] Payment Systems)	Payments remitted via national interbank settlement systems are considered final in accordance with the rules of the national payment system in which the funds transfer is executed. For purposes of establishing settlement finality and discharge of obligations, funds become irrevocable when such funds are no longer subject to unwinding or a revocation period.
All Other Payment Methods (for example, book transfer and local payment systems)	Payments remitted through any other method are considered final when (i) funds are received by, or sent from, as the case may be, the National Scheme Operator settlement Service Provider, and (ii) such transfer of funds becomes irrevocable. For purposes of establishing settlement finality and discharge of obligations, funds become irrevocable when such funds are no longer subject to unwinding or a revocation period.

Appendix 38

(الملحق رقم 38)

Type	Non-Interactive
Interbank Settlement Systems	The settlement obligation of a net-debit customer is deemed discharged (i) upon crediting of funds in full to the National Scheme Operator settlement Service Provider’s CBL account, and (ii) when such receipt of funds becomes irrevocable. The payment obligation to a net-credit customer is deemed discharged upon debiting of funds in full from the National Scheme Operator settlement Service Provider’s CBL account for the benefit of such net-credit Member.
Book Transfer	The settlement obligation of a net-debit customer is deemed discharged (i) upon debiting of funds from the Member designated settlement account at the National Scheme Operator settlement Service Provider and credited in full to the National Scheme Operator settlement account or the National Scheme Operator settlement Service Provider’s in-transit account, and (ii) when such receipt of funds becomes irrevocable. The payment obligation to a net-credit customer is deemed discharged upon crediting of funds to the customer-designated settlement account at the National Scheme Operator settlement Service Provider for the benefit of such net-credit Member.
Local Payment Systems (if settlement occurs in commercial bank funds [and not through an interbank settlement system])	The settlement obligation of a net-debit Member is deemed discharged (i) upon crediting of funds in full to the National Scheme Operator settlement account or National Scheme Operator settlement Service Provider’s in-transit account, and (ii) when such receipt of funds becomes irrevocable. The payment obligation to a net-credit Member is deemed discharged upon debiting of funds in full from the National Scheme Operator settlement account or the National Scheme Operator settlement Service Provider’s in-transit bank account for the benefit of such net-credit customer.

Appendix 39

(الملحق رقم 39)

Unpaid Settlement Obligation	Daily Assessment
LYD 0.00 to LYD XXXXXX	Interest only
LYD XXXXXX to LYD XXXXXX	LYD XXXXX plus interest
LYD XXXXXX or more	0.xx% of the unpaid settlement obligation (multiply by 0.00xx) plus interest

Appendix 40

Compensation	=	Principal	x	Settlement Agent Earnings Credit Rate	x	Number of Days
				360		

النوع	تفاعلي
نظام التسوية بين المصارف (على سبيل المثال، أنظمة الدفع ذات القيمة العالية [RTGS] والقيمة المنخفضة [ACH])	تعتبر المدفوعات المحولة عبر أنظمة التسوية الوطنية بين المصارف نهائية وفقًا لقواعد شبكة الدفع المحلية الذي يتم فيه تنفيذ تحويل الأموال. لأغراض تحديد نهائية التسوية والوفاء بالالتزامات، تصبح الأموال غير قابلة للإلغاء عندما لا تكون هذه الأموال خاضعة للتصفية أو فترة الإلغاء.
جميع طرق الدفع الأخرى (على سبيل المثال، تحويل الكتاب وأنظمة الدفع المحلية)	تعتبر المدفوعات المحولة من خلال أي طريقة أخرى نهائية عندما: (1) يتم استلام الأموال من قبل مقدم خدمة التسوية لمشغل شبكة الدفع المحلية أو إرسالها منه، حسب الحالة. (2) يصبح تحويل الأموال هذا غير قابل للإلغاء. لأغراض تحديد نهائية التسوية والوفاء بالالتزامات، تصبح الأموال غير قابلة للإلغاء عندما لا تكون هذه الأموال خاضعة للتصفية أو فترة الإلغاء.

أنظمة التسوية بين المصارف	يُعتبر التزام التسوية الخاص بعميل مدين صافي مُبرأ: (1) عند إيداع الأموال بالكامل في حساب مصرف ليبيا المركزي الخاص بمقدم خدمة التسوية لمشغل شبكة الدفع المحلية (2) عندما يصبح هذا الاستلام غير قابل للإلغاء. يُعتبر التزام الدفع لعميل الائتمان الصافي مُبرأ منه عند خصم الأموال بالكامل من حساب مصرف ليبيا المركزي الخاص بمقدم خدمة التسوية لمشغل شبكة الدفع المحلية لصالح عضو صافي الائتمان هذا.
تحويل الكتاب	يُعتبر التزام التسوية الخاص بعميل صافي المدين مُبرأ منه: (1) عند خصم الأموال من حساب التسوية المعين للعضو في مقدم خدمة تسوية مشغل شبكة الدفع المحلية وإضافته بالكامل إلى حساب تسوية مشغل شبكة الدفع المحلية أو تسوية مشغل شبكة الدفع المحلية الحساب العابر لمقدم الخدمة (2) عندما يصبح هذا الاستلام للأموال غير قابل للإلغاء. يُعتبر التزام الدفع لعميل الائتمان الصافي مُبرئًا عند إيداع الأموال في حساب التسوية المخصص للعميل في مقدم خدمة تسوية مشغل شبكة الدفع المحلية لصالح عضو صافي الائتمان
أنظمة الدفع المحلية (في حالة حدوث التسوية بأموال المصارف التجارية) (وليس من خلال نظام تسوية بين المصارف).	يُعتبر التزام التسوية لعضو مدين صافي مُبرأ: (1) عند إيداع الأموال بالكامل في حساب تسوية مشغل شبكة الدفع المحلية أو الحساب العابر لمقدم خدمة تسوية مشغل شبكة الدفع المحلية (2) عندما يصبح استلام الأموال غير قابل للإلغاء. يُعتبر التزام الدفع لعضو الائتمان الصافي مُبرأً منه عند خصم الأموال بالكامل من حساب تسوية مشغل شبكة الدفع المحلية أو الحساب المصرفي العابر لمقدم خدمة التسوية لمشغل شبكة الدفع المحلية لصالح عميل صافي الائتمان.

(الملحق رقم 39)

التزام التسوية غير المسددة	التقييم اليومي
0.00 دينار ليبي إلىXXXXXX دينار ليبي	الفائدة فقط
XXXXXX دينار ليبي إلى XXXXXX دينار ليبي	XXXXX دينارليبي بالإضافة إلى الفائدة
XXXXXX دينار ليبي أو أكثر	xx.0٪ من التزام التسوية غير المسدد (الضرب في 0.00xx) بالإضافة إلى الفائدة

(الملحق رقم 40)

Compensation	=	Principal	x	Settlement Agent Earnings Credit Rate	x	Number of Days
				360		

Appendix 41

Compensation	=	Principal	x	(Settlement Agent Overdraft Rate + 2 percent)	x	Number of Days
360						

Appendix 42

For the following Transaction...	The Transaction date is the date on which...
Face-to-Face	The products or services are exchanged.
Non-Face-to-Face	The products are shipped or services performed.
Vehicle Rental	The vehicle is returned, or, if applicable, the prepayment date.
Lodging	Checkout occurred, or if applicable, the prepayment date.
No-show	The Cardholder was expected to arrive at the lodging Merchant and failed to appear.
Airline/Railway	The airline or railway ticket was issued.
Cruise Line	The transportation documents were issued.
On-board Cruise Line	The passenger disembarks.
Refund	The Merchant grants a credit or price adjustment.

Appendix 43

An Issuer with both of the following...	Daily Assessment
- Greater than two times the global fraud basis points average - LYD XXXXXX or more, annually in fraud losses	Implement additional fraud loss control monitoring programs to detect fraudulent Transactions

Appendix 44

Period	Amount assessed a month
First quarter of noncompliance	LYD XXXXX a month
Second quarter of noncompliance	LYD XXXXX a month
Third quarter of noncompliance	LYD XXXXX a month
Each month after the third quarter of noncompliance	LYD XXXXX a month

Appendix 45

The following cybersecurity Standards documents:	May be found at:
PCI Security Standards, including all of the documents listed in Table 6.3	https://www.pcisecuritystandards.org
NIST Cybersecurity Framework (NIST CSF) and NIST CSF “Informative References”	https://www.nist.gov/cyberframework

(الملحق رقم 41)

Compensation	=	Principal	x	(Settlement Agent Overdraft Rate + 2 percent)	x	Number of Days
360						

(الملحق رقم 42)

بالنسبة للمعاملة التالية...	تاريخ المعاملة هو التاريخ الذي ...
وجها لوجه	يتم فيه تبادل المنتجات أو الخدمات.
ليست وجها لوجه	يتم فيه شحن المنتجات أو تنفيذ الخدمات.
إيجار مركبة	يتم فيه إرجاع المركبة، أو تاريخ الدفع المسبق، إن أمكن.
الإقامة	يتم فيه تسجيل الخروج، أو تاريخ الدفع المسبق، إن أمكن.
عدم الحضور	كان من المتوقع فيه أن يصل حامل البطاقة إلى تاجر الإقامة وفشل في الحضور.
الخطوط الجوية/السكك الحديدية	يتم فيه إصدار تذكرة الطيران أو القطار.
خطوط الرحلات البحرية	يتم فيه إصدار وثائق النقل.
خطوط الرحلات البحرية على متن السفينة	ينزل فيه الراكب.
الاسترداد	يمنح فيه التاجر الائتمان أو تعديل السعر.

(الملحق رقم 43)

جهة الإصدار مع كلاً مما يلي ...	التقييم اليومي
- أكثر من ضعف متوسط نقاط الاحتيال العالمية - دينار ليبي XXXXXX أو أكثر سنويًا في خسائر الاحتيال	تنفيذ برامج إضافية لمراقبة مكافحة خسائر الاحتيال للكشف عن المعاملات الاحتيالية

(الملحق رقم 44)

الفترة	المبلغ المقدر في الشهر
الربع الأول من عدم الامتثال	XXXXX دينار في الشهر
الربع الثاني من عدم الامتثال	XXXXX دينار في الشهر
الربع الثالث من عدم الامتثال	XXXXX دينار في الشهر
كل شهر بعد الربع الثالث من عدم الامتثال	XXXXX دينار في الشهر

(الملحق رقم 45)

مستندات معايير الأمن السيبراني التالية:	يمكن العثور عليها في:
معايير أمان صناعة بطاقات الدفع، بما في ذلك جميع المستندات المدرجة في الجدول 6.3	https://www.pcisecuritystandards.org
المعهد الوطني للمعايير والتكنولوجيا إطار الأمن السيبراني و"المراجع الإعلامية" للمعهد الوطني للمعايير والتكنولوجيا إطار الأمن السيبراني	https://www.nist.gov/cyberframework

Appendix 46

(الملحق رقم 46)

PCI Security Standard	Compliance is Required for:
PCI Data Security Standard (“PCI DSS”)	All Issuers, Acquirers, Merchants, Service Providers, and any other person or entity that a Member permits, directly or indirectly, to store, transmit, or process Account data. Validation of compliance is required for Level 1, 2 and 3 Merchants and all Service Providers under the Site Data Protection Program.
PCI Payment Application Data Security Standard (“PCI PA-DSS”)	All Merchants and Service Providers that use third party-provided payment applications. Refer to the PCI PA-DSS Program Guide for information about the applicability of the PCI PA-DSS to third party-provided payment applications. Refer to the PCI QIR Program Guide for information about the applicability of Qualified Integrator & Reseller (QIR) engagement for third party-provided payment application implementation. Use of a QIR listed on the PCI Security Standards Council (SSC) website is strongly recommended.
PCI Forensic Investigator Program Guide (“PFI Program Guide”)	Any Acquirer that engages the services of a PCI SSC Forensic Investigator (PFI) to conduct an independent forensic investigation in order to assess the cause, scope, magnitude, duration, and effects of an Account Data Compromise Event or Potential Account Data Compromise Event.
PCI Token Service Providers—Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens) (“PCI TSP Security Requirements”)	Any Issuer that performs Token Service Provider (TSP) services on its own behalf and any entity that performs or proposes to perform TSP Program Service as the TSP of a Member.
PCI 3-D Secure—Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: Access Control Server (ACS), Directory Server (DS), and 3DS Server (3DSS) (“PCI 3DS Core Security Standard”)	Any Service Provider that performs or provides 3-D Secure (3DS) functions as defined in the EMV 3-D Secure Protocol and Core Functions Specification. Validation of compliance is required for such Service Providers under the Site Data Protection. Compliance is strongly recommended for any Merchant that performs or provides 3DS functions as defined in the EMV 3-D Secure Protocol and Core Functions Specification.
PCI 3-D Secure—Security Requirements and Assessment Procedures for EMV 3-D Secure SDK (“PCI 3DS SDK Security Standard”)	Any Service Provider that uses 3-D Secure (3DS) Software Development Kits (SDKs). Use of approved 3DS SDKs is strongly recommended for any Merchant that performs or provides 3DS functions as defined in the EMV 3-D Secure Protocol and Core Functions Specification. Approved 3DS SDKs are listed on the PCI SSC website at www.pcisecuritystandards.org .
PCI Point-to-Point Encryption: Solution Requirements and Testing Procedures	Eligible Merchants participating in the PCI DSS Compliance Validation Exemption Program and implementing a Point-to-Point (P2PE) solution.
PCI Card Production & Provisioning Physical Security Requirements PCI Card Production & Provisioning Logical Security Requirements	All Card production vendors, pursuant to the Global Vendor Certification Program (GVCP), and any Issuer that performs Card production activities on its own behalf.
PCI PIN Security Requirements PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements PCI PIN Transaction Security (PTS) Hardware Security Module (HSM) Security Requirements PCI PIN Transaction Security (PTS) Device Testing and Approval Program Guide and PCI Approved PTS Devices list	All Members and their agents performing PIN encipherment or any other aspect of PIN processing involving PIN entry by means of a: - PIN Entry Device (PED) or Encrypting PIN PAD (EPP) on a Terminal (including an MPOS Terminal); or - PIN CVM Application in a Software-based PIN entry on Commercial Off-The-Shelf (COTS) device (“SPoC Solution”).

معيار أمان PCI	الامتثال مطلوب من أجل:
معيار أمان بيانات PCI DSS (“PCI”)	جميع جهات الإصدار وجهات القبول والتجار ومقدمي الخدمات وأي شخص أو كيان آخر يسمح له العضو، بشكل مباشر أو غير مباشر، بتخزين بيانات الحساب أو نقلها أو معالجتها. التحقق من الامتثال المطلوب للتجار من المستوى 1 و 2 و 3 وجميع مقدمي الخدمة بموجب برنامج حماية بيانات الموقع
معيار أمان بيانات تطبيق الدفع PCI PA-DSS (“PCI”)	جميع التجار ومقدمي الخدمات الذين يستخدمون تطبيقات الدفع المقدمة من جهات خارجية. راجع دليل برنامج PCI PA-DSS للحصول على معلومات حول إمكانية تطبيق PCI PA-DSS على تطبيقات الدفع المقدمة من جهات خارجية.
دليل برنامج محقق التحقيق الجنائي PCI (“دليل برنامج PFI”)	أرجع إلى دليل برنامج PCI QIR للحصول على معلومات حول إمكانية تطبيق مشاركة المُدمج المؤهل والبائع (QIR) لتنفيذ تطبيق الدفع المقدم من جهة خارجية. يوصى بشدة باستخدام QIR المدرج في موقع PCI مجلس معايير أمان (SSC).
مقدمو خدمة رمز PCI - متطلبات الأمان الإضافية وإجراءات التقييم لمقدمي خدمة الرمز المميز (رموز الدفع EMV) (“متطلبات أمان PCI TSP”)	أي جهة أستحواذ تستخدم خدمات المحقق الجنائي (PFI) لـ PCI SSC لإجراء تحقيق جنائي مستقل من أجل تقييم السبب والنطاق والحجم والمدة والتأثيرات لحدث اختراق بيانات الحساب أو حدث اختراق بيانات الحساب المحتمل.
PCI 3-D Secure - متطلبات الأمان وإجراءات التقييم للمكونات الأساسية الآمنة EMV® 3-D Secure: خادم التحكم في الوصول (ACS) وخادم الدليل (DS) وخادم 3DS (“معيار الأمان الأساسي لـ PCI 3DS”)	أي جهة إصدار تؤدي خدمات مقدم خدمة الرموز (TSP) نيابةً عنه وأي كيان يؤدي أو يقترح أداء خدمة برنامج TSP كعضو TSP.
أي مقدم خدمة الذي ينفذ أو يوفر وظائف 3-D Secure (3D Secure) على النحو المحدد في بروتوكول EMV 3-D الآمن ومواصفات الوظائف الأساسية.	مطلوب التحقق من الامتثال لمقدمي الخدمة هؤلاء بموجب حماية بيانات الموقع.
يوصى بشدة بالامتثال لأي تاجر يؤدي أو يوفر وظائف DS3 على النحو المحدد في بروتوكول EMV 3-D الآمن ومواصفات الوظائف الأساسية.	
أي مقدم خدمة يستخدم مجموعات تطوير البرامج (SDKs) ثلاثية الأبعاد الآمنة (3DS). يوصى بشدة باستخدام حزم SDK ثلاثية الأبعاد المعتمدة لأي تاجر يؤدي أو يقدم وظائف 3DS على النحو المحدد في بروتوكول EMV ثلاثي الأبعاد الآمن ومواصفات الوظائف الأساسية. يتم سرد حزم SDK ثلاثية الأبعاد المعتمدة على موقع ويب PCI SSC على www.pcisecur-citystandards.org .	
تشفير PCI من نقطة إلى نقطة: متطلبات الحل وإجراءات الاختيار.	التجار المؤهلون المشاركون في برنامج الإعفاء من التحقق من الامتثال لـ PCI DSS وتنفيذ حل من نقطة إلى نقطة (P2PE).
إنتاج بطاقة PCI وتوفير متطلبات الأمن المادي. إنتاج بطاقة PCI وتوفير متطلبات الأمان المنطقية.	جميع باتعي إنتاج البطاقات، وفقاً لبرنامج اعتماد البائعين العالميين (GVCP)، وأي جهة إصدار تؤدي أنشطة إنتاج البطاقات نيابةً عنها.
متطلبات أمان PCI PIN. متطلبات الأمان المعيارية لنقطة التفاعل (POI) الخاصة بأمان معاملات PCI PIN (PTS) متطلبات أمان وحدة أمان الأجهزة (HSM) الخاصة بأمان معاملات PCI PIN (PTS) دليل برنامج اختبار واعتماد جهاز PCI PIN لأمان المعاملات (PTS) وقائمة أجهزة PTS المعتمدة من PCI PCI إدخال رقم التعريف الشخصي المستند إلى البرامج في متطلبات أمان SPoC (COTS)	يقوم جميع الأعضاء ووكلائهم بإجراء تشفير رقم التعريف الشخصي أو أي جانب آخر من جوانب معالجة رقم التعريف الشخصي تتضمن إدخال رقم التعريف الشخصي عن طريق: - جهاز إدخال رقم التعريف الشخصي (PED) أو تشفير PIN PAD (EPP) على جهاز (بما في ذلك محطة MPOS) ؛ أو - تطبيق PIN CVM في إدخال رقم التعريف الشخصي المستند إلى البرامج على جهاز تجاري خارج الرق (COTS) (“حل SPoC”).

Appendix 47

(الملحق رقم 47)

Failure of the following to comply with the SDP Program mandate...	Can result in an assessment of...
Classification	Violations per calendar year
Level 1 and Level 2 Merchants	Up to LYD XXXXX for the first violation Up to LYD XXXXX for the second violation Up to LYD XXXXX for the third violation Up to LYD XXXXX for the fourth violation
Level 3 Merchants	Up to LYD XXXXX for the first violation Up to LYD XXXXX for the second violation Up to LYD XXXXX for the third violation Up to LYD XXXXX for the fourth violation
Level 1 and Level 2 Service Providers	Up to LYD XXXXX for the first violation Up to LYD XXXXX for the second violation Up to LYD XXXXX for the third violation Up to LYD XXXXX for the fourth violation

Appendix 48

For this reporting period...	Submit the form(s) no later than...
1 October to 31 March	31 March
1 April to 30 September	30 September

Appendix 49

Code	Description
00	Lost Fraud —A fraudulent Transaction that occurs with the use of a lost Card or other Access Device (or other instrument accessing an Account—for example, convenience and balance transfer checks) without the actual, implied, or apparent authority of the Cardholder.
01	Stolen Fraud —A fraudulent Transaction that occurs with the use of a stolen Card or other Access Device (or other instrument accessing an Account—for example, convenience and balance transfer checks) without the actual, implied, or apparent authority of the Cardholder.
02	Never Received or Issued —The interception and use of a Card or other Access Device (or other instrument accessing an Account—for example, convenience and balance transfer checks), before receipt by the Cardholder, by a person without the actual, implied, or apparent authority of the Cardholder.
03	Fraudulent Application —A fraudulent Transaction that occurs with the use of a Card or other Access Device that was obtained with an application using a false name or other false identification information.
04	Counterfeit Card Fraud —The use of an altered or illegally reproduced Card or other Access Device (or other instrument accessing an Account—for example, convenience and balance transfer checks) including the replication or alteration of the magnetic stripe or embossing.
05	Account Takeover Fraud —An existing credit or debit Account is used without the actual, implied, or apparent authority of the Cardholder, by a person who gains access to and use of the Account through unauthorized means, such as a change of address or request for the re-issuance of a Card or other Access Device (or other instrument for accessing an Account—for example, convenience and balance transfer checks) but not lost or stolen Cards.
06	Card Not Present Fraud —A fraudulent Transaction that occurs with the use of credit or debit Account information including pseudo-account information without the Card or other Access Device being involved, via the phone, mail, Internet, or other electronic means without the actual, implied, or apparent authority of the Cardholder.
51	Bust-out Collusive Merchant —A collusive Cardholder engaging in Transactions with a collusive Merchant as defined in the Questionable Merchant Audit Program.
55	Manipulation of Payment (EEA only) —An unauthorized payment transaction made as the result of the loss, theft, or misappropriation of sensitive payment data or payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed by the payer.
56	Manipulation of Cardholder (EEA only) —Any payment transaction that was made as a result of the payer being manipulated by the fraudster to provide payment, or to give instruction to do so to the payment service provider, in good-faith, to a payment account that the Issuer believes belongs to a legitimate payee.

فشل ما يلي في الامتثال لتفويض برنامج SDP يمكن أن يؤدي إلى تقييم ...		
التصنيف	الانتهاكات في السنة التقويمية	
التجار من المستوى 1 والمستوى 2	ما يصل إلى XXXXX دينار ليبي عن المخالفة الأولى ما يصل إلى XXXXX دينار ليبي عن المخالفة الثانية ما يصل إلى XXXXX دينار ليبي عن للمخالفة الثالثة حتى XXXXX دينار ليبي عن للمخالفة الرابعة	
التجار من المستوى 3	ما يصل إلى XXXXX دينار ليبي عن المخالفة الأولى ما يصل إلى XXXXX دينار ليبي عن المخالفة الثانية ما يصل إلى XXXXX دينارليبي عن المخالفة الثالثة حتى XXXXX دينار ليبي عن المخالفة الرابعة	
مقدمي الخدمات من المستوى 1 والمستوى 2	ما يصل إلى XXXXX دينار ليبي عن المخالفة الأولى ما يصل إلى XXXXX دينار ليبي عن المخالفة الثانية ما يصل إلى XXXXX دينار ليبي عن المخالفة الثالثة حتى XXXXX دينار ليبي عن المخالفة الرابعة	

(الملحق رقم 48)

للفترة المشمولة بالتقرير ...	تقديم النموذج (النماذج) في موعد لا يتجاوز ...
من 1 أكتوبر إلى 31 مارس	31 مارس
من 1 أبريل إلى 30 سبتمبر	30 سبتمبر

(الملحق رقم 49)

الرمز	الوصف
00	الاحتيال المفقود - معاملة احتيالية تحدث باستخدام بطاقة مفقودة، أو جهاز وصول آخر (أو أداة أخرى للوصول إلى حساب - على سبيل المثال، شبكات الملاءمة وتحويل الرصيد) بدون السلطة الفعلية أو الضمنية أو الواضحة لحامل البطاقة.
01	الاحتيال المسروق - معاملة احتيالية تحدث باستخدام بطاقة مسروقة، أو جهاز وصول آخر (أو أداة أخرى للوصول إلى حساب - على سبيل المثال، شبكات الملاءمة وتحويل الرصيد) بدون السلطة الفعلية أو الضمنية أو الواضحة لحامل البطاقة.
02	لم يتم استلامها أو إصدارها مطلقًا - اعتراض واستخدام بطاقة أو جهاز وصول آخر (أو أداة أخرى للوصول إلى حساب - على سبيل المثال، شبكات الملاءمة وتحويل الرصيد)، قبل استلامها من قبل حامل البطاقة، من قبل شخص بدون السلطة الفعلية أو الضمنية أو الواضحة لحامل البطاقة.
03	تطبيق احتيالي - معاملة احتيالية تحدث باستخدام بطاقة أو جهاز وصول آخر تم الحصول عليه باستخدام تطبيق يستخدم اسمًا مزيفًا أو معلومات تعريف زائفة أخرى.
04	احتيال البطاقات المزورة - استخدام بطاقة معدلة أو مستنسخة بشكل غير قانوني، أو جهاز وصول آخر (أو أداة أخرى للوصول إلى حساب - على سبيل المثال، شبكات الملاءمة وتحويل الرصيد) بما في ذلك نسخ أو تغيير الشريط المغناطيسي أو النقش.
05	احتيال الاستيلاء على الحساب - يتم استخدام حساب ائتمان أو خصم قائم بدون السلطة الفعلية أو الضمنية أو الواضحة لحامل البطاقة، من قبل شخص يمكنه الوصول إلى الحساب واستخدامه من خلال وسائل غير مصرح بها، مثل تغيير العنوان أو طلب إعادة إصدار بطاقة أو جهاز وصول آخر (أو أداة أخرى للوصول إلى حساب - على سبيل المثال، صكوك الملائمة وتحويل الرصيد) ولكن ليست البطاقات المفقودة أو المسروقة.
06	احتيال البطاقة غير الموجودة - معاملة احتيالية تحدث باستخدام معلومات حساب الائتمان أو الخصم، بما في ذلك معلومات الحساب الزائفة دون استخدام البطاقة أو أي جهاز وصول آخ، عبر الهاتف أو البريد أو الإنترنت أو أي وسيلة إلكترونية أخرى دون الحاجة إلى السلطة الضمنية أو الواضحة لحامل البطاقة.
51	التاجر المتواطئ - حامل بطاقة متواطئ يشارك في معاملات مع تاجر متواطئ على النحو المحدد في برنامج تدقيق التاجر المشكوك فيه.
55	التلاعب بالدفع (EEA فقط) - معاملة دفع غير مصرح بها يتم إجراؤها نتيجة لفقدان أو سرقة أو اختلاس بيانات الدفع الحساسة أو وسيلة الدفع، سواء كان ذلك ممكنًا للدافع قبل الدفع أم لا، وسواء كان ذلك يسبب إهمال جسيم من الدافع أو تنفيذه من قبل الدافع.
56	التلاعب بحامل البطاقة (EEA فقط) - أي معاملة دفع تم إجراؤها نتيجة للتلاعب بالدافع من قبل المحتمل لتقديم الدفع، أو لإعطاء تعليمات للقيام بذلك إلى مقدم خدمة الدفع، بحسن نية، لحساب الدفع الذي تعتقد جهة الإصدار أنه ينتمي إلى المستفيد\الدافع الشرعي.

Appendix 50

For CVV 1	For CVV 2	For Chip CVV	Length (all)
Output from Step 1	Output from Step 1	Output from Step 1	16
Card expiration date (as presented in Track 2 encoding)	Card expiration date (as presented on the Card)	Card expiration date (as presented in Track 2 Equivalent Data encoding)	4
Service code value must NOT be “000”	Service code value must be “000”	Service code value must be “999”	3
Total			23

Appendix 51

IF the capture...	THEN pay this amount...
Resulted from a “Merchant Suspicious” phone call	LYD XXXX
Did not result from a “Merchant Suspicious” phone call	LYD XXXX
Leads to the capture of additional Cards	LYD XXX for each Card captured, with a maximum total of LYD XXXX for any one incident

Appendix 52

البيان	يناير	فبراير	مارس	أبريل	مايو	يونيو	يوليو	أغسطس	سبتمبر	أكتوبر	نوفمبر	ديسمبر	الإجمالي	النسبة المئوية
عدد الأجهزة													0	#DIV/0!
عدد الحركات													0	#DIV/0!
قيمة الحركات													د.ل. 0.00	#DIV/0!
الإجمالي	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	

(الملحق رقم 50)

بالنسبة لقيمة التحقق من البطاقة CVV 1	بالنسبة لقيمة التحقق من البطاقة CVV 2	بالنسبة لشريحة قيمة التحقق من البطاقة CVV	الطول (الكل)
الإخراج من الخطوة 1	الإخراج من الخطوة 1	الإخراج من الخطوة 1	16
تاريخ انتهاء صلاحية البطاقة (كما هو معروض في ترميز المسار 2)	تاريخ انتهاء صلاحية البطاقة (كما هو موضح على البطاقة)	تاريخ انتهاء صلاحية البطاقة (كما هو موضح في ترميز البيانات المكافئة للمسار 2)	4
يجب ألا تكون قيمة رمز الخدمة “000”	يجب أن تكون قيمة رمز الخدمة “000”	يجب أن تكون قيمة رمز الخدمة “999”	3
المجموع			23

(الملحق رقم 51)

إذا كان الاستيلاء ...	فادفع هذا المبلغ ...
ناتج عن مكالمة هاتفية "مشبوهة لدى التاجر"	XXXX دينار ليبي
لم ينتج عن مكالمة هاتفية "مشبوهة لدى التاجر"	XXXX دينار ليبي
يؤدي إلى الاستيلاء على بطاقات إضافية	XXX دينار ليبي لكل بطاقة تم الاستيلاء عليها، بحد أقصى XXXX دينار ليبي لأي حادثة واحدة

(الملحق رقم 52)

البيان	يناير	فبراير	مارس	أبريل	مايو	يونيو	يوليو	أغسطس	سبتمبر	أكتوبر	نوفمبر	ديسمبر	الإجمالي	النسبة المئوية
عدد الأجهزة													0	#DIV/0!
عدد الحركات													0	#DIV/0!
قيمة الحركات													د.ل. 0.00	#DIV/0!
الإجمالي	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	د.ل. 0.00	

BOOK 2
Technical Legal
Standards

الكتاب 2
المعايير القانونية
الفنية

Regulatory Rules of The Libyan National Payment Scheme

BOOK 2 Technical Legal Standards Table of Contents

Chapter 1 Membership	447
1.1 Rules for Joining the Scheme	447
1.2 Membership	447
1.3 Eligibility to be a Member	447
1.4 Membership Types	447
1.5 New Members Joining the Network.....	449
1.5.1 Interim membership	449
1.5.2 Special Conditions of Membership, License or Activity	449
1.6 Membership Not Transferable	451
1.7 Right to Affiliate Additional Licensed Participant	451
1.8 Liabilities and Indemnifications	451
1.9 Scheme Members Responsibilities	451
1.10 Scheme Programs and Product Usage.....	453
1.11 License	453
1.12 Area of Use.....	453
1.13 Scheme Intellectual Property	453
1.14 Brand and Licensed Technology	455
1.15 Brand Usage	455
1.16 Rules Governing Members	455
1.17 Sponsorships/Partnerships	455
1.18 Definition: Bank Identification Number (BIN) Licensing	457
1.19 BIN License and Administration.....	457
1.20 BIN Licensing	457
1.21 Mergers and Acquisitions	457
1.22 Membership Status	457
1.23 BIN Licensee	457

القواعد التنظيمية لشبكة الدفع المحلية الليبية

الكتاب 2 المعايير القانونية الفنية جدول المحتويات

الفصل 1 - العضوية	446
1.1 قواعد الانضمام إلى الشبكة	446
2.1 العضوية	446
3.1 الأهلية المطلوبة للعضوية.....	446
4.1 أنواع العضوية	446
5.1 انضمام أعضاء جدد إلى الشبكة	448
1.5.1 العضوية المؤقتة.....	448
2.5.1 الشروط الخاصة بالعضوية أو الترخيص أو النشاط.....	448
6.1 العضوية غير قابلة للتنازل أو النقل	450
7.1 الحق في انضمام مشارك مرخص إضافي	450
8.1 المسؤوليات والتعويضات	450
9.1 مسؤوليات أعضاء الشبكة	450
10.1 برامج الشبكة واستخدام المنتج	452
11.1 الترخيص	452
12.1 مجال ونطاق الاستخدام	452
13.1 نظام الملكية الفكرية	452
14.1 العلامة التجارية، والتكنولوجيا المرخصة	454
15.1 استخدام العلامة التجارية	454
16.1 القواعد التي تحكم الأعضاء	454
17.1 الرعاية /الشراكات	454
18.1 التعريف: ترخيص رقم التعريف المصرفي.....	456
19.1 ترخيص وإدارة رقم التعريف المصرفي.....	456
20.1 ترخيص رقم التعريف المصرفي.....	456
21.1 عمليات الاندماج و عمليات الإستحواذ.....	456
22.1 حالة العضوية	456
23.1 مرخص رقم التعريف المصرفي	456

1.24 BIN Licensee – Responsibilities	457
1.25 BIN Use	459
1.26 Member Use of Scheme BINs	459
1.27 Merchant Use, Disclosure and Management of BIN Information	459
1.28 Use of Scheme-Owned EMV Technology	459
1.29 Software License	459
1.30 Ownership and Confidentiality	459
1.31 Non-Transferability without Prior Scheme Consent	461
1.32 Software Enhancements/Modifications	461
1.33 Suspension or Amendment of Membership Status	461
1.34 Termination of Membership	461
1.35 Rights, Liabilities, and Obligations of Terminated Principal Members	461
1.36 Participation in the Payment Scheme	465
1.36.1 Registration for Non-Issuing/Acquiring Activities	465
1.36.2 Card Production	465
1.36.3 Contracting with Card Registration Companies	467
1.36.4 Working with Vendors, Card Manufacturers and Personalization Bureaus	469
1.37 Types of Service Providers	469
1.37.1 Independent Sales Organization (ISO) Program Service	471
1.37.2 Third Party Processor (TPP) Program Service	471
1.37.3 Data Storage Entity (DSE) Program Service	471
1.37.4 Payment Service Provider (PSP) Program Service	471
1.37.5 Staged Digital Wallet Operator (SDWO) Program Service	479
1.37.6 Digital Activity Service Provider (DASP) Program Service	479
1.37.7 Token Service Provider (TSP)	479
1.37.8 Merchant Monitoring Program (MMS) Program Service	481
1.37.9 Terminal Servicer (TS) Program Service	481
1.37.10 3-D Secure Service Provider (3-DSSP) Program Service	481
1.38 Member Use of Service Providers	481
1.39 Confidential Information of Service Providers	481
1.40 Use of National Scheme Operator's Systems and Confidential Information	483
1.41 Other Service Providers (Non-Member)	483
1.42 Performing Program Service	485
1.43 Member Responsibility and Control	485
1.44 Notification to the National Scheme	485
1.45 Disclosure of Standards	487
1.46 Member Point of Contact	487

24.1 مرخص رقم التعريف المصرفي - المسؤوليات	456
25.1 استخدام رقم التعريف المصرفي	458
26.1 استخدام الأعضاء لنظام أرقام التعريف المصرفية	458
27.1 استخدام وكشف و إدارة التاجر لمعلومات رقم التعريف المصرفي	458
28.1 استخدام تقنية EMV المملوكة للشبكة	458
29.1 ترخيص البرنامج	458
30.1 الملكية والسرية	458
31.1 عدم قابلية التحويل دون الموافقة المسبقة للشبكة	460
32.1 تحسينات/تعديلات البرامج	460
33.1 تعليق أو تعديل حالة العضوية	460
34.1 إنهاء العضوية	460
35.1 حقوق ومسؤوليات والتزامات الأعضاء المسؤولين المنتهية عضويتهم	460
36.1 الاشتراك في شبكة الدفع	464
1.36.1 التسجيل في الأنشطة غير المصدرة/ القابلة	464
2.36.1 إنتاج البطاقة	464
3.36.1 التعاقد مع شركات تسجيل البطاقات	466
4.36.1 العمل مع البائعين، ومصنعي البطاقات ومكاتب التخصيص	468
37.1 أنواع مقدمي الخدمة	468
1.37.1 خدمة برنامج منظمة المبيعات المستقلة	470
2.37.1 خدمة برنامج معالج الطرف الثالث	470
3.37.1 خدمة برنامج كيان تخزين البيانات	470
4.37.1 خدمة برنامج مقدم خدمة الدفع	470
5.37.1 خدمة برنامج مشغل المحفظة الرقمية المرحلية	478
6.37.1 خدمة البرنامج مقدم خدمة النشاط الرقمي	478
7.37.1 مقدم خدمة الترميز	478
8.37.1 خدمة برنامج برنامج مراقبة التاجر	480
9.37.1 خدمة برنامج خدمة المحطة	480
10.37.1 خدمة برنامج مقدم الخدمة الآمنة ثلاثية الأبعاد	480
38.1 استخدام الأعضاء لمقدمي الخدمة	480
39.1 المعلومات السرية لمقدمي الخدمة	480
40.1 استخدام أنظمة مشغل شبكة الدفع المحلية والمعلومات السرية	482
41.1 مقدمو الخدمات الآخرون (غير الأعضاء)	482
42.1 أداء خدمة البرنامج	484
43.1 مسؤولية العضو والتحكم	484
44.1 إخطار الشبكة المحلية	484
45.1 الإفصاح عن المعايير	486
46.1 نقطة اتصال العضو	486

1.47 Use of the Brand	487
1.48 Service Provider Identification on a Card	489
1.49 Program Materials	489
1.50 Fees	489
1.51 Settlement Failure Obligation	489
1.52 Data Security	489
1.53 Access to Merchant Account	489
1.54 Acquiring Programs	491
1.55 Merchant Agreement	491
1.56 Collection of Funds from a Merchant	493
1.57 Access to Documentation	493
1.58 Authority to Terminate Merchant Agreement	493
1.59 Issuing Programs	493
1.60 Registration Requirements for Payment Service Providers	495
1.61 Registration Requirements for Token Service Providers	495
1.62 Audits	497
1.63 No Endorsement by the National Scheme Operator	497
Chapter 2 - NUMO Brand Usage	499
2.1 Right to Use National Scheme Brand "NUMO"	499
2.2 Brand Ownership, Reserving National Payment Scheme Rights	499
2.3 Registration of a Card Design	501
2.4 Misuse of the Brand	501
2.5 Use or register similar logos, designs and names	501
2.6 Terms and Conditions of Brand usage	503
2.7 Use of Multiple Logos	503
2.8 Particular Uses of the National Payment Scheme Logo	503
2.8.1 Generic Use	505
2.8.2 Use of Modifiers	505
2.8.3 Use on Stationery	505
2.8.4 Use of the National Payment Scheme Logo in Text	505
2.9 Use of Scheme Brand in Member Corporate Identity	505
2.10 Program Names	505
2.11 Use of Product Branding	505
2.12 Use of the National Payment Scheme Logo	507
2.13 Use of the National Payment Scheme Card Design in Cardholder Statement Enclosures	507
2.14 Usage of other Scheme Corporate Names (Non-Scheme Brand)	507
2.15 Scheme Corporate Identity	507
2.16 Primacy of Scheme Brand	507

47.1 استخدام العلامة التجارية	486
48.1 تحديد هوية مقدم الخدمة على البطاقة	488
49.1 مواد البرنامج	488
50.1 الرسوم	488
51.1 فشل التسوية	488
52.1 أمن البيانات	488
53.1 الوصول إلى حساب التاجر	488
54.1 قبول البرامج	490
55.1 عقد (اتفاقية) التاجر	490
56.1 تحصيل الأموال من التاجر	492
57.1 الوصول إلى الوثائق	492
58.1 سلطة إنهاء عقد (اتفاقية) التاجر	492
59.1 إصدار البرامج	492
60.1 متطلبات التسجيل لمقدمي خدمات الدفع	494
61.1 متطلبات التسجيل لمقدمي خدمة الترميز	494
62.1 عمليات التدقيق	496
63.1 عدم وجود مصادقة من قبل مشغل شبكة الدفع المحلية	496
الفصل 2 - استخدام علامة نمو التجارية	498
1.2 الحق في استخدام علامة شبكة الدفع المحلية نمو	498
2.2 ملكية العلامة التجارية، الاحتفاظ بحقوق شبكة الدفع المحلية	498
3.2 تسجيل تصميم البطاقة	500
4.2 إساءة استخدام العلامة التجارية	500
5.2 استخدام أو تسجيل شعارات وتصميمات وأسماء مماثلة	500
6.2 شروط وأحكام استخدام العلامة التجارية	502
7.2 استخدام شعارات (علامات) متعددة	502
8.2 الاستخدامات المعينة لشعار شبكة الدفع المحلية	502
1.8.2 الاستخدام العام	504
2.8.2 استخدام المعدلات	504
3.8.2 استخدام القرطاسية	504
4.8.2 استخدام شعار شبكة الدفع المحلية في النص	504
9.2 استخدام علامة الشبكة التجارية في هوية الشركة العضو	504
10.2 أسماء البرامج	504
11.2 استخدام العلامة التجارية للمنتج	504
12.2 استخدام شعار شبكة الدفع المحلية	506
13.2 استخدام تصميم بطاقة شبكة الدفع المحلية في مرفقات بيان حامل البطاقة	506
14.2 استخدام أسماء شركات الشبكة الأخرى (علامة تجارية غير نظامية)	506
15.2 هوية شركة النظام	506
16.2 أولوية العلامة التجارية للنظام	506

2.17 Use of Brand on Cards	507
2.18 Brand Positioning	507
2.19 General Card Design	507
2.20 Multiple Brands on Cards	507
2.21 Competitive Logos	507
2.22 Member Rights to Identification – General	509
2.23 Member Rights to Identification on Scheme Branded Products	509
2.24 Non-Member Brands on Cards	509
2.25 Co-Brand and Premium Card Program Requirements	509
2.26 High Value Consumer Segment Card Programs	509
2.27 Scheme Brand on Payment Devices	509
2.28 Card Acceptance at Point of Sale (POS) or Card Not Present (CNP)	509
2.29 ATM Network Program Logos	511
2.30 Card Acceptance at ATM	511
2.31 Card Acceptance in International Points of Acceptance	511
2.32 General Use of Scheme Brands for Promotional Purposes	511
2.33 Use of a Card Design in Issuer Advertising and Promotional Material	511
2.34 Use of a Card Design in Merchant Advertising and Signage	513
2.35 Brand Usage for Promotion and Advertising Activities	513
2.36 Member Sponsorships	513
2.37 Sponsorships Usage Requirements	513
Book 2 Chapter 3 – NUMO Products Guide	513
3.1 Introduction	513
3.1.1 Overview	513
3.1.2 Who Should Use This Book	513
3.2 Basic Requirements	515
3.3 NUMO Debit Cards	515
3.3.1 Product Construct – Features and Benefits	515
3.3.2 Technical Considerations	515
3.4 Prepaid Cards	517
3.4.1 Types of NUMO Prepaid Cards	517
3.4.2 Technical Considerations	517
3.4.3 Not-Personalized Prepaid Product Specific Requirements	519
3.4.4 Personalized Prepaid Product Requirements	521
3.4.5 Recommended Features – personalized Prepaid Products	521
3.4.6 Personalized Prepaid Product Types	521
3.5 General Implementation Considerations	525

17.2 استخدام العلامة التجارية على البطاقات	506
18.2 وضع العلامة التجارية	506
19.2 تصميم البطاقة العام	506
20.2 علامات تجارية متعددة على البطاقات	506
21.2 الشعارات التنافسية	506
22.2 حقوق الأعضاء في التحديد – عام	508
23.2 حقوق الأعضاء في التحديد على المنتجات ذات علامة النظام التجارية	508
24.2 العلامات التجارية غير الأعضاء على البطاقات	508
25.2 متطلبات برنامج العلامة التجارية المشتركة والبطاقة المميزة	508
26.2 برامج بطاقة شريحة المستهلك عالية القيمة	508
27.2 العلامة التجارية للنظام على أجهزة الدفع	508
28.2 قبول البطاقة في نقاط البيع أو البطاقة غير الموجودة	508
29.2 شعارات برنامج شبكة أجهزة الصراف الآلي	510
30.2 قبول البطاقة في أجهزة الصراف الآلي	510
31.2 قبول البطاقة في نقاط القبول الدولية	510
32.2 الاستخدام العام لعلامات النظام التجارية للأغراض الترويجية	510
33.2 استخدام تصميم البطاقة في إعلانات جهة الإصدار والمواد الترويجية	510
34.2 استخدام تصميم البطاقة في إعلانات التاجر واللافقات	512
35.2 استخدام العلامة التجارية للأنشطة الترويج والإعلان	512
36.2 رعاية الأعضاء	512
37.2 متطلبات استخدام الرعاية	512
الفصل 3 - دليل منتجات نمو	512
1.3 مقدمة	512
1.1.3 نظرة عامة	512
2.1.3 من يجب أن يستخدم هذا الكتاب	512
2.3 المتطلبات الأساسية	514
3.3 بطاقات خصم نمو	514
1.3.3 تكوين المنتج - الميزات والفوائد	514
2.3.3 الاعتبارات الفنية	514
4.3 البطاقات مسبقة الدفع	516
1.4.3 أنواع بطاقات نمو مسبقة الدفع	516
2.4.3 الاعتبارات الفنية	516
3.4.3 المتطلبات المحددة لمنتج مسبق الدفع غير المخصصة	518
4.4.3 متطلبات منتجات الدفع المسبق المخصصة	520
5.4.3 الميزات الموصى بها - منتجات الدفع المسبق المخصصة	520
6.4.3 أنواع منتجات الدفع المسبق المخصصة	520
5.3 اعتبارات التنفيذ العامة	524

3.5.1 Guidelines to Issuers 525

3.5.2 Guidelines to Acquirers 525

Appendix number (1) 527

Appendix number (2) 527

Appendix number (3) 527

Appendix number (4) 529

Appendix number (5) 529

Appendix number (6) 529

Appendix number (7) 531

Appendix number (8) 531

1.5.3 إرشادات لجهات الإصدار 524

2.5.3 إرشادات للقبولين 524

الملحق رقم (1) 526

الملحق رقم (2) 526

الملحق رقم (3) 526

الملحق رقم (4) 528

الملحق رقم (5) 528

الملحق رقم (6) 528

الملحق رقم (7) 530

الملحق رقم (8) 530

Chapter 1 Membership

1.1 Rules for Joining the Scheme

This Chapter intended to be the reference and the rule book for the entities that shows interest in joining the National Scheme and to be a part of Libya Domestic Scheme.

1.2 Membership

(Category A as referenced in Book 1 Chapter 1)

An eligible entity that has the right to apply for Membership to become a Member of Libya National Payment Scheme.

No entity is permitted to participate in a payment Activity until that entity is approved to be a Member, and has executed the applicable certification for the proposed payment Activity in a form acceptable to the National Scheme Operator, and has paid all associated fees and other costs according to the preset charges and fees.

1.3 Eligibility to be a Member

(Category A as referenced in Book 1 Chapter 1)

A licensed financial institution or other legal entity authorized to engage in financial transactions through CBL and in accordance with the laws and government regulations of Libya is eligible to be a Member.

Any such financial institution or other legal entity must also have the requisite right, power, and authority, to be a Member and to engage in the proposed Activity.

For purposes of this Rule, “financial transactions” means the making of commercial or consumer payments, the taking of consumer or commercial deposits, the establishment of prepaid accounts and issuance of electronic money or stored value, or the execution of related payment transactions, including effecting such transactions with payment cards or other payment devices or methods. A financial institution applicant is regulated and supervised by the CBL and governmental authorities.

The decision to admit an applicant as a Principal or Participant is made in the sole discretion of the CBL.

1.4 Membership Types

The types of Member are Principal and Participant.

- A Principal participates directly in issuing or acquiring Activity. A Principal has the right to sponsor Participants provided that the approval of the National Scheme Operator is obtained.

Only Banks have the right to be Principal Members

- A Participant participates indirectly in issuing or acquiring Activity via its Sponsoring Principal, usually defined as a Payment Service Provider.

الفصل 1 - العضوية

1.1 قواعد الانضمام إلى الشبكة

يهدف هذا الفصل إلى أن يكون المرجع ودليل القواعد للجهات التي ترغب في الانضمام إلى الشبكة المحلية، وأن تكون جزءًا من الشبكة المحلية الليبية.

2.1 العضوية

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يكون للجهة المؤهلة الحق في التقدم بطلب الحصول على العضوية، لتكون عضوًا في برنامج شبكة الدفع المحلية الليبية.

ولا يُسمح للجهة بالمشاركة في نشاط الدفع، إلا بعد حصولها على الموافقة، وقيامها بتنفيذ الشهادة المعمول بها لنشاط الدفع المقترح في شكل مقبول من قبل مشغل شبكة الدفع المحلية، إضافة إلى قيامها بسداد جميع الرسوم المحددة مسبقًا، والتكاليف الأخرى، المتعلقة بممارسة هذا النشاط.

3.1 الأهلية المطلوبة للعضوية

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

تكون مؤهلة للحصول على العضوية، كل مؤسسة مالية مرخصة، أو جهة اعتبارية أخرى مرخص لها بالمشاركة في المعاملات المالية من خلال مصرف ليبيا المركزي ووفقًا للقوانين واللوائح المعمول بها في ليبيا.

يجب أن تتمتع المؤسسة المالية أو الجهة الاعتبارية الأخرى، بالتفويض، والتنظيم، والسلطة المطلوبة لتكون عضوًا والمشاركة في النشاط المقترح.

لأغراض تطبيق هذه القاعدة، تعني “المعاملات المالية” إجراء مدفوعات تجارية أو استهلاكية، أو أخذ ودائع استهلاكية أو تجارية، أو إنشاء حسابات الدفع المسبق، وإصدار نقود إلكترونية أو قيمة مخزنة، أو تنفيذ معاملات الدفع ذات الصلة، بما في ذلك إجراء مثل هذه المعاملات باستخدام بطاقات الدفع أو وسائل الدفع الأخرى. ويخضع مقدم الطلب من المؤسسة المالية للتنظيم والإشراف من قبل مصرف ليبيا المركزي والسلطات الحكومية.

ويتم اتخاذ قرار قبول مقدم الطلب كمسؤول أو مشارك وفقًا للسلطة التقديرية لمصرف ليبيا المركزي.

4.1 أنواع العضوية

تنقسم أنواع العضوية إلى نوعين هما: العضو المسؤول، والعضو المشارك.

- يشارك العضو المسؤول مباشرة في نشاط الإصدار والقبول. يحق له كفالة/رعاية المشاركين بشرط الحصول على موافقة مشغل شبكة الدفع المحلية. ويشترط في العضو المسؤول أن يكون مصرفاً.
- يشارك العضو المشارك بشكل غير مباشر في إصدار أو الحصول على نشاط عبر مسؤوله الراعي، والذي يُعرف عادةً باسم مقدم خدمة الدفع.

1.5 New Members Joining the Network

(Category A as referenced in Book 1 Chapter 1)

This section contains Rules that apply specifically to new Members in connection with joining the payment scheme.

1.5.1 Interim membership

Pending approval of an application to be a Member, the National Scheme has the right but not the obligation to authorize the applicant to participate in Activity on an interim basis as if the applicant were a Member. As a condition of such interim authorization, the applicant must agree, and by commencement of any Activity the applicant is deemed to have agreed, to comply during this interim period (and thereafter as applicable) with the Standards and to discontinue immediately any use of the Brand and Activity if the application to be a Member is declined.

All damages, losses, costs, and liabilities arising directly or indirectly, or consequentially, from or related to any interim participation in Activity by the applicant and from the disapproval of the application to be a Member is solely at the applicant's risk and expense, and the National Scheme has no responsibility for any such damages, losses, costs, or liabilities.

1.5.2 Special Conditions of Membership, License or Activity

The CBL has the right to condition membership, the grant of any License, or the conduct of Activity on compliance by the Member with special conditions, such as the establishment of escrow arrangements, the delivery of letters of credit, or other arrangements that the CBL deems necessary or appropriate to maintain the integrity of the payment scheme and/or the Interchange System, including but not limited to conditions imposed pursuant to anti-money laundering and sanctions requirements.

The CBL within his authority has the right at any time to require that a Member enter into a security arrangement with the National Scheme. If a Member does not enter into a security arrangement with the National Scheme that is satisfactory to the National Scheme, the CBL has the right at any time to collect from the Member, in addition to any amount otherwise due and payable by the Member to the National Scheme or to other Members, such additional amount from the Member as collateral as the CBL deems appropriate. The CBL has the right to collect any such additional amount by any means available to the National Scheme including by way of example and not limitation:

1. By taking any funds deposited by any persons from any account that the National Scheme is authorized to draw upon for any purpose.
2. By taking any funds due to such Member from other Members.
3. By taking any funds being paid by such Member to other Members.

In each case in which the National Scheme takes any such collateral, the CBL has the right to take ownership of all or any part of such collateral (such as by placing funds taken in an account in the National Scheme Operator's name as a secured party) and to apply such collateral as payment toward any obligation of the Member in accordance with the Standards.

5.1 انضمام أعضاء جدد إلى الشبكة

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يحتوي هذا القسم على القواعد التي تنطبق بشكل خاص على الأعضاء الجدد فيما يتعلق بالانضمام إلى شبكة الدفع.

1.5.1 العضوية المؤقتة

إلى حين الحصول على الموافقة على طلب العضوية، يجوز لمشغل شبكة الدفع المحلية منح تفويض مؤقت لمقدم الطلب للمشاركة في النشاط، كما لو كان مقدم الطلب عضوًا. ويشترط للحصول على التفويض المؤقت، موافقة مقدم الطلب، وتعتبر بداية ممارسة النشاط موافقة ضمنية منه على قبول التفويض المؤقت، ويجب عليه الامتثال خلال هذه الفترة المؤقتة (وبعد ذلك حسب الاقتضاء) للمعايير والتوقف فورًا عن أي استخدام للعلامة التجارية والنشاط إذا تم رفض طلب العضوية.

يتحمل مقدم الطلب المسؤولية عن جميع الأضرار والخسائر والتكاليف الناشئة بشكل مباشر أو غير مباشر، والتي قد تتحقق نتيجة المشاركة المؤقتة في النشاط من قبل مقدم الطلب، أو من رفض الطلب، ولا يتحمل مشغل شبكة الدفع المحلية أي مسؤولية عن أي أضرار أو خسائر أو تكاليف أو التزامات.

2.5.1 الشروط الخاصة بالعضوية أو الترخيص أو النشاط

لمصرف ليبيا المركزي أن يشترط للحصول على العضوية أو منح الترخيص أو إجراء النشاط امتثال العضو لشروط خاصة، مثل وضع ترتيبات الضمان، أو تسليم خطابات الاعتماد، أو الترتيبات الأخرى التي يفرضها مصرف ليبيا المركزي تعتبر ضرورية أو مناسبة للحفاظ على سلامة شبكة الدفع و/أو نظام التبادل، بما في ذلك على سبيل المثال لا الحصر الشروط المفروضة وفقًا لمتطلبات مكافحة غسيل الأموال والعقوبات.

لمصرف ليبيا المركزي في نطاق اختصاصه وفي أي وقت أن يطلب من العضو الدخول في ترتيب أمني مع مشغل شبكة الدفع المحلية. وإذا لم يقيم العضو بالدخول في ترتيب أمني مع مشغل شبكة الدفع المحلية، كان لمصرف ليبيا المركزي في أي وقت تحصيل مبلغ من العضو، بالإضافة إلى استرداد المبلغ مستحق الدفع من قبل العضو إلى مشغل شبكة الدفع المحلية أو للأعضاء الآخرين، وقد يمثل هذا المبلغ الإضافي من العضو ضماناً مناسباً حسبما يراه مصرف ليبيا المركزي. ويملك مصرف ليبيا المركزي تحصيل أي مبلغ إضافي من هذا القبيل بأي وسيلة متاحة للشبكة المحلية بما في ذلك على سبيل المثال وليس الحصر:

1. أخذ الأموال المودعة من قبل أي شخص من أي حساب تصرح الشبكة المحلية بالاستفادة منه لأي غرض من الأغراض.
2. أخذ الأموال المستحقة لهذا العضو من أعضاء آخرين.
3. أخذ الأموال التي يدفعها هذا العضو إلى أعضاء آخرين.

في كل حالة يحصل فيها مشغل شبكة الدفع المحلية على ضمانات، فإن لمصرف ليبيا المركزي الحصول على ملكية كل أو جزء من هذه الضمانات (مثل وضع الأموال في حساب باسم مشغل شبكة الدفع المحلية كطرف مضمون) وتطبيق مثل هذه الضمانات كمبلغ مقابل أي التزام على العضو وفقاً للمعايير.

Each Member hereby appoints and authorizes the National Scheme to act as the Member's attorney and Service Provider for any and all purposes in connection with the filing, recording, or other perfecting of the National Scheme's rights under the Standards. This Rule constitutes a security agreement between each Member and the National Scheme, and vests in the National Scheme a security interest in any collateral collected as provided in these Standards, granted in exchange and as a condition for the continuation of the Member's membership and Licenses.

1.6 Membership Not Transferable

(Category A as referenced in Book 1 Chapter 1)

A Member must not transfer or assign its membership or any License, whether by sale, consolidation, merger, operation of law, or otherwise, without the written consent of the CBL. However, in the event that the Cards issued by, the Ownership of, or any Activity of a Member are acquired by any person, whether by sale, consolidation, merger, operation of law or otherwise, the obligations, but not the rights, of such Member shall transfer to the person acquiring such Member.

1.7 Right to Affiliate Additional Licensed Participant

(Category A as referenced in Book 1 Chapter 1)

A Principal has the right to affiliate an eligible Participant Member, subject to notifying the National Scheme.

1.8 Liabilities and Indemnifications

Same rules been set forth in Book 1 Organization Principals article 2.9 are applied here in addition to the following

1. Not abiding the Fraud and Risk rules that been stated and provided in Book 1 Chapter 6 Fraud and Risk Management, in addition to early preset rules by CBL for AML/CFT
2. Members are totally obliged to maintain a system whereby it can cater for potential operational losses and to make the right provisioning for such potentials.
3. The National Scheme Operator's interpretation, enforcement, or failure to enforce any Standards.

In no event will the national scheme operator be liable for any indirect, incidental, special or consequential damages, for loss of profits, or any other cost or expense incurred by a member or any third party arising from or related to use or receipt of the systems, whether in an action in contract or in tort, and even if the member or any third party has been advised of the possibility of such damages. Each member assumes the entire risk of use or receipt of the systems.

1.9 Scheme Members Responsibilities

(Category A as referenced in Book 1 Chapter 1)

Members have the following responsibilities:

1. Accept and present to the Issuer records of Transactions arising from the use of a Card issued by any other Member at any POI location the Member has authorized to honor Cards;
2. Accept and pay for Transactions received from another Member arising from the use of any Card issued by it. If a Participant ceases to be an affiliate to a Principal, the Principal

يعين كل عضو، لمشغل شبكة الدفع المحلية ويفوضه للعمل، كمحامي العضو ومقدم الخدمة لجميع الأغراض، فيما يتعلق بالإيداع، أو التسجيل أو تحسين حقوق مشغل شبكة الدفع المحلية بموجب المعايير. تشكل هذه القاعدة اتفاقية أمنية بين كل عضو ومشغل شبكة الدفع المحلية، وتعطي لمشغل شبكة الدفع المحلية مصلحة أمنية في أي ضمانات يتم جمعها على النحو المنصوص عليه في هذه المعايير، الممنوحة بالمقابل وكشرط لاستمرار عضوية العضو وتراخيصه.

6.1 العضوية غير قابلة للتنازل أو النقل

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على العضو عدم نقل أو التنازل عن عضويته أو أي ترخيص، سواء عن طريق البيع أو الدمج أو الاندماج أو تطبيق القانون أو غير ذلك، دون الحصول على موافقة مكتوبة من مصرف ليبيا المركزي. ومع ذلك، وفي حالة حصول أي شخص على البطاقات الصادرة لأي عضو آخر أو ملكيتها، أو نشاط ذلك العضو، سواء عن طريق البيع أو الدمج أو الاندماج أو تطبيق القانون أو غير ذلك، فإن إلتزامات العضو الأول.

7.1 الحق في انضمام مشترك مرخص إضافي

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يحق للمسؤول ضم عضو مشترك مؤهل، بشرط إخطار مشغل شبكة الدفع المحلية.

8.1 المسؤوليات والتعويضات

تنطبق نفس القواعد في المادة 2.9 من الكتاب الأول للمبادئ التنظيمية بالإضافة إلى التالي:

1. عدم الالتزام بقواعد الاحتيال والمخاطر التي تم ذكرها في الكتاب الأول، الفصل السادس (إدارة الاحتيال والمخاطر)، بالإضافة إلى القواعد المحددة مسبقًا من قبل مصرف ليبيا المركزي لمكافحة غسيل الأموال، وتمويل الإرهاب.
 2. يلتزم الأعضاء بالحفاظ على نظام يمكنهم من خلاله مواجهة الخسائر التشغيلية المحتملة وتوفير المخصصات المناسبة لذلك.
 3. تفسير مشغل شبكة الدفع المحلية أو تطبيقه أو إخفاقه في تطبيق أي معايير.
- لا يعد مشغل شبكة الدفع المحلية مسؤولاً بأي حال من الأحوال عن الأضرار غير المباشرة أو العارضة أو التبعية، الناتجة عن خسارة الأرباح، أو أي تكاليف أخرى أو المصاريف التي تكبدها عضو أو طرف ثالث، وكانت ناشئة عن أو مرتبطة باستخدام أو استلام الأنظمة، سواء في دعوى بموجب عقد أو ضرر، وحتى إذا تم إخطار العضو أو الطرف الثالث بإمكانية حدوث مثل هذه الأضرار. يتحمل كل عضو المسؤولية الكاملة عن مخاطر استخدام أو استلام الأنظمة.

9.1 مسؤوليات أعضاء الشبكة

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يتحمل الأعضاء المسؤوليات التالية:

1. قبول وتقديم سجلات المعاملات الناشئة عن استخدام بطاقة صادرة عن العضو الآخر إلى جهة الإصدار في أي موقع من مواقع نقاط التفعيل التي خولها العضو لقبول البطاقات.
2. قبول ودفع المعاملات المستلمة من عضو آخر الناشئة عن استخدام البطاقات الصادرة عنه. وإذا

- remains obligated to other Members to accept and pay for Transactions arising from the use of Cards issued by that Participant;
3. Maintain a functional 24-hour-per-day operating connection to the Interchange System, either directly or by means of a Service Provider operating on its behalf, and use that operating connection for the processing of Transactions.
 4. Provide valid, accurate, complete, unaltered, and consistent data in all authorization and clearing Transaction messages.

A Member must not directly or indirectly engage in or facilitate any action that is illegal or that, in the opinion of the CBL and whether or not addressed elsewhere in the Standards, damages or may damage the goodwill or reputation of the National Scheme or of the Brand. Upon request of the National Scheme, a Member must promptly cease engaging in or facilitating any such action.

In addition, a Member must not place or cause to be placed on any Card or any Terminal or other acceptance device any image, information, application or product that would in any way, directly or indirectly, have or potentially have the effect of diminishing or devaluing the reputation or utility of the Brand, a Card, or any of the National Scheme's products, programs, services, networks, or systems.

1.10 Scheme Programs and Product Usage

The National Scheme Operator reserves the right to control the nature and quality of the programs and products associated with the Brand.

1.11 License

(Category A as referenced in Book 1 Chapter 1)

Each Member agrees, and by use of the Brand agrees, to comply with all provisions of the License pertaining to use of the Brand and with the Standards in effect from time to time.

In the event of an inconsistency between a Standard and a provision in a License, the Standard prevails, and the License is deemed to be amended so as to be consistent with the Standard.

Each Member must assist the National Scheme in recording any License granted to the Member if required or upon request of the National Scheme Operator.

1.12 Area of Use

(Category A as referenced in Book 1 Chapter 1)

The area of use of the NUMO License is Libya. It maybe used outside of Libya subject to CBL directions.

1.13 Scheme Intellectual Property

Scheme intellectual property comprises the Brand and the systems, tools and technology which support the functioning of the payment scheme.

- توقف العضو المشارك عن كونه تابعًا لأحد المسؤولين، يظل العضو المسؤول ملزمًا تجاه الأعضاء الآخرين بقبول ودفع المعاملات الناشئة عن استخدام البطاقات الصادرة عن ذلك العضو المشارك.
3. الحفاظ على اتصال وتشغيل فعال على مدار 24 ساعة في اليوم بنظام التبادل، إما بشكل مباشر أو عن طريق مقدم خدمة يعمل نيابة عنه، واستخدام اتصال التشغيل هذا لمعالجة المعاملات.
 4. توفير بيانات صحيحة، ودقيقة وكاملة وغير معدلة ومتسقة في جميع رسائل التفويض والمقاصة الخاصة بالمعاملات.

يجب على العضو عدم القيام بشكل مباشر أو غير مباشر، أو تسهيل أي إجراء غير قانوني، من شأنه، في تقدير مصرف ليبيا المركزي، وسواء تم تحديد ذلك في المعايير أو لم يتم تحديده، أن يلحق الضرر أو قد يضر بسمعة مشغل شبكة الدفع المحلية أو العلامة التجارية. وبناءً على طلب مشغل شبكة الدفع المحلية، يجب على العضو التوقف فوراً عن المشاركة في أي إجراء من هذا القبيل أو تسهيله.

بالإضافة إلى ذلك، يجب على العضو عدم وضع، أو التسبب في وضع، أي صورة أو معلومات أو تطبيق أو منتج على البطاقة أو المحطة أو أي جهاز قبول آخر، قد يكون له بأي شكل من الأشكال، بطريق مباشر أو غير مباشر، أو يحتمل أن يكون له تأثير التقليل من قيمة سمعة أو منفعة العلامة التجارية أو البطاقة أو أي من منتجات أو برامج أو خدمات أو شبكات أو أنظمة مشغل شبكة الدفع المحلية.

10.1 برامج الشبكة واستخدام المنتج

يحتفظ مشغل شبكة الدفع المحلية بالحق في التحكم في طبيعة وجودة البرامج والمنتجات المرتبطة بالعلامة التجارية.

11.1 الترخيص

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على كل عضو يقوم باستخدام العلامة التجارية، الموافقة على الامتثال لجميع أحكام الترخيص المتعلقة باستخدام العلامة التجارية والمعايير السارية من وقت لآخر.

وفي حالة وجود تضارب بين معيار، وأحد أحكام الترخيص، تكون الأسبقية في التطبيق للمعيار، ويُعتبر حكم الترخيص معدلاً بحيث يتوافق مع المعيار.

يجب على كل عضو مساعدة مشغل شبكة الدفع المحلية في تسجيل الترخيص الممنوح للعضو إذا لزم الأمر، أو بناءً على طلب مشغل شبكة الدفع المحلية.

12.1 مجال ونطاق الاستخدام

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

مجال استخدام بطاقة نمو هي دولة ليبيا. وقد يتم استخدامها خارج ليبيا وفقاً لتوجيهات مصرف ليبيا المركزي.

13.1 نظام الملكية الفكرية

تتألف الملكية الفكرية للنظام من العلامة التجارية، والأنظمة والأدوات والتكنولوجيا التي تدعم عمل شبكة الدفع.

1.14 Brand and Licensed Technology

(Category A as referenced in Book 1 Chapter 1)

Each Member and each of its Service Providers acknowledges that the National Scheme is the exclusive owner and/or licensor of the Brand and the licensed technology, and agrees not to contest or assist others, either directly or indirectly, in contesting the National Scheme's sole ownership of the Brand and licensed technology, or otherwise take or fail to alert the National Scheme of any action that would be inconsistent with that ownership. All use of the Brand and licensed technology will insure solely to the benefit of the National Scheme.

No Member, Licensee or Service Provider has the right to register, attempt to register or in any way make use of a Brand, or any Logo or term that, in the opinion of the National Scheme, is deemed to be derivative of, similar to, or in any way related to the Brand. In particular, no use of a Brand is permitted on or in connection with any card, device or other application associated with a payment service that the National Scheme deems to be competitive with any Activity.

Without limitation, the foregoing shall apply to the registration or use of any Brand or term that incorporates, references or otherwise could be confused or associated with a Brand currently or previously Licensed, sublicensed, or otherwise used by a Member, the Member's permittees, and their respective successors or assignees (including, without limitation, by means of acquisition by merger or otherwise, bankruptcy or voluntary or involuntary winding-up).

If a Member is threatened with litigation or is sued with regard to any matter relating to use of the Brand or licensed technology, the Member must immediately notify the National Scheme in writing. The National Scheme, in its discretion, has the right to then defend, settle, or consent to the entry of a judicial order, judgment or decree that would terminate any such litigation, or permit such Member to do so.

1.15 Brand Usage

An applicant that is approved to become a Principal Member receives a Permission to use the NUMO brand in connection with its Card issuing and/or acquiring Activities.

The Member must use the Brand License only for the purpose of engaging in Payment Activity.

1.16 Rules Governing Members

(Category A as referenced in Book 1 Chapter 1)

The Rules apply compulsory to all Members (Principals and Participants).

1.17 Sponsorships/Partnerships

(Category A as referenced in Book 1 Chapter 1)

The National Scheme has the sole right to decide whether to permit the use of the Brand pursuant to any sponsorship or partnership agreement.

14.1 العلامة التجارية، والتكنولوجيا المرخصة

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يقر كل عضو وكل مقدمي الخدمة التابعين له، بأن مشغل شبكة الدفع المحلية هو المالك الحصري و/ أو المرخص للعلامة التجارية والتكنولوجيا المرخصة، (مع مراعاة حقوق الملكية الفكرية التي تنظمها القوانين) ويوافق على عدم المنافسة أو مساعدة الآخرين، سواء بشكل مباشر أو غير مباشر، في الطعن في الملكية الفردية لمشغل شبكة الدفع المحلية للعلامة التجارية والتكنولوجيا المرخصة، أو يتخذ أو يقصر في تنبيه مشغل شبكة الدفع المحلية بأي إجراء قد يتعارض مع تلك الملكية. جميع استخدامات العلامة التجارية والتكنولوجيا المرخصة ستؤمن فقط لصالح مشغل شبكة الدفع المحلية.

لا يجوز لأي عضو أو مرخص له أو مقدم خدمة، التسجيل أو محاولة التسجيل أو استخدام أي علامة تجارية بأي شكل من الأشكال أو أي شعار أو مصطلح يعتبر، في تقدير مشغل شبكة الدفع المحلية، مشتقًا، أو مشابهًا أو مرتبط بأي شكل من الأشكال بالعلامة التجارية. وعلى وجه الخصوص، لا يُسمح باستخدام أي علامة تجارية على، أو فيما يتعلق بأي بطاقة أو جهاز أو تطبيق آخر مرتبط بخدمة الدفع التي يعتبرها مشغل شبكة الدفع المحلية منافسة لنشاطه.

على وجه الإطلاق، تسري هذه القاعدة، على كل تسجيل أو استخدام أي علامة تجارية أو مصطلح يتضمن، أو يشير، أو خلًا لذلك، قد يحدث الخلط بينه أو ربطه بعلامة تجارية مُرخصة حاليًا أو مُرخصة سابقًا أو مُرخصة من الباطن أو مستخدمة بطريقة أخرى من قبل العضو، وتصاريح الأعضاء، و خلفائهم أو المتنازل لهم عنهم (بما في ذلك، على سبيل المثال لا الحصر، عن طريق القبول أو عن طريق الاندماج أو غير ذلك، الإفلاس أو التصفية الطوعية أو غير الطوعية).

إذا تعرض العضو لاحتمال مقاضاته، أو تمت مقاضاته فيما يتعلق بأي مسألة تتعلق باستخدام العلامة التجارية أو التكنولوجيا المرخصة، فيجب على العضو إخطار مشغل شبكة الدفع المحلية على الفور بذلك كتابيًا. يحق لمشغل شبكة الدفع المحلية، ووفقًا لتقديره، الدخول في الدعوى، أو طلب تسوية المنازعة بالطرق الودية، أو الموافقة على إدخال أمر قضائي أو حكم أو مرسوم من شأنه إنهاء أي من هذه الدعاوى القضائية أو السماح لهذا العضو بالقيام بذلك.

15.1 استخدام العلامة التجارية

يتلقى مقدم الطلب الذي تمت الموافقة عليه ليصبح عضوًا مسؤولًا إذنا باستخدام العلامة التجارية نمو فيما يتعلق بإصدار البطاقة و/أو اكتساب الأنشطة.

يجب على العضو استخدام ترخيص العلامة التجارية فقط لغرض المشاركة في نشاط الدفع.

16.1 القواعد التي تحكم الأعضاء

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

تطبق القواعد بشكل إلزامي على جميع الأعضاء (المسؤولين والمشاركين).

17.1 الرعاية /الشراكات

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

لمشغل شبكة الدفع المحلية وحده الحق في ترخيص السماح باستخدام العلامة التجارية وفقًا لعقود الرعاية أو الشراكة.

1.18 Definition: Bank Identification Number (BIN) Licensing

A Bank identification number (BIN) is a unique number assigned for use by an Issuer in connection with the issuance of Cards.

1.19 BIN License and Administration

The Brand License includes a License for a BIN. The National Scheme administers the BIN assignments.

An Issuer is permitted to receive additional BINs upon payment of the corresponding fee.

1.20 BIN Licensing

The National Scheme handles all aspects of BIN Licensing.

1.21 Mergers and Acquisitions

(Category A as referenced in Book 1 Chapter 1)

In the case of a planned merger or acquisition affecting a Member, the National Scheme Operator must be informed thereof at least 30 days before the effective date of the merger or acquisition.

A Member must promptly provide the National Scheme Operator any information requested by the National Scheme Operator relating to such an event or proposed event.

The National Scheme has the right to take any of the following actions:

1. Suspend or impose conditions on any Permissions granted to the Member.
2. Amend rights, obligations, or both of a Member.

CBL has the right to terminate the Licenses of any Member that:

- a. Transfers or attempts to transfer Control of the Member to an entity that is not a Member or
- b. Merges into or is consolidated with an entity that is not a Member; or
- c. Sells all or substantially all of its assets; or
- d. Sells all or substantially all of its Issuer or Acquirer Portfolios; or
- e. Experiences a change in Control or Ownership.

1.22 Membership Status

Each BIN Licensee must be a Principal Member.

1.23 BIN Licensee

A Principal Member that has received a BIN is a BIN Licensee.

1.24 BIN Licensee - Responsibilities

(Category A as referenced in Book 1 Chapter 1)

The BIN Licensee is responsible to the National Scheme Operator and to all other Members for Transactions arising from the use of the BINs that the National Scheme Operator assigned to it, and for any Cards that the BIN Licensee has issued. The BIN Licensee is also responsible for the Cards issued by any of its Affiliated Participants.

18.1 التعريف: ترخيص رقم التعريف المصرفي

رقم التعريف المصرفي هو رقم مميز، يتم تعيينه للاستخدام من قبل جهة الإصدار فيما يتعلق بإصدار البطاقات.

19.1 ترخيص وإدارة رقم التعريف المصرفي

يتضمن ترخيص العلامة التجارية، ترخيصًا لرقم التعريف المصرفي. ويدير مشغل شبكة الدفع المحلية تعيينات رقم التعريف المصرفي.

يُسمح لجهة الإصدار باستلام أرقام تعريف إضافية عند دفع الرسوم المقابلة.

20.1 ترخيص رقم التعريف المصرفي

يعالج مشغل شبكة الدفع المحلية جميع جوانب ترخيص رقم التعريف المصرفي.

21.1 عمليات الاندماج و عمليات الإستحواذ

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

في حالة الاندماج أو الإستحواذ المخطط له والذي قد يؤثر على أحد الأعضاء، يجب إخطار مشغل شبكة الدفع المحلية بذلك قبل 30 يومًا على الأقل من تاريخ حصول الاندماج أو الإستحواذ.

يجب على العضو تزويد مشغل شبكة الدفع المحلية على الفور بالمعلومات التي يطلبها مشغل شبكة الدفع المحلية فيما يتعلق بحالة الإندماج أو الإستحواذ.

لمشغل شبكة الدفع المحلية اتخاذ أي من الإجراءات التالية:

1. تعليق، أو فرض شروط على أي أذونات ممنوحة للعضو.
2. تعديل حقوق أو التزامات العضو، أو كليهما.

ولمصرف ليبيا المركزي سلطة إنهاء تراخيص العضو، في الحالات التالية:

- أ. نقل أو محاولة نقل التحكم في العضو إلى جهة ليست عضوًا.
- ب. عندما يندمج في جهة ليست عضوًا أو يتم دمج معها.
- ت. عندما يبيع جميع أصوله أو معظمها.
- ث. عندما يبيع كل أو معظم محافظ جهة الإصدار أو القابل.
- ج. يقع تغيير في الجهة المسيطرة عليه أو المالكة له .

22.1 حالة العضوية

يجب أن يكون كل مرخص رقم تعريف مصرفي عضوًا مسؤولًا.

23.1 مرخص رقم التعريف المصرفي

العضو المسؤول الذي حصل على رقم تعريف مصرفي، هو مرخص رقم التعريف المصرفي.

24.1 مرخص رقم التعريف المصرفي - المسؤوليات

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يكون مرخص رقم التعريف المصرفي مسؤولًا أمام مشغل شبكة الدفع المحلية، وتجاه جميع الأعضاء الآخرين، عن جميع المعاملات الناشئة عن استخدام أرقام التعريف المصرفية التي عينها له مشغل شبكة الدفع المحلية، وعن البطاقات التي أصدرها مرخص رقم التعريف المصرفي. ويكون مرخص رقم التعريف المصرفي مسؤول أيضًا عن البطاقات الصادرة عن المسؤولين التابعين له.

1.25 BIN Use

(Category A as referenced in Book 1 Chapter 1)

Each Member must use BINs only in accordance with the Standards and for the purposes of Card issuing activities.

Neither a principal nor any of its affiliated Participants has the right to use BINs in any manner other than as specified by the National Scheme.

1.26 Member Use of Scheme BINs

(Category A as referenced in Book 1 Chapter 1)

The National Scheme Operator has the right to assign a Member one or more BINs.

Use of a BIN must not be sublicensed or re-assigned or otherwise transferred.

The National Scheme Operator has the right to:

- Review a Member’s BIN usage for compliance with the Standards; and
- Retract the assignment of any BIN that has been assigned to a Member for a proper reason.

1.27 Merchant Use, Disclosure and Management of BIN Information

(Category A as referenced in Book 1 Chapter 1)

A Merchant must not use or in any manner disclose BIN or Account data to anyone other than its Acquirer, to the National Scheme, or in response to a valid government demand. This prohibition applies to BIN or Account data contained in Card imprints, carbon copies, Transaction receipts, mailing lists, tapes, database files, and all other media created or obtained as a result of a Transaction.

A Merchant must treat BIN and Account data with the same care as it accords to its own confidential data.

1.28 Use of Scheme-Owned EMV Technology

The License also includes the right for the Member to use any EMV technology specified and owned by the National Scheme.

1.29 Software License

Each Member receives a non-exclusive, limited, non-transferable, non-sublicensable license to use the software of the National Scheme Operator solely for the purpose of operating its Card issuing and/or acquiring program.

1.30 Ownership and Confidentiality

(Category A as referenced in Book 1 Chapter 1)

The Member acknowledges the sole ownership by the National Scheme of the payment scheme software. The Member shall not in any way assert any ownership rights in the payment scheme software.

The Member will treat the payment scheme software carefully and confidential.

25.1 استخدام رقم التعريف المصرفي

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على كل عضو استخدام أرقام التعريف المصرفية فقط، طبقاً للمعايير ولأغراض أنشطة إصدار البطاقة.

لا يحق للمسؤول أو المسؤولين التابعين له استخدام أرقام التعريف المصرفية بطريقة تخالف ماهو محدد من قبل مشغل شبكة الدفع المحلية.

26.1 استخدام الأعضاء لنظام أرقام التعريف المصرفية

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

لمشغل شبكة الدفع المحلية أن يعين للعضو رقم تعريف شخصي واحد، أو أكثر.

يجب ألا يتم ترخيص استخدام رقم التعريف المصرفي من الباطن، أو إعادة تعيينه أو نقله بطريقة أخرى.

لمشغل شبكة الدفع المحلية الحق في:

- مراجعة استخدام العضو لرقم التعريف المصرفي للامتثال للمعايير.
- سحب التنازل عن أي رقم تعريف مصرفي تم تعيينه لعضو لسبب مناسب.

27.1 استخدام وكشف و إدارة التاجر لمعلومات رقم التعريف المصرفي

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على التاجر عدم استخدام أو الإفصاح بأي شكل من الأشكال عن بيانات رقم التعريف المصرفي أو الحساب لأي شخص آخر غير القابل، أو إلى مشغل شبكة الدفع المحلية، أو استجابة لطلب سلطة رسمية مختصة.

وينطبق هذا الحظر على بيانات رقم التعريف المصرفي أو الحساب الموجودة في بصمات البطاقة، ونسخ الكربون، وإيصالات المعاملات، والقوائم البريدية، والأشرطة، وملفات قاعدة البيانات، وجميع الوسائط الأخرى التي تم إنشاؤها أو الحصول عليها نتيجة لمعاملة.

يجب أن يتعامل التاجر مع بيانات رقم التعريف المصرفي و الحساب بنفس العناية التي يتعامل بها مع بياناته السرية.

28.1 استخدام تقنية EMV المملوكة للشبكة

يشمل الترخيص، حق العضو في استخدام أي تقنية EMV محددة ومملوكة من قبل مشغل شبكة الدفع المحلية.

29.1 ترخيص البرنامج

يمنح كل عضو ترخيصاً غير حصري ومحدود وغير قابل للتنازل أو النقل وغير قابل للترخيص من الباطن لاستخدام برنامج مشغل شبكة الدفع المحلية فقط لغرض تشغيل برنامج إصدار البطاقة و/أو الحصول عليها.

30.1 الملكية والسرية

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يقر العضو بالملكية الحصرية لمشغل شبكة الدفع المحلية لبرنامج شبكة الدفع. ولا يجوز للعضو بأي حال من الأحوال تأكيد أي حقوق ملكية في برنامج شبكة الدفع. يلتزم كل العضو بأن يتعامل مع برنامج شبكة الدفع بكل عناية وسرية.

1.31 Non-Transferability without Prior Scheme Consent

(Category A as referenced in Book 1 Chapter 1)

The Member’s license to use payment scheme software is non-transferable, unless the National Scheme Operator has given prior consent to the transfer.

1.32 Software Enhancements/Modifications

The National Scheme Operator has the right to make enhancements and modifications to the payment scheme software from time to time. It shall endeavor to provide at least 3 months advance notice of enhancements and modifications whenever possible.

1.33 Suspension or Amendment of Membership Status

The CBL has the right, in its discretion, to suspend or amend the membership status of a Member, if it ceases to fulfil the criteria and conditions for its current membership status.

1.34 Termination of Membership

When the License of a Member is terminated, its Scheme membership also terminates. And he must Provide written notice and submit any documentation required by the National Scheme.

The notice will be effective [30] days after receipt thereof by the National Scheme.

1.35 Rights, Liabilities, and Obligations of Terminated Principal Members

(Category A as referenced in Book 1 Chapter 1)

All of the following apply with respect to a terminated Principal Member.

- Except as otherwise set forth in the Standards, a terminated Member has no right to use the Brand or to otherwise engage or participate in any Activity. A terminated Member must immediately cease its use of the Brand and must ensure that such Brand is no longer used by any of the following:
 - The Member’s Merchants;
 - Any Affiliated Participant by a terminated Principal;
 - Any Service Providers that support the terminated Principal and/or any Affiliated Participant by the terminated Principal;
 - Merchants of an Affiliated Participant by a terminated Principal;
 - Any other entity or person acting to provide, directly or indirectly, service related to Activity undertaken pursuant to the authority or purported authority of the terminated Member.
- A terminated Member is not entitled to any refund of dues, fees, assessments, or other payments and remains liable for, and must promptly pay to this National Scheme (a) any and all applicable dues, fees, assessments, or other charges as provided in the Standards and (b) all other charges, debts, liabilities, and other amounts arising or owed in connection with the Member’s Activities, whether arising, due, accrued, or owing before or after termination.
- The terminated Member must promptly cancel all Cards then outstanding that were issued by the terminated Member and, if the terminated Member is a Principal, by all of that Member’s Affiliated Participants. All Payment Applications resident on Chip Cards issued by a terminated Member must be eradicated or disabled no more than six months after the effective date of termination. With respect to any such Card not used during

31.1 عدم قابلية التحويل دون الموافقة المسبقة للشبكة

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

ترخيص العضو لاستخدام برنامج شبكة الدفع غير قابل للتنازل أو النقل، ما لم يكن مشغل شبكة الدفع المحلية قد أعطى موافقة الكتابية المسبقة على النقل.

32.1 تحسينات/تعديلات البرامج

لمشغل شبكة الدفع المحلية إجراء التحسينات والتعديلات على برنامج شبكة الدفع بشكل دوري. ويجب أن يسعى لتقديم إشعار مسبق قبل 3 أشهر على الأقل بالتحسينات والتعديلات كلما أمكن ذلك.

33.1 تعليق أو تعديل حالة العضوية

لمصرف ليبيا المركزي، وفقاً لسلطته التقديرية، تعليق أو تعديل حالة عضوية العضو، إذا توقف عن استيفاء المعايير وشروط العضوية الحالية.

34.1 إنهاء العضوية

عند إنتهاء ترخيص العضو، تنتهي عضوية العضو في النظام أيضاً. ويجب عليه تقديم إشعار كتابي وتقديم الوثائق المطلوبة من قبل مشغل شبكة الدفع المحلية. سيكون الإشعار ساري المفعول بعد [30] يومًا من استلامه من قبل مشغل شبكة الدفع المحلية.

35.1 حقوق ومسؤوليات والتزامات الأعضاء المسؤولين المنتهية عضويتهم

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

تسري القواعد التالية على العضو المسؤول المنتهية عضويته:

- باستثناء ما هو منصوص عليه في المعايير، لا يحق للعضو المنتهية عضويته استخدام العلامة التجارية، أو الانخراط أو المشاركة في أي نشاط. ويجب على العضو المنتهية عضويته التوقف فوراً عن استخدام العلامة التجارية ويجب عليه التحقق من أن هذه العلامة التجارية لم تعد مستخدمة من قبل أي مما يلي:
 - التجار الأعضاء.
 - العضو المشارك المنتسب من قبل عضو مسؤول منتهية عضويته.
 - مقدمو الخدمة الذين يدعمون العضو المسؤول المنتهية عضويته و/أو العضو المشارك التابع للعضو المسؤول المنتهية عضويته.
 - التجار التابعون للعضو المشارك التابع للعضو المسؤول المنتهية عضويته.
 - أي جهة أو شخص آخر يعمل بشكل مباشر أو غير مباشر على تقديم خدمة ذات صلة بالنشاط المضطلع به وفقاً للصلاحيات أو للصلاحيات المزعومة للعضو المنتهية عضويته.
- لا يحق للعضو المنتهية عضويته استرداد أي مستحقات أو رسوم أو تقييمات أو مدفوعات أخرى، ويظل مسؤولاً وبشكل عاجل عن السداد لمشغل شبكة الدفع المحلية: (أ) جميع المستحقات أو الرسوم أو التقييمات السارية أو الرسوم الأخرى على النحو المنصوص عليه في المعايير. (ب) جميع الرسوم والديون والمسؤوليات الأخرى والمبالغ الأخرى الناشئة أو المستحقة فيما يتعلق بأنشطة العضو، سواء كانت ناشئة أو مستحقة أو متراكمة قبل أو بعد الإنهاء.
- يجب على العضو المنتهية عضويته إلغاء جميع البطاقات المعلقة التي تم إصدارها من قبل العضو المنتهية عضويته فوراً، وإذا كان العضو المنتهية عضويته عضواً مسؤولاً، فيجب على جميع المشاركين المنتسبين لهذا العضو إلغاؤها على الفور. ويجب إلغاء أو تعطيل جميع طلبات الدفع

the six-month period, the Issuer must block all Payment Applications the first time the Card goes online. The terminated Member must promptly cause all of its Cardholders and the Cardholders of any Sponsored Participants to be notified of the cancellation of Cards in writing. Such notice must be in a form and substance satisfactory to the National Scheme Operator.

4. A terminated Member must give prompt notice of its termination to any Merchants the Member has authorized to honor Cards. If any such Merchant wishes to continue to accept Cards, the terminated Member must cooperate with the National Scheme Operator and other Members in facilitating the transfer of such Merchant to another Member.
5. If a terminated Member does not take an action that this Rule or any other Standard or that the National Scheme otherwise requires, the National Scheme has the right to take any such required action without prior notice to the terminated Member and on behalf of and at the expense of the Member.
6. 6. If a Participant terminates its Affiliated relationship by a Principal, the Affiliated Principal must cause the Participant to take the actions required of a terminated Member under this Rule. If that Participant fails to so comply, the National Scheme Operator has the right to take any action that this Rule requires without notice to the Participant or the Sponsoring Principal on behalf of and at the expense of the Affiliated Principal.
7. If a Participant ceases to be Affiliated through a Principal, such Principal is nonetheless obligated, pursuant to and in accordance with the Standards, to accept from other Members the records of Transactions arising from the use of Cards issued by that formerly Sponsored Participant and whether such Transactions arise before or after the cessation of the Sponsorship.
8. A terminated Member has no right to present records of Transactions effected after the date of termination to any other Member, except as permitted by the Standards.
9. A terminated Member continues to have the rights and obligations set forth in the Standards and Licenses with respect to its use of the Brand and conduct of Activity until such time as the National Scheme determines that such rights and obligations cease.
10. A terminated Member has a continuing obligation to provide promptly to the National Scheme Operator, on request, Member Reports and any other information about Activity.
11. A terminated Member must, at the option of the National Scheme Operator, immediately either destroy, or take such steps as the National Scheme Operator shall require regarding all confidential and proprietary information of the National Scheme Operator in any form previously received as a Member.
12. The CBL has the right to continue the membership and Licenses, as the case may be, of a terminated Member for purposes of the orderly winding down or transfer of the terminated Member's business. Such continuation of membership and Licenses is subject to such terms as are required by the National Scheme Operator.

المقيمة على بطاقات الشريحة الصادرة عن العضو المنتهية عضويته في مدة لا تزيد عن ستة أشهر بعد التاريخ الفعلي للإلغاء. وفيما يتعلق بالبطاقات التي لم يتم استخدامها خلال فترة الستة أشهر، يجب على جهة الإصدار حظر جميع تطبيقات الدفع في المرة الأولى التي يتم فيها استخدام البطاقة عبر الإنترنت. ويجب على العضو المنتهية عضويته أن يقوم على الفور بإخطار جميع حاملي بطاقته وحاملي بطاقات أي مشارك مكفول كتابيًا بإلغاء البطاقات. وحتى يكون هذا الإشعار صحيحاً، يجب أن يكون من حيث الشكل والمضمون طبقاً لما يقدره مشغل شبكة الدفع المحلية.

4. يجب على العضو المنتهية عضويته تقديم إشعار فوري بالإلغاء إلى التجار الذين فوضهم العضو لقبول البطاقات. وإذا رغب أي تاجر في الاستمرار في قبول البطاقات، يجب على العضو المنتهية عضويته التعاون مع مشغل شبكة الدفع المحلية والأعضاء الآخرين في تسهيل نقل هذا التاجر إلى عضو آخر.

5. إذا لم يتخذ العضو المنتهية عضويته إجراءً تتطلبه هذه القاعدة، أو أي معيار آخر أو أن مشغل شبكة الدفع المحلية يتطلب خلاف ذلك، فإن مشغل شبكة الدفع المحلية له الحق في اتخاذ أي إجراء مطلوب من هذا القبيل دون إشعار مسبق للعضو المنتهية عضويته، وبالنسبة عن وعلى حساب العضو.

6. إذا قام أحد المشتركين بإنهاء علاقته التابعة للمسؤول، فيجب على المسؤول التابع أن يوجه العضو المشارك إلى اتخاذ الإجراءات المطلوبة من العضو المنتهية عضويته بموجب هذه القاعدة. إذا فشل هذا المشارك في الامتثال لذلك، كان لمشغل شبكة الدفع المحلية اتخاذ أي إجراء تتطلبه هذه القاعدة دون إشعار للمشارك أو المسؤول الراعي نيابة عن وعلى نفقة المسؤول التابع.

7. إذا لم يعد أحد المشتركين منتسباً من خلال المسؤول، فإن هذا المسؤول ملزم مع ذلك، وفقاً للمعايير، أن يقبل من أعضاء آخرين سجلات المعاملات الناشئة عن استخدام البطاقات الصادرة عن العضو المشارك المكفول سابقاً، سواء أكانت هذه المعاملات تنشأ قبل أو بعد توقف الكفالة.

8. لا يحق للعضو المنتهية عضويته تقديم سجلات المعاملات المنفذة بعد تاريخ الإنهاء إلى أي عضو آخر، باستثناء ما تسمح به المعايير.

9. يستمر العضو المنتهية عضويته في التمتع بالحقوق والالتزامات المنصوص عليها في المعايير والتراخيص فيما يتعلق باستخدامه للعلامة التجارية وإجراء النشاط حتى يحين الوقت الذي يقرر فيه مشغل شبكة الدفع المحلية توقف الحقوق والالتزامات.

10. يستمر العضو المنتهية عضويته بالتزامه بتقديم تقارير الأعضاء والمعلومات الأخرى حول النشاط إلى مشغل شبكة الدفع المحلية على الفور، عند الطلب.

11. يجب على العضو المنتهية عضويته فوراً، بناءً على اختيار مشغل شبكة الدفع المحلية، إما أن يدمر أو يتخذ الخطوات التي يطلبها مشغل شبكة الدفع المحلية فيما يتعلق بجميع المعلومات السرية والمملوكة لمشغل شبكة الدفع المحلية بأي شكل تم استلامه مسبقاً كعضو.

12. لمصرف ليبيا المركزي سلطة تقرير مواصلة عضوية وتراخيص العضو المنتهية عضويته حسب مقتضى الحال لأغراض التصفية المنظمة أو نقل أعمال العضو المنتهية عضويته. يخضع استمرار العضوية والتراخيص للشروط التي يطلبها مشغل شبكة الدفع المحلية.

1.36 Participation in the Payment Scheme

The following sections apply to participation in the payment scheme. And the principle members deemed obliged to ensure that the following sections abided by the below mentioned entities.

1.36.1 Registration for Non-Issuing/Acquiring Activities

Entities that do not directly engage in issuing or acquiring Activity have the right to participate in the payment scheme if they are duly registered by the National Scheme Operator. Examples of such entities are Card manufacturers, and Terminal vendors.

1.36.2 Card Production

(Category A as referenced in Book 1 Chapter 1)

1.36.2.1 Compliance with Card Production Standards

The requirements in this section apply with respect to Cards and other types of Access Devices, including Contactless Payment Devices and Mobile Payment Devices.

An Issuer engaged in Card production must comply with all applicable Standards, including but not limited to those set forth in this section and in the following documents:

- Card Design Standards (chapter 6 of these rules)
- Card Production Physical Security Requirements
- Card Production Logical Security Requirements
- Security Requirements for Mobile Payment Provisioning

The Card Production Physical Security Requirements and the Card Production Logical Security Requirements documents are available on the Payment Card Industry Security Standards Council (PCI SSC) website under the Card Production tab at www.pcisecuritystandards.org/security_standards/documents.php.

Card production activities subject to compliance with these Standards include, by way of example and not limitation, the treatment and safeguarding of Cards, Card manufacture, printing, embossing, encoding, and mailing, as well as any phase of the production and distribution of Cards or Card account information.

1.36.2.2 Monitoring of Personnel

To the extent permitted by law, Issuers must conduct credit and criminal record checks for all personnel handling embossed or unembossed Cards, including part-time and temporary personnel. In addition, to the extent permitted by law, Issuers must not employ such personnel with one or more known criminal convictions, high credit risk backgrounds, or both, in Card storage and processing areas. Issuers must not allow such personnel access to account numbers, embossed or unembossed Cards, embossing or encoding equipment, nor are they permitted to engage such personnel in security or waste processing work. Issuers are responsible for any fraud that occurs owing to their noncompliance with this Rule.

36.1 الاشتراك في شبكة الدفع

تنطبق الأقسام التالية على الاشتراك في شبكة الدفع. ويعتبر الأعضاء المسؤولون ملزمين بضمان التزام الجهات التالية بالأقسام المذكورة أدناه.

1.36.1 التسجيل في الأنشطة غير المصدرة/ القابلة

يجوز للجهات التي لا تشارك بشكل مباشر في إصدار أو الحصول على نشاط، المشاركة في شبكة الدفع إذا كانت مسجلة حسب الأصول من قبل مشغل شبكة الدفع المحلية. ومن أمثلة هذه الجهات مصنعي البطاقات وموردي الأجهزة.

2.36.1 إنتاج البطاقة

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

1.2.36.1 الامتثال لمعايير إنتاج البطاقات

تنطبق القواعد الواردة في هذا القسم فيما يتعلق بالبطاقات وأنواع أخرى من أجهزة الوصول، بما في ذلك أجهزة الدفع عن بعد، وأجهزة الدفع عبر الهاتف المحمول.

يجب أن تمثل جهة الإصدار المشاركة في إنتاج البطاقة لجميع المعايير المعمول بها، بما في ذلك على سبيل المثال، تلك المنصوص عليها في هذا القسم وفي المستندات التالية:

- معايير تصميم البطاقة (الفصل 6 من هذه القواعد).
- متطلبات الأمان المادية لإنتاج البطاقة.
- متطلبات الأمان المنطقية لإنتاج البطاقة.
- متطلبات الأمان لتوفير الدفع بواسطة الهاتف المحمول.

تتوفر متطلبات الأمان المادية لإنتاج البطاقة، ووثائق متطلبات الأمان المنطقية لإنتاج البطاقة على موقع مجلس معايير أمان صناعة بطاقات الدفع (PCI SSC) ضمن علامة التبويب "إنتاج البطاقات" على www.pcisecuritystandards.org / معايير الأمان / ts.phpmendocu .

تشمل أنشطة إنتاج البطاقات الخاضعة للامتثال لهذه المعايير، على سبيل المثال، معالجة البطاقات وحمايتها، تصنيع البطاقات، الطباعة، النقش، التشفير، البريد، وكذلك أي مرحلة من مراحل إنتاج وتوزيع البطاقات أو معلومات حساب البطاقة.

2.2.36.1 مراقبة الموظفين

في حدود القانون، يجب على جهات الإصدار إجراء فحوصات ائتمانية، وسجلات جنائية لجميع الموظفين الذين يتعاملون مع البطاقات المنقوشة أو غير المنقوشة، بما في ذلك الموظفين بدوام جزئي والمؤقتين. بالإضافة إلى ذلك، يجب على جهات الإصدار عدم توظيف من صدر ضده حكم في جنائية أو جنحة مخلّة بالشرف، أو خلفيات ائتمانية عالية المخاطر، أو كليهما، في مناطق تخزين البطاقات ومعالجتها. ويجب ألا تسمح جهات الإصدار لهؤلاء الموظفين بالوصول إلى أرقام الحسابات أو البطاقات المنقوشة أو غير المنقوشة أو معدات النقش أو التشفير، ولا يُسمح لهم بإشراك هؤلاء الموظفين في أعمال الأمن أو معالجة النفايات. وتعد جهات الإصدار مسؤولة عن أي احتيال يحدث بسبب عدم امتثالهم لهذه القاعدة.

1.36.3 Contracting with Card Registration Companies

A card registration company (“Company”) is any entity that stores Card account numbers and, upon notification by the Cardholder, reports the loss or theft of the Card(s) to the Issuer(s).

The Issuer must at all times be entirely responsible for and must manage, direct, and control all aspects of its Program and Program Service performed by Service Providers.

Any Issuer having a contractual agreement with a Company pursuant to which the Company registers that Issuer’s Cardholder account numbers must ensure that the contract includes the following obligations on the part of the Company:

- The Company shall maintain any Cardholder information, including, without limitation, names, addresses, phone numbers, and account numbers in strictest confidence and disclose them only to the Issuer. The Company shall keep any media containing this type of information in an area limited to selected personnel having access on a need-to-know basis. Before discarding such media, the Company shall destroy it in a manner that will render the data unreadable.
- The Company shall control and limit access to account numbers stored in a computer environment by establishing procedures that must include, but are not limited to, a password system for computer remote terminal (CRT) access and control over dial-up lines or any other means of access.
- The Company must not use the name of NUMO in any promotion or advertising, except as provided by a contractual agreement with the Issuer for purposes of soliciting and providing services to the Issuer’s Cardholders. The National Scheme Operator reserves the right to approve any such materials.
- The Company must maintain a 24-hours-per-day, seven-days-per-week service to receive Cardholder reports on lost or stolen Cards. The Company shall transmit each report immediately and in any event no later than two hours after receiving the report, by the most expeditious means, for example, phone or fax, to the appropriate Issuer.

At a minimum, the notification must include:

- Account number
- Issuer’s name
- Cardholder’s name, address, and phone number
- Phone number where the Cardholder can be reached
- Whether the Card was lost or stolen
- Time and location of the reported loss or theft
- The Company shall report any loss or theft of Cardholder information whether due to act or omission, to the National Scheme Operator and to the Issuer with which it has a contract within 24 hours of discovery of the loss or theft.
- The Company must convey a Cardholder request for a replacement Card to the Issuer.
- The contract must include an indemnification clause holding the National Scheme Operator, its officers, its directors and employees, its Members, and the Issuer having the contract with the Company not liable for any loss or damage claimed by or on behalf of the Cardholder, Issuer, or other person or entity that is alleged to be attributable to the Company’s failure to properly provide the services described in the contract or failure to safeguard account information.

1.36.3 التعاقد مع شركات تسجيل البطاقات

شركة تسجيل البطاقة (“الشركة”) هي جهة تقوم بتخزين أرقام حسابات البطاقة، وبناءً على إشعار من حامل البطاقة، يقوم بالإبلاغ عن فقد أو سرقة البطاقة (البطاقات) إلى جهة الإصدار (جهات الإصدار). يجب أن تكون جهة الإصدار مسؤولة ومسؤولية كاملة في جميع الأوقات عن إدارة وتوجيه والتحكم في جميع جوانب البرنامج وخدمة البرنامج التي يقوم بها مقدمي الخدمة.

على جهة الإصدار المتعاقدة مع إحدى الشركات التي سجلت أرقام جهة إصدار حامل البطاقة ، أن تلتزم بتضمين العقد الالتزامات التالية للشركة :

- تحتفظ الشركة بالمعلومات الخاصة بحامل البطاقة، بما في ذلك، على سبيل المثال ، الأسماء والعناوين وأرقام الهواتف وأرقام الحسابات بسرية تامة والإفصاح عنها فقط لجهة الإصدار. ويجب على الشركة الاحتفاظ بالوسائط التي تحتوي على هذا النوع من المعلومات في منطقة تقتصر على موظفين مختارين لديهم إمكانية الوصول على أساس الحاجة إلى المعرفة. قبل التخلص من هذه الوسائط، يجب على الشركة تدميرها بطريقة تجعل البيانات غير قابلة للقراءة.
- يجب أن تتحكم الشركة وتحد من الوصول إلى أرقام الحسابات المخزنة في بيئة الكمبيوتر عن طريق وضع إجراءات يجب أن تتضمن، على سبيل المثال، نظام كلمة مرور للوصول إلى منظومة الكمبيوتر عن بُعد، والتحكم في خطوط الاتصال الهاتفي أو أي وسيلة أخرى من الوصول.
- يجب ألا تستخدم الشركة اسم نمو في أي ترويج أو إعلان، باستثناء ما هو منصوص عليه في العقد مع جهة الإصدار لأغراض التماس وتقديم الخدمات إلى حاملي بطاقات جهة الإصدار. ويحتفظ مشغل شبكة الدفع المحلية بالحق في الموافقة على أي من هذه المواد.
- يجب أن تحافظ الشركة على خدمة 24 ساعة في اليوم وسبعة أيام في الأسبوع، لتلقي تقارير حامل البطاقة عن البطاقات المفقودة أو المسروقة. ويجب على الشركة إرسال كل تقرير على الفور وفي أي حال في موعد لا يتجاوز ساعتين بعد استلام التقرير، بأسرع الوسائل، على سبيل المثال، الهاتف أو الفاكس، إلى جهة الإصدار المناسبة.

كحد أدنى، يجب أن يتضمن الإخطار ما يلي:

- رقم الحساب.
- اسم جهة الإصدار.
- اسم حامل البطاقة وعنوانه ورقم هاتفه.
- رقم الهاتف الذي يمكن من خلاله الوصول إلى حامل البطاقة.
- ما إذا كانت البطاقة مفقودة أو مسروقة.
- وقت ومكان الفقد أو السرقة المبلغ عنها.
- يتعين على الشركة الإبلاغ عن ضياع أو سرقة معلومات حامل البطاقة سواء كان ذلك بسبب فعل أو إهمال، إلى مشغل شبكة الدفع المحلية، وجهة الإصدار الذي أبرمت معه عقدًا خلال 24 ساعة من اكتشاف واقعة الفقدان أو السرقة.
- يجب على الشركة نقل طلب حامل البطاقة للحصول على بطاقة بديلة إلى جهة الإصدار.
- يجب أن يشتمل العقد على بند تعويض يجعل مشغل شبكة الدفع المحلية ومسؤوليه ومديره وموظفيه وأعضائه وجهة الإصدار المتعاقدة مع الشركة غير مسؤولين عن أي خسارة أو ضرر يُطالب به حامل البطاقة أو جهة الإصدار أو نيابة عنها، أو أي شخص أو جهة أخرى يُعزى إليها فشل الشركة في تقديم الخدمات الموضحة في العقد بشكل صحيح أو الفشل في حماية معلومات الحساب.

- The Company must be covered by liability, fidelity, fire, and theft insurance and must have a disaster recovery plan to ensure continuity of services in the event of natural or other events that disrupt or threaten to disrupt service unless otherwise agreed to in writing by the National Scheme Operator. Coverage must be reasonable and adequate in consideration of the nature and volume of work performed, the plant location, physical condition, and security of the plant, and the number and duties of employees.
- The Company must comply with all applicable laws, rules, and regulations, including, without limitation, consumer protection laws, applicable to the services offered and performed by the Company.

1.36.4 Working with Vendors, Card Manufacturers and Personalization Bureaus

Before employing the services of a vendor for Card production and/or personalization, including any associated services, a Member must ensure that the vendor has been certified by the National Scheme Operator. The Member shall contact the National Scheme Operator to obtain a list of the currently certified vendors.

Prior to certification and annual recertification of a vendor facility, the National Scheme Operator has the right to conduct an on-site audit of the facility to evaluate its compliance with physical, logical, and mobile payment provisioning security Standards.

The Card Production Physical Security Requirements and the Card Production Logical Security Requirements documents are available on the PCI SSC website under the Card Production tab at www.pcisecuritystandards.org/security_standards/documents.php. A certified vendor facility is issued a compliance certification, which is subject to annual renewal provided the vendor facility remains in good standing.

Any agreement between an Issuer and a vendor for Card production services should contain terms stating that the vendor agrees to safeguard and control usage of Account data and to comply with all applicable Standards then in effect, including but not limited to those set forth in this section.

3.36.4.1 Order Request Required to Produce Cards

No vendor has the right to print or manufacture any Card, sample, or facsimile, on plastic or any other material, except in response to a specific order from a Member or from the National Scheme Operator.

The National Scheme Operator reserves the right to request from a vendor Card samples for review.

1.37 Types of Service Providers

A Service Provider is categorized by the National Scheme Operator based upon the National Scheme Operator's understanding of the nature of the Program Services to be performed, as described below. A Service Provider is permitted to perform exclusively the Program Services it is registered to perform.

(See appendix number 1)

The following are descriptions of the types of Program Service.

- يجب أن تكون الشركة مغطاة بتأمين ضد المسؤولية والإخلاء والحريق والسرقة، ويجب أن يكون لديها خطة للتعافي من الكوارث لضمان استمرارية الخدمات في حالة الأحداث الطبيعية أو غيرها من الأحداث التي تعطل أو تهدد بتعطيل الخدمة ما لم يتفق على خلاف ذلك كتابيًا من قبل مشغل شبكة الدفع المحلية. ويجب أن تكون التغطية معقولة، وكافية بالنظر إلى طبيعة وحجم العمل المنجز، وموقع المصنع، والحالة المادية، وأمن المصنع، وعدد وواجبات الموظفين.
- يجب أن تمثل الشركة لجميع القوانين والقواعد واللوائح المعمول بها، قوانين حماية المستهلك التي تنطبق على الخدمات المعروضة من الشركات والخدمات المقدمة منها .

1.36.4 العمل مع البائعين، ومصنعي البطاقات ومكاتب التخصيص

قبل استخدام خدمات البائع لإنتاج البطاقة و/أو إضفاء الطابع الشخصي، بما في ذلك الخدمات المرتبطة معها، يجب على العضو التحقق من اعتماد البائع من قبل مشغل شبكة الدفع المحلية. ويجب على العضو التواصل مع مشغل شبكة الدفع المحلية للحصول على قائمة البائعين المعتمدين حاليًا.

وقبل الحصول على الشهادة، وإعادة التصديق السنوية لمنشأة البائع، يجوز لمشغل شبكة الدفع المحلية إجراء تدقيق وفحص في موقع المنشأة لتقييم امتثالها لمعايير تأمين الدفع المادية والمنطقية والمتنقلة.

تتوفر متطلبات الأمان المادية لإنتاج البطاقة ومستندات متطلبات الأمان المنطقية لإنتاج البطاقة على موقع الويب PCI SSC ضمن علامة التبويب "إنتاج البطاقات" على www.pcisecuritystandards.org/documents.php / معايير الأمان / documents.php .

يتم إصدار شهادة امتثال منشأة بائع معتمد، والتي تخضع للتجديد السنوي بشرط أن تظل منشأة البائع في وضع جيد.

يجب أن يحتوي العقد بين جهة الإصدار والبائع لخدمات إنتاج البطاقة على شروط: تنص على أن البائع يوافق على حماية بيانات الحساب والتحكم فيها والامتثال لجميع المعايير المعمول بها في ذلك الوقت، بما في ذلك على سبيل المثال، تلك المنصوص عليها في هذا القسم.

1.36.4.1 طلب الأمر المطلوب لإنتاج البطاقات

لا يحق للبائع طباعة أو تصنيع أي بطاقة أو عينة أو صورة طبق الأصل على البلاستيك أو أي مادة أخرى، إلا في حالة الاستجابة لطلب معين من أحد الأعضاء أو من مشغل شبكة الدفع المحلية. و لمشغل شبكة الدفع المحلية الحق في طلب عينات من بطاقة البائع للمراجعة.

1.37 أنواع مقدمي الخدمة

يتم تصنيف مقدمي الخدمة من قبل مشغل شبكة الدفع المحلية بناءً على تقدير مشغل شبكة الدفع المحلية لطبيعة خدمات البرنامج التي يتعين القيام بها، كما هو موضح أدناه. يُسمح لمقدم الخدمة بأداء خدمات البرنامج المسجلة لأدائها حصريًا.

(انظر الملحق رقم 1)

فيما يلي وصف لأنواع خدمة البرنامج .

1.37.1 Independent Sales Organization (ISO) Program Service

is a third-party payment processing company that is authorized to handle merchant accounts for businesses. ISOs have relationships with acquiring member banks, and this allows them to provide merchant services to their customers.

1.37.2 Third Party Processor (TPP) Program Service

- Support for mobile remote payment functionality, which is initiated by an enrolled Cardholder from a Cardholder-controlled mobile phone registered with the Issuer, and used for entry of a Cardholder’s PIN or mobile-specific credentials
- Authorization services, including but not limited to authorization routing, payment gateway and switching services, voice authorization, and call referral processing
- Clearing file preparation and submission
- Settlement processing (excluding possession, ownership, or control of settlement funds, which is not permitted)
- Cardholder and/or Merchant statement preparation affording access to Account data, Transaction data, or both
- Cardholder customer service including access to Account data, Transaction data, or both
- Fraud control and risk monitoring, including but not limited to fraud screening and fraud scoring services
- Chargeback processing for Acquirers and/or Issuers
- Chargeback processing for Merchants or Sub merchants
- Any other service determined by the National Scheme Operator in its sole discretion to be TPP Program Service

Third Party Processor

(Category A as referenced in Book 1 Chapter 1)

All TPPs must comply with applicable Standards, including these Service Provider Rules, in order to remain in good standing as a TPP.

TPP are categorized as An entity processing the activity of Issuing cards on behalf of a Member Bank.

1.37.3 Data Storage Entity (DSE) Program Service

An entity that stores, processes or transmits transactions on behalf of a Member, Merchant or Member Service Provider (MSP).

1.37.4 Payment Service Provider (PSP) Program Service

(Category A as referenced in Book 1 Chapter 1)

A Payment Service Provider is a party that performs any one or more of the services described as Acquiring Payment Services on behalf of licensed Acquirer Bank. A Member, either directly or through a Payment service Provider, is responsible for ensuring that each merchant complies on an ongoing basis with all Standards applicable to Merchants.

The Acquirer is responsible for all acts and omissions of a Payment Service Provider and of any Merchant.

1.37.1 خدمة برنامج منظمة المبيعات المستقلة

هي شركة معالجة مدفوعات تابعة لجهات خارجية، ومرخص لها بمعالجة حسابات التاجر للشركات. تتمتع منظمة المبيعات المستقلة بعلاقات مع المصارف القابلة على الأعضاء، وهذا يسمح لهم بتقديم خدمات التاجر لعملائهم.

2.37.1 خدمة برنامج معالج الطرف الثالث

- دعم وظائف الدفع عن بعد عبر الهاتف المحمول، والتي يبدأها حامل البطاقة المسجل من هاتف محمول يتحكم فيه حامل البطاقة ومسجل لدى جهة الإصدار، ويستخدم لإدخال رقم التعريف الشخصي لحامل البطاقة أو بيانات الاعتماد الخاصة بالهاتف المحمول.
- خدمات التفويض، بما في ذلك على سبيل المثال، توجيه التفويض وبوابة الدفع وخدمات التحويل والتفويض الصوتي ومعالجة إحالة المكالمات.
- تحضير ملف المقاصة وتقديمه.
- معالجة التسوية (باستثناء الحيازة أو الملكية أو التحكم في أموال التسوية، وهو أمر غير مسموح به).
- إعداد كشف حساب حامل البطاقة و/أو التاجر يتيح الوصول إلى بيانات الحساب أو بيانات المعاملات أو كليهما.
- خدمة عملاء حامل البطاقة بما في ذلك الوصول إلى بيانات الحساب أو بيانات المعاملات أو كليهما.
- مراقبة الاحتيال ومراقبة المخاطر، بما في ذلك على سبيل المثال، فحص الاحتيال وخدمات تسجيل الاحتيال.
- معالجة رد المبالغ المدفوعة للقابليين و/أو جهات الإصدار.
- معالجة رد المبالغ المدفوعة للتجار أو التجار من الباطن.
- أي خدمة أخرى يحددها مشغل شبكة الدفع المحلية وفقًا لتقديره الخاص لتكون خدمة برنامج معالج الطرف الثالث.

معالج الطرف الثالث

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب أن تمثل جميع معالجات الطرف الثالث للمعايير المعمول بها، بما في ذلك قواعد مقدم الخدمة هذه، من أجل البقاء في وضع جيد كشريك معالج الطرف الثالث. يتم تصنيف معالج الطرف الثالث على أنها جهة تعالج نشاط إصدار البطاقات نيابة عن مصرف عضو.

3.37.1 خدمة برنامج جهة تخزين البيانات

هو كيان يقوم بتخزين المعاملات أو معالجاتها أو نقلها نيابة عن عضو أو تاجر أو مقدم خدمة عضو.

4.37.1 خدمة برنامج مقدم خدمة الدفع

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

مقدم خدمة الدفع هو طرف يؤدي خدمة أو أكثر من الخدمات الموصوفة على أنها الحصول على خدمات الدفع نيابة عن مصرف القابل المرخص. ويتحمل العضو، سواء بشكل مباشر أو من خلال مقدم خدمة الدفع، مسؤولية ضمان امتثال كل تاجر بشكل مستمر لجميع المعايير المطبقة على التجار. القابل مسؤول عن جميع حالات تقصير مقدم خدمة الدفع، وعن أي تاجر.

1.37.4.1 Responsibility for Payment Service Provider and Sub merchant Activity

The Acquirer is responsible for the Activity of the Payment Service Provider and each of the Payment Service Provider’s Sub merchants. The Acquirer must ensure ongoing compliance with all of the following.

1. Each Sub merchant must be located in Libya.
2. Settlement funds which the Acquirer permits a Payment Service Provider to access must only be used to pay Sub merchants pursuant to the terms of Sub merchant Agreements.
3. An Acquirer has the right to permit a Payment Service Provider to manage the following obligations on behalf of the Acquirer, and remains fully responsible for the fulfillment of each to the extent that the Payment Service Provider fails to do so:
 - a. Verify that a Sub merchant is a bona fide business operation;
 - b. Retain records concerning the investigation of a prospective Sub merchant, provided that such records are provided to the Acquirer immediately upon request;
 - c. Pay a Sub merchant for Transactions;
 - d. Ensure that a Sub merchant is supplied with materials necessary to effect Transactions; and
 - e. Monitor a Sub merchant’s Activity on an ongoing basis to deter fraud or other wrongful activity.
4. Neither the Payment Service Provider nor the Sub merchant has the right to require a Cardholder to waive a right to dispute a Transaction.
5. The Acquirer must provide to the National Scheme Operator a quarterly Activity report for each Sub merchant of the Payment Service Provider that includes:
 - a. Sub merchant name and location as shown in clearing records
 - b. Sub merchant “doing business as” name or URL
 - c. Sub merchant MCCs
 - d. Transaction sales count and amount for each MCC
 - e. Transaction chargeback count and amount for each MCC

Provided the Acquirer is compliant with paragraphs 6 and 7 set forth immediately below, and unless otherwise required by the National Scheme Operator, the requirements set forth in this paragraph 5 are not applicable.

6. An Acquirer that uses a Payment Service Provider must populate the Submerchant field with a Submerchant ID in all authorization and clearing messages. The Submerchant ID must match the Submerchant ID assigned by the Acquirer or Payment Service Provider.
7. An Acquirer that uses a Payment Service Provider that proposes to sponsor a Submerchant conducting business described under any one of the following MCCs must register such Submerchant separately with the National Scheme Operator.
 - Non-face-to-face pharmaceutical Merchants—MCC 5122 and MCC 5912
 - High-risk cyberlocker Merchants—MCC 4816
 - High-risk securities Merchants—MCC 6211

1.4.37.1. المسؤولية عن مقدم خدمة الدفع ونشاط التاجر من الباطن

القابل مسؤول عن نشاط مقدم خدمة الدفع، وكل تاجر من الباطن لمقدم خدمة الدفع. يجب أن يضمن القابل الامتثال المستمر لكل ما يلي:

1. يجب أن يكون لكل تاجر من الباطن موطناً مختاراً في دولة ليبيا.
2. أموال التسوية التي يسمح القابل لمقدم خدمة الدفع حق الوصول لها يجب استخدامها فقط للدفع للتجار من الباطن وفقاً لشروط اتفاقيات التجار من الباطن.
3. يحق للقابل السماح لمقدم خدمة الدفع بإدارة الالتزامات التالية نيابة عن القابل، ويظل مسؤولاً بالكامل عن الوفاء بكل منها إلى الحد الذي يفشل فيه مقدم خدمة الدفع في القيام بذلك:
 - أ. التحقق من أن التاجر من الباطن هو مشغل أعمال تجارية حسن النية.
 - ب. الاحتفاظ بالسجلات المتعلقة بالتحقيق مع التاجر من الباطن المحتمل، بشرط أن يتم تقديم هذه السجلات إلى القابل فوراً عند الطلب.
 - ت. الدفع للتاجر من الباطن مقابل المعاملات.
 - ث. التحقق من تزويد التاجر من الباطن بالمواد اللازمة لتنفيذ المعاملات.
 - ج. مراقبة نشاط التاجر من الباطن بشكل مستمر لمكافحة معاملات الاحتيال والأنشطة غير المشروعة.
4. لا يحق لمقدم خدمة الدفع ولا التاجر من الباطن مطالبة حامل البطاقة بالتنازل عن حق الاعتراض على المعاملة.
5. يجب أن تقدم جهة القبول إلى مشغل شبكة الدفع المحلية تقرير ربع سنوي عن نشاط كل تاجر من الباطن لمقدم خدمة الدفع يتضمن:

- أ. اسم التاجر من الباطن والموقع كما هو موضح في سجلات المقاصة.
- ب. اسم التاجر من الباطن “ممارسة الأعمال التجارية باسم” أو عنوان URL.
- ت. MCCs للتاجر من الباطن.
- ث. عدد مبيعات المعاملات والمبلغ لكل MCC.
- ج. عدد عمليات رد المبالغ المدفوعة ومبلغها لكل MCC.

بشرط أن تكون جهة القبول مستوفية لحكم الفقرتين 6 و 7 المنصوص عليهما أدناه مباشرة، وما لم يطلب مشغل شبكة الدفع المحلية خلاف ذلك، فإن المتطلبات المنصوص عليها في هذه الفقرة 5 غير قابلة للتطبيق.

6. يجب على جهة القبول التي تستخدم مقدم خدمة الدفع أن تملأ حقل من الباطن بمعرف التاجر من الباطن في جميع رسائل التفويض والمقاصة. يجب أن يتطابق معرف التاجر من الباطن مع معرف التاجر المعين من قبل جهة القبول أو مقدم خدمة الدفع.
7. يجب على جهة القبول التي تستخدم مقدم خدمة الدفع الذي يقترح كفالة\رعاية تاجر من الباطن يدير الأعمال الموصوفة في أي من MCCs التالية أن تسجل هذا التاجر من الباطن بشكل منفصل مع مشغل شبكة الدفع المحلية.

- تجار الأدوية غير المتواجدين وجهًا لوجه — MCC 5122 و MCC 5912.
- تجار السيبرانيون ذوو الخطورة العالية — MCC 4816.
- تجار الضمانات ذوو الخطورة العالية - MCC 6211.

1.37.4.2 Payment Service Provider Obligations

(Category A as referenced in Book 1 Chapter 1)

The Acquirer must ensure that each of its Payment Service Providers satisfies all of the obligations set forth in this Rule.

Sub merchant Agreement

Pursuant to a written agreement between an Acquirer and a Payment Service Provider, a Payment Service Provider has the right to enter into a Sub merchant Agreement with a Sub merchant for the purpose of facilitating the Acquirer's acquiring of Transactions from the Sub merchant.

The Sub merchant Agreement must conform to Standards pertaining to Merchant Agreements, and must clearly and conspicuously:

- Identify the Acquirer;
- Disclose contact information of the Acquirer that the Sub merchant is permitted use to address questions and concerns; and
- Reflect that the Payment Service Provider is entering into the Sub merchant Agreement on behalf of and as a Service Provider of the identified Acquirer.

The Sub merchant Agreement must not interfere with or lessen the right of the Payment Service Provider, the Acquirer, or the National Scheme Operator to terminate the agreement at any time. The National Scheme Operator reserves the right to restrict a Payment Service Provider from entering into a Sub merchant Agreement based on the business of the entity or other criteria which the National Scheme Operator deems appropriate.

Required Sub merchant Agreement Terms

A Sub merchant Agreement must include all provisions required to be included in a Merchant Agreement, in addition to complying with this section. The failure of the Payment Service Provider to include the substance of any one or more of such Standards in the Sub merchant Agreement, or the grant of a variance by the National Scheme Operator with respect to any one or more such Standards, does not relieve an Acquirer from responsibility for chargebacks or compliance related to the Activity of or use of the Brand by the Sub merchant.

The Sub merchant Agreement must, in substance, include all of the following provisions:

1. On an ongoing basis, the Sub merchant is promptly to provide the Payment Service Provider with the current address of each of its offices, all “doing business as” (DBA) names used by the Sub merchant, and a complete description of goods sold and services provided.
2. In the event of any inconsistency between any provision of the Sub merchant Agreement and the Standards, the Standards will govern.
3. The Payment Service Provider is responsible for the Card acceptance policies and procedures of the Submerchant and has the right to require any changes to its website or otherwise that it deems necessary or appropriate to ensure that the Sub merchant remains in compliance with the Standards governing the use of the Brand.
4. The Sub merchant Agreement automatically and immediately terminates if the National Scheme Operator de-registers the Payment Service Provider or if the Payment Service Provider's Acquirer ceases to be a Member for any reason or if such Acquirer fails to have a valid License with the National Scheme Operator to use the Brand.

2.4.37.1. التزامات مقدمي خدمة الدفع

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على جهة القبول التحقق من أن كل مقدمي خدمة الدفع يفون بجميع الالتزامات المنصوص عليها في هذه القاعدة.

تعاهد التاجر من الباطن

وفقًا لعقد مكتوب بين جهة القبول ومقدم خدمة الدفع، يحق لمقدم خدمة الدفع التعاقد من الباطن مع تاجر لغرض تسهيل حصول جهة القبول على المعاملات من التاجر من الباطن. يجب أن يتوافق تعاهد التاجر من الباطن مع المعايير المتعلقة بعقود التاجر، ويجب أن يقوم بشكل واضح:

- تحديد جهة القبول.
- الإفصاح عن معلومات الاتصال الخاصة بالقابل والتي يُسمح للتاجر من الباطن باستخدامها لمعالجة الأسئلة والمخاوف.
- يعكس صورة خدمة الدفع المتعاقد مع التاجر من الباطن، نيابة عن، وكمقدم خدمة القابل المحدد.

يجب ألا يتعارض تعاهد التاجر من الباطن مع أو يقلل من حق مقدم خدمة الدفع أو جهة القبول أو مشغل شبكة الدفع المحلية في إنهاء العقد في أي وقت. ولمشغل شبكة الدفع المحلية تقييد مقدم خدمة الدفع من الدخول في تعاهد التاجر من الباطن بناءً على أعمال الكيان أو المعايير الأخرى التي يراها مشغل شبكة الدفع المحلية مناسبة.

الشروط المطلوبة لتعاقد التاجر من الباطن

يجب أن يتضمن تعاهد التاجر من الباطن جميع الأحكام المطلوب تضمينها في عقد التاجر، بالإضافة إلى الامتثال لهذا القسم. إن فشل مقدم خدمة الدفع في تضمين جوهر المعايير في عقد التاجر من الباطن، أو منح تباين من قبل مشغل شبكة الدفع المحلية فيما يتعلق بأي معيار أو أكثر من هذه المعايير، فإنه لا يعفي الجهة القابلة من مسؤولية عمليات رد المبالغ المدفوعة أو الامتثال المتعلق بنشاط أو استخدام العلامة التجارية من قبل التاجر من الباطن.

يجب أن يتضمن عقد التاجر من الباطن، من حيث الجوهر، جميع الأحكام التالية:

1. بشكل مستمر، يجب على التاجر من الباطن أن يزود مقدم خدمة الدفع على الفور بالعنوان الحالي لكل مكتب من مكاتبه، وجميع أسماء “ممارسة الأعمال التجارية” التي يستخدمها التاجر من الباطن، ووصفًا كاملًا للبضائع المباعة و الخدمات المقدمة.
2. في حالة وجود تعارض بين حكم من أحكام عقد التاجر من الباطن والمعايير، فإن المعايير هي التي تسري ، ويُلقى كل حكم مخالف لها في العقد.
3. يكون مقدم خدمة الدفع مسؤولًا عن سياسات وإجراءات قبول البطاقة الخاصة بالتاجر من الباطن وله الحق في طلب أي تغييرات على موقعه أو خلاف ذلك يراه ضروريًا أو مناسبًا لضمان التزام التاجر من الباطن بالمعايير التي تحكم الاستخدام للعلامة التجارية.
4. ينتهي عقد التاجر من الباطن تلقائيًا وفوريًا إذا ألغى مشغل شبكة الدفع المحلية تسجيل مقدم خدمة الدفع، أو إذا لم تعد جهة القبول التابعة لمقدم خدمة الدفع عضوًا لأي سبب أو إذا فشلت هذه الجهة في الحصول على ترخيص ساري المفعول مع مشغل شبكة الدفع المحلية لاستخدام العلامة التجارية.

5. The Payment Service Provider has the right, at its discretion or at the direction of its Acquirer or the National Scheme Operator, to immediately terminate the Sub merchant Agreement for activity deemed to be fraudulent or otherwise wrongful by the Payment Service Provider, its Acquirer, or the National Scheme Operator.
6. The Sub merchant acknowledges and agrees:
 7. To comply with all applicable Standards, as amended from time to time;
 - a. That the National Scheme Operator is the sole and exclusive owner of the Mark;
 - b. Not to contest the ownership of the Mark for any reason;
 - c. The National Scheme Operator has the right, at any time, immediately and without advance notice, to prohibit the Sub merchant from using the Mark for any reason;The National Scheme Operator has the right to enforce any provision of the Standards and to prohibit the Sub merchant and/or its Payment Service Provider from engaging in any conduct which the National Scheme Operator deems could injure or could create a risk of injury to the National Scheme Operator, including injury to reputation, or that could adversely affect the integrity of the Interchange System, the National Scheme Operator's Confidential Information, or both; and
 - d. The Sub merchant will not take any action that could interfere with or prevent the exercise of this right by the National Scheme Operator.
 - e. The Sub merchant Agreement must not contain any terms that conflict with any Standard.

1.37.4.3 Payment Service Provider's Obligations as Sponsor of Sub merchants

(Category A as referenced in Book 1 Chapter 1)

A Payment Service Provider must fulfill all of the following obligations with respect to each of its Sub merchants.

Submit Valid Transactions

The Payment Service Provider must submit to its Acquirer records of valid Transactions submitted by a Sub merchant and involving a bona fide Cardholder. The Payment Service Provider must not submit to its Acquirer any Transaction that the Payment Service Provider or the Sub merchant knows or should have known to be fraudulent or not authorized by the Cardholder, or that either knows or should have known to be authorized by a Cardholder colluding with the Sub merchant for a fraudulent purpose. For purposes of this Rule, the Sub merchant is deemed to be responsible for the conduct of its employees, Service Providers, and representatives.

Sub merchant Compliance with the Standards

The Payment Service Provider must ensure that each of its Sub merchants complies with the Standards applicable to Merchants.

Maintaining Sub merchant Information

The Payment Service Provider must maintain, on an ongoing basis, the names, addresses, and URLs if applicable of each of its Sub merchants. The Acquirer must ensure that the Payment Service Provider promptly supplies the National Scheme Operator with any such information upon request.

5. يحق لمقدم خدمة الدفع، وفقاً لتقديره أو بناءً على توجيه من جهة القبول أو مشغل شبكة الدفع المحلية، إنهاء عقد التاجر من الباطن على الفور بسبب النشاط الذي يعتبره مقدم خدمة الدفع أو القابل أو مشغل شبكة الدفع المحلية، من أعمال الاحتيال أو غير مشروع.

6. يقر التاجر من الباطن ويوافق على:
 - أ. الامتثال لجميع المعايير المعمول بها، بحسب ما يتم تعديله من وقت لآخر.
 - ب. أن مشغل شبكة الدفع المحلية هو المالك الوحيد والحصري للعلامة.
 - ت. عدم الطعن في ملكية العلامة لأي سبب من الأسباب.
 - ث. لمشغل شبكة الدفع المحلية، في أي وقت، ودون إشعار مسبق، منع التاجر من الباطن من استخدام العلامة لأي سبب من الأسباب.
 - ج. يحق لمشغل شبكة الدفع المحلية تنفيذ أي بند من أحكام المعايير وحظر التاجر من الباطن و/أو مقدم خدمة الدفع التابع له من ممارسة النشاط، الذي يقدر مشغل شبكة الدفع المحلية أنه يمكن أن يضر أو قد يؤدي إلى إصابة مشغل شبكة الدفع المحلية، بما في ذلك الضرر الذي يلحق بالسمعة، أو قد يؤثر سلباً على سلامة نظام التبادل أو المعلومات السرية لمشغل شبكة الدفع المحلية أو كليهما.
 - ح. يمتنع التاجر من الباطن عن اتخاذ أي إجراء قد يتداخل مع، أو يمنع ممارسة هذا الحق من قبل مشغل شبكة الدفع المحلية.
 - خ. يجب ألا يحتوي عقد التاجر من الباطن على أي شروط تتعارض مع أي معيار.

1.37.4.3. التزامات مقدم خدمة الدفع كراعٍ لتجار من الباطن

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على مقدم خدمة الدفع الوفاء بجميع الالتزامات التالية فيما يتعلق بكل تاجر من تجار الباطن.

تقديم معاملات صالحة

يجب على مقدم خدمة الدفع أن يقدم إلى جهة القبول سجلات المعاملات الصالحة المقدمة من التاجر من الباطن، والتي تشمل حامل بطاقة حسن النية. ويجب عليه، ألا يقدم إلى جهة القبول أي معاملة يعلم مقدم خدمة الدفع أو التاجر من الباطن أو ينبغي أن يكون على علم بكونها احتيالية أو غير مصرح بها من قبل حامل البطاقة، أو أنه يعلم أو ينبغي أن يكون على علم بأنه قد تم التصريح بها من قبل حامل البطاقة عبر التواطؤ مع التاجر من الباطن لغرض احتيالي. لأغراض تطبيق هذه القاعدة، يعتبر التاجر من الباطن مسؤولاً عن سلوك موظفيه ومقدمي الخدمات والممثلين.

امتثال التاجر من الباطن للمعايير

يجب على مقدم خدمة الدفع التحقق من امتثال كل من التجار من الباطن للمعايير المطبقة على التجار.

الاحتفاظ بمعلومات التاجر من الباطن

يجب أن يحتفظ مقدم خدمة الدفع، وبشكل مستمر، بالأسماء والعناوين وعناوين URL، إذا كان ذلك ممكناً لكل من التجار من الباطن التابعين له. ويجب على جهة القبول التحقق من أن مقدم خدمة الدفع يزود مشغل شبكة الدفع المحلية على الفور بهذه المعلومات عند الطلب.

Payments to Sub merchants

Each Payment Service Provider must pay each Sub merchant for all Transactions the Payment Service Provider submits to its Acquirer on the Sub merchant's behalf. This obligation is not discharged with regard to a Transaction until the Sub merchant receives payment from the Payment Service Provider, notwithstanding any payment arrangement between the Sub merchant and the Payment Service Provider or between the Payment Service Provider and its Acquirer.

A Sub merchant Agreement is permitted to provide for a Payment Service Provider to withhold amounts for chargeback reserves or similar purposes.

Supplying Materials to Sub merchants

Each Payment Service Provider must regularly ensure that each of its Sub merchants is provided with all materials necessary to effect Transactions in accordance with the Standards and to signify Card acceptance.

Sub merchant Monitoring

Each Payment Service Provider must monitor on an ongoing basis the Activity and use of the Mark of each of its Sub merchants for the purpose of deterring fraudulent and other wrongful activity and to ensure ongoing compliance with the Standards. For purposes of this Rule, the minimum Merchant monitoring Standards set forth in the Security Rules and Procedures manual apply with respect to Sub merchants.

1.37.5 Staged Digital Wallet Operator (SDWO) Program Service

A Staged Digital Wallet has a 2-stage payment process that is conducted to complete a purchase initiated by the cardholder: Funding stage - The Staged Digital Wallet Operator (DWO) uses the stored account information to take a payment from the cardholder

1.37.6 Digital Activity Service Provider (DASP) Program Service

An entity proposing to be a Digital Activity Service Provider must satisfy all certification and testing procedures established by the National Scheme Operator before such entity is registered by a Member as its Digital Activity Service Provider.

Digital Activity Service Provider (DASP) Program Service

- Account Enablement System
- Credentials Management System
- Transaction Management System
- Trusted Service Manager
- Any other service specified by the National Scheme Operator in its discretion from time to time.

1.37.7 Token Service Provider (TSP)

An entity proposing to be a Token Service Provider (TSP) must satisfy all certification and testing procedures established by the National Scheme before such entity is registered by a Member as its TSP.

المدفوعات للتجار من الباطن

يجب على كل مقدم خدمة دفع أن يدفع لكل تاجر من الباطن مقابل جميع المعاملات التي يقدمها مقدم خدمة الدفع إلى جهة القبول نيابة عن التاجر من الباطن. ولا تبرأ ذمته من الوفاء بهذا الالتزام فيما يتعلق بالمعاملة حتى يتلقى التاجر من الباطن الدفع من مقدم خدمة الدفع، وبغض النظر عن وجود ترتيبات للدفع بين التاجر من الباطن ومقدم خدمة الدفع، أو بين مقدم خدمة الدفع وجهة القبول.

يُسمح في عقد التاجر من الباطن أن ينص على أن لمقدم خدمة الدفع حجز مبالغ لاحتياطات رد المبالغ المدفوعة أو أغراض مماثلة.

توريد المواد إلى التجار من الباطن

يجب على كل مقدم خدمة دفع أن يضمن بانتظام تزويد كل من التجار من الباطن بجميع المواد اللازمة لتنفيذ المعاملات وفقاً للمعايير وللتأكيد على قبول البطاقة.

مراقبة التاجر من الباطن

يجب على كل مقدم خدمة دفع أن يراقب بشكل مستمر نشاط واستخدام العلامة الخاصة بكل من التجار من الباطن لغرض مكافحة الأنشطة الاحتيالية، وغيرها من الأنشطة غير المشروعة، ولضمان الامتثال المستمر للمعايير. لأغراض تطبيق هذه القاعدة، ينطبق الحد الأدنى من معايير مراقبة التاجر المنصوص عليها في دليل قواعد وإجراءات الأمان فيما يتعلق بالتجار من الباطن.

5.37.1 خدمة برنامج مشغل المحفظة الرقمية المرحلية

تحتوي المحفظة الرقمية المرحلية على عملية دفع من مرحلتين، يتم إجراؤها لإكمال عملية شراء بدأها حامل البطاقة: مرحلة التمويل - يستخدم مشغل المحفظة الرقمية المرحلية معلومات الحساب المخزنة لأخذ دفعة من حامل البطاقة.

6.37.1 خدمة برنامج مقدم خدمة النشاط الرقمي

يجب على الجهة التي تقترح أن يكون مقدم خدمة النشاط الرقمي، أن تفي بجميع إجراءات التصديق والاختبار التي وضعها مشغل شبكة الدفع المحلية، قبل أن يتم تسجيل هذه الجهة من قبل العضو كمقدم خدمة النشاط الرقمي.

خدمة برنامج مقدم خدمة النشاط الرقمي

- نظام تمكين الحساب.
- نظام إدارة أوراق الاعتماد.
- نظام إدارة المعاملات.
- مدير خدمة موثوق.
- أي خدمة أخرى يحددها مشغل شبكة الدفع المحلية وفقاً لتقديره من وقت لآخر.

7.37.1 مقدم خدمة الترميز

يجب على الجهة التي تطلب أن تكون مقدم خدمة ترميز، أن تفي بجميع إجراءات التصديق والاختبار التي وضعها مشغل شبكة الدفع المحلية، قبل أن يتم تسجيل هذه الجهة من قبل أحد الأعضاء باعتبارها مقدم خدمة الترميز الخاص به.

1.37.8 Merchant Monitoring Program (MMS) Program Service

Merchant Monitoring Program is the entity responsible for monitoring merchants behavior.

1.37.9 Terminal Servicer (TS) Program Service

A Terminal Servicer is an entity that provides ongoing maintenance and support of a payment terminal. Terminal Servicers access the merchant's transaction environment and equip the merchants with technologies that allow Scheme cardholders to pay with a variety of methods including magnetic stripe plastic cards, contactless, EMV chip-enabled cards, and a variety of mobile wallet applications. Terminal Servicers may also provide services that assist merchants with the administration of the point-of-sale (POS) systems and maintain compliance with PCI Standards.

1.37.10 3-D Secure Service Provider (3-DSSP) Program Service

A 3-D Secure Service Provider is a Service Provider that performs one or more of the services described in section 3.48 as 3-D Secure Program Service.

A 3-D Secure Service Provider adheres to the 3-D Secure protocol that is designed to offer an additional layer of security for online transactions. The protocol provides an authentication step prior to authorization. Authentication is based on the three-domain model which includes domains for the Issuer, Acquirer, and interoperability. The National Scheme Operator operates within the interoperability layer via its Directory Server (DS) which routes all 3-D Secure-enabled traffic to the appropriate Merchant and Issuer solutions for Cardholder authentication.

1.38 Member Use of Service Providers

(Category A as referenced in Book 1 Chapter 1)

A Member has the right to contract with Service Providers to assist it in its Card issuing or acquiring Activities. The Member must conduct appropriate due diligence prior to contracting a Service Provider. The Member retains full responsibility for its Card Programs and Activities and for the acts or omissions of its Service Providers.

A Member must conduct meaningful monitoring of its Service Providers to ensure their ongoing compliance with the Standards.

The Member must register each of its Service Providers with the National Scheme.

1.39 Confidential Information of Service Providers

With regard to any Service Provider, and regardless of (i) how it is categorized, (ii) the nature of services that it performs, and (iii) whether it is registered with the National Scheme, the following information is not confidential information:

1. The name, address and other contact information of the Service Provider;
2. The identity of any Member the National Scheme believes to be receiving services from the Service Provider;
3. The nature of services the National Scheme believes the Service Provider to be performing for any Member; and
4. Any information the National Scheme deems necessary or appropriate to disclose in order to safeguard the financial, reputational or other interests of the National Scheme Operator, Members, or both.

8.37.1 خدمة برنامج مراقبة التاجر

برنامج مراقبة التاجر هو الجهة المسؤولة عن مراقبة سلوك التاجر.

9.37.1 خدمة برنامج خدمة المحطة

تعتبر خدمة المحطة جهة توفر صيانة، ودعمًا مستمرين لمحطات الدفع. تصل المحطات إلى بيئة معاملات التاجر وتزود التاجر بالتقنيات التي تسمح لحاملي بطاقات النظام بالدفع بمجموعة متنوعة من الطرق بما في ذلك البطاقات البلاستيكية ذات الشريط المغناطيسي، وبطاقات الدفع عن بعد، والبطاقات الممكنة بشريحة EMV، ومجموعة متنوعة من تطبيقات المحفظة المحمولة. وقد توفر المحطات أيضًا خدمات تساعد التاجر في إدارة أنظمة نقاط البيع، والحفاظ على الامتثال لمعايير PCI.

10.37.1 خدمة برنامج مقدم الخدمة الآمنة ثلاثية الأبعاد

مقدم الخدمة الآمنة ثلاثية الأبعاد هو مقدم خدمة يؤدي خدمة أو أكثر من الخدمات الموضحة في القسم 3.48 كخدمة برنامج آمن ثلاثي الأبعاد.

يلتزم مقدم الخدمة الآمنة ثلاثية الأبعاد بالبروتوكول الآمن ثلاثي الأبعاد المصمم لتوفير طبقة إضافية من الأمان للمعاملات عبر الإنترنت. يوفر البروتوكول خطوة مصادقة قبل التفويض. وتعتمد المصادقة على نموذج المجالات الثلاثة الذي يتضمن نطاقات جهة الإصدار وجهة القبول وقابلية التشغيل البيئي. ويعمل مشغل شبكة الدفع المحلية ضمن طبقة التشغيل البيئي عبر خادم الدليل الذي يوجه جميع حركة المرور ثلاثية الأبعاد الممكنة الآمنة إلى طول التاجر وجهة الإصدار المناسبة لمصادقة حامل البطاقة.

38.1 استخدام الأعضاء لمقدمي الخدمة

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يحق للعضو التعاقد مع مقدمي الخدمة لمساعدته في نشاطات اصدار أو قبول البطاقات. ويجب على العضو بذل العناية المطلوبة قبل التعاقد مع مقدم الخدمة. ويتحمل العضو المسؤولية الكاملة عن برامج البطاقة، وأنشطته وعن تصرفات مقدمي الخدمة وأفعالهم.

يجب على العضو إجراء مراقبة حقيقية لمقدمي الخدمة لضمان امتثالهم المستمر للمعايير.

يجب على العضو تسجيل مقدمي الخدمة في شبكة الدفع.

39.1 المعلومات السرية لمقدمي الخدمة

فيما يتعلق بمقدم الخدمة، وبغض النظر عن (1) كيفية تصنيفه، (2) طبيعة الخدمات التي يؤديها. (3) ما إذا كان مسجلًا في شبكة الدفع، فإن المعلومات التالية لا تعد من قبيل المعلومات السرية:

1. الاسم والعنوان ومعلومات الاتصال الأخرى لمقدم الخدمة.
2. هوية العضو الذي يعتقد مشغل شبكة الدفع المحلية أنه يتلقى خدمات من مقدم الخدمة.
3. طبيعة الخدمات التي يعتقد مشغل شبكة الدفع المحلية أن مقدم الخدمة يؤديها لأي عضو.
4. أي معلومات يقدر مشغل شبكة الدفع المحلية أنها ضرورية أو مناسبة للإفصاح عنها من أجل حماية المصالح المالية، أو المتعلقة بالسمعة أو المصالح الأخرى لمشغل شبكة الدفع المحلية أو الأعضاء، أو كليهما.

1.40 Use of National Scheme Operator's Systems and Confidential Information

(Category A as referenced in Book 1 Chapter 1)

For purposes of this section, "the National Scheme Operator's Systems" means any of the National Scheme Operator's equipment and software and "the National Scheme Operator's Confidential Information" means any of the National Scheme Operator's information identified or reasonably understood to be confidential or proprietary.

A Service Provider must agree to:

1. Use any of the National Scheme Operator's Systems, including any connection to the Interchange System, and any of the National Scheme's Confidential Information, solely in order to perform service on behalf of the Member;
2. Treat the National Scheme Operator's Systems and Confidential Information in at least as careful and confidential.
3. Acknowledge that access to the National Scheme Operator's Systems and Confidential Information does not provide the Service Provider with any right to use them further;
4. Limit access to the National Scheme Operator's Systems and Confidential Information to those Service Provider employees with a need to have access in order to enable the Service Provider to perform service and to implement and to maintain reasonable and appropriate safeguards to prevent unauthorized access to the National Scheme Operator's Systems or disclosure of the National Scheme Operator's Confidential Information;
5. Immediately cease any use of the National Scheme Operator's Systems and Confidential Information upon request of the National Scheme Operator or the Member or upon the earlier of the termination or completion of the Service Provider's performance of service, and to immediately deliver all of the National Scheme Operator's Systems and Confidential Information to the National Scheme Operator; and
6. Immediately advise the Member and the National Scheme Operator if any unauthorized person seeks to gain or gains access to the National Scheme Operator's Systems or Confidential Information, whether by legal proceedings or otherwise.

The obligations set forth in this section survive the termination or expiration of the service agreement.

1.41 Other Service Providers (Non-Member)

The National Scheme Operator has the right to define other types of Service Providers and the requirements applicable to them.

Terminal Vendors

(Category A as referenced in Book 1 Chapter 1)

The National Scheme Operator issues for Members a list of certified Terminal vendors and will update the list from time to time. Only Terminals from certified vendors are permitted to be deployed.

A certified Terminal vendor is issued a compliance certification, which is subject to annual renewal provided the Terminal vendor remains in good standing.

40.1 استخدام أنظمة مشغل شبكة الدفع المحلية والمعلومات السرية

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

لأغراض تطبيق هذا القسم، تعني "أنظمة مشغل شبكة الدفع المحلية" أيًا من معدات وبرمجيات مشغل شبكة الدفع المحلية، وتعني "المعلومات السرية لمشغل شبكة الدفع المحلية" أيًا من معلومات مشغل شبكة الدفع المحلية المحددة أو التي يُفهم بشكل معقول أنها سرية أو مملوكة له. يجب أن يوافق مقدم الخدمة على:

1. استخدام أنظمة مشغل شبكة الدفع المحلية، بما في ذلك أي اتصال بنظام التبادل، وأي من المعلومات السرية لمشغل شبكة الدفع المحلية، فقط من أجل أداء الخدمة نيابة عن العضو.
2. التعامل مع أنظمة مشغل شبكة الدفع المحلية والمعلومات السرية على الأقل بحذر وسرية.
3. الإقرار بأن الوصول إلى أنظمة مشغل شبكة الدفع المحلية والمعلومات السرية لا يمنح مقدم الخدمة أي حق في استخدامها خارج هذا المجال.
4. تقييد الوصول إلى أنظمة مشغل شبكة الدفع المحلية والمعلومات السرية على موظفي مقدم الخدمة الذين يحتاجون إلى الوصول من أجل تمكين مقدم الخدمة من أداء الخدمة والتنفيذ والحفاظ على الضمانات المعقولة والمناسبة لمنع الوصول غير المصرح به إلى أنظمة مشغل شبكة الدفع المحلية أو الإفصاح عن المعلومات السرية لمشغل شبكة الدفع المحلية.
5. التوقف فورًا عن أي استخدام لأنظمة مشغل شبكة الدفع المحلية والمعلومات السرية بناءً على طلب مشغل شبكة الدفع المحلية أو العضو، أو عند إنهاء أو إكمال أداء مقدم الخدمة للخدمة في وقت سابق، وتقديم جميع أنظمة أو معلومات مشغل شبكة الدفع المحلية السرية، لمشغل شبكة الدفع المحلية على الفور.
6. إبلاغ العضو ومشغل شبكة الدفع المحلية على الفور إذا كان أي شخص غير مصرح له يسعى للحصول، أو الوصول إلى أنظمة مشغل شبكة الدفع المحلية أو المعلومات السرية، سواء عن طريق الإجراءات القانونية أو غير ذلك.

تظل الالتزامات المحددة في هذا القسم سارية بعد إنهاء عقد الخدمة أو انتهاء صلاحيتها.

41.1 مقدمو الخدمات الآخرون (غير الأعضاء)

لمشغل شبكة الدفع المحلية تحديد أنواع مقدمي الخدمة الآخرين والشروط المطلوبة فيهم .

باعة المحطات

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يُصدر مشغل شبكة الدفع المحلية، للأعضاء قائمة ببائعي المحطات المعتمدين، وسوف يقوم بتحديث القائمة بشكل دوري. ويُسمح فقط بنشر المحطات من البائعين المعتمدين.

ويتم إصدار شهادة امتثال لبائع المحطة المعتمد، والتي تخضع للتجديد السنوي، بشرط أن يظل بائع المحطة في وضع جيد.

1.42 Performing Program Service

Before an entity commences to perform Program Service that supports or benefits a Member's Program, the Member must verify that the entity is operating a bona fide business, has sufficient safeguards in place to protect Account and Transaction data from unauthorized disclosure or use, and complies with applicable laws; and cause such an entity to be registered by the National Scheme as a Service Provider.

A Service Provider has the right to perform only the type of Program Service that is registered to perform.

A corporate affiliate of a Member that is Owned and Controlled by the Member or by the Member's ultimate parent and which performs Program Service exclusively for the Member and not for any other Member is deemed not to be a Service Provider.

The Member must ensure that an entity performing Program Service that supports or benefits the Member's Program, and whether or not such entity is registered by the National Scheme Operator as a Service Provider:

1. Complies with all Standards applicable to the Program Service provided (including, by way of example and not limitation, data use and protection, confidentiality and privacy Standards) for so long as such entity performs such Program Service. This Member obligation arises and continues regardless of the nature of the Program Service performed and whether the entity is performing Program Service pursuant to an agreement or other arrangement with the Member, a Service Provider of the Member, or any other entity.
2. Promptly provides to the National Scheme Operator any information requested by the National Scheme pertaining to the Program Service or the performance thereof.
- 3.

Program Service in support of or benefitting a Participant Program is deemed to be Program Service in support of or benefitting the Program of the Principal that been affiliated with such Participant. A Participant wishing to receive Program Service from a Service Provider must obtain the prior written consent of the Participant's Principal member.

1.43 Member Responsibility and Control

(Category A as referenced in Book 1 Chapter 1)

The Member must at all times be entirely responsible for and must manage, direct, and control all aspects of its Program and Program Service performed by Service Providers, and establish and enforce all Program management and operating policies in accordance with the Standards.

A Member must not transfer or assign any part of such responsibilities or in any way limit its responsibility with regard to any of its Service Providers. A Member must conduct meaningful monitoring of its Service Providers to ensure ongoing compliance by its Service Providers with the Standards.

1.44 Notification to the National Scheme

(Category A as referenced in Book 1 Chapter 1)

Each Member must advise the National Scheme promptly when any of its Service Providers or any of its Sponsored Participants' Service Providers ceases to perform Program Service in connection with the Member's or Participant's Program or undergoes a change of name or transfer of Ownership or Control.

42.1 أداء خدمة البرنامج

قبل أن تبدأ الجهة في أداء خدمة البرنامج التي تدعم برنامج العضو أو تفيده، يجب على العضو التحقق من أن هذه الجهة تدير نشاطًا تجاريًا بحسن نية، ولديها ضمانات كافية لحماية بيانات الحساب والمعاملات من الإفصاح أو الاستخدام غير المصرح به، وتخضع للقوانين المعمول بها؛ والتسبب في تسجيل مثل هذه الجهة من قبل مشغل شبكة الدفع المحلية كمقدم خدمة.

لمقدم الخدمة الحق في أداء نوع خدمة البرنامج المسجل للأداء فقط.

شركة تابعة لعضو مملوك ومسيطر عليه من قبل العضو أو الأصل النهائي للعضو والذي يؤدي خدمة البرنامج حصريًا للعضو، وليس لعضو آخر لا يعتبر مقدم خدمة.

يجب على العضو التحقق من أن الجهة التي تؤدي خدمة البرنامج التي تدعم أو تفيد برنامج العضو، وما إذا كانت هذه الجهة مسجلة أم لا بواسطة مشغل شبكة الدفع المحلية كمقدم خدمة:

1. تخضع لجميع المعايير المطبقة على خدمة البرنامج المقدمة (بما في ذلك، على سبيل المثال، استخدام البيانات والحماية ومعايير السرية والخصوصية) طالما أن هذه الجهة تؤدي خدمة البرنامج. وينشأ التزام العضو ويستمر بغض النظر عن طبيعة خدمة البرنامج التي يتم تنفيذها، وما إذا كانت الجهة تؤدي خدمة البرنامج وفقًا لاتفاق أو ترتيب آخر مع العضو أو مقدم خدمة العضو أو أي جهة أخرى.

2. تزويد مشغل شبكة الدفع المحلية على الفور بالمعلومات التي يطلبها، فيما يتعلق بخدمة البرنامج أو أدائها.

تعتبر خدمة البرنامج التي تدعم أو تستفيد من برنامج مشترك، بمثابة خدمة برنامج لدعم أو الاستفادة من برنامج المسؤول المنتسب إلى هذا المشارك. ويجب على المشارك الذي يرغب في تلقي خدمة البرنامج من مقدم الخدمة، الحصول على موافقة كتابية مسبقة من العضو المسؤول عن العضو المشارك.

43.1 مسؤولية العضو وتحكمه

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب أن يكون العضو مسؤولًا مسؤولية كاملة في جميع الأوقات، ويجب عليه إدارة وتوجيه ومراقبة جميع جوانب البرنامج، وخدمة البرنامج التي يقوم بها مقدمو الخدمة، وإنشاء وتنفيذ جميع سياسات إدارة البرامج، وتشغيلها وفقًا للمعايير.

يجب على العضو عدم نقل، عدم الاتفاق على الحد من المسؤولية أو الاعفاء مع مقدمي الخدمة. ويجب على العضو إجراء مراقبة حقيقية لمقدمي الخدمة، لضمان امتثالهم المستمر للمعايير.

44.1 إخطار الشبكة المحلية

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على كل عضو إخطار مشغل شبكة الدفع المحلية، على الفور، عندما يتوقف أحد مقدمي الخدمة أو أي من مقدمي خدمة المشاركين المكفولين عن أداء خدمة البرنامج، فيما يتعلق ببرنامج العضو أو المشارك أو يخضع لتغيير الاسم أو نقل الملكية أو التحكم.

Each Type TPP must advise the National Scheme Operator promptly in writing when it:

1. Commences to perform or ceases to perform any Program Service for any Member, and on an ongoing basis, inform the National Scheme Operator of all Member ID numbers pertaining to which it is performing any Program Service;
2. Undergoes a change of name or transfer of Ownership or Control;
3. Fails or refuses to make payments in the ordinary course of business;
4. Makes an assignment for the benefit of creditors; or
5. Seeks bankruptcy protection or similar protection.

A Member must not receive Program Service from any other entity or person unless otherwise provided in the Standards.

1.45 Disclosure of Standards

(Category A as referenced in Book 1 Chapter 1)

Before a Member proposes an entity to be registered as a Service Provider by the National Scheme Operator, the Member must provide or ensure the proposed Service Provider has access to the Standards then in effect applicable to Service Providers and Program Service the proposed Service Provider is expected to perform. After registration, the Member must provide, or ensure a Service Provider is notified of, any change to the Standards applicable to such Program Service.

1.46 Member Point of Contact

(Category A as referenced in Book 1 Chapter 1)

A Service Provider must promptly provide a name and title of, and a telephone number for an employee of the Member upon request by a Cardholder, or if the Service Provider is unable or unwilling to respond to a question to the Cardholder's satisfaction.

1.47 Use of the Brand

(Category A as referenced in Book 1 Chapter 1)

A Service Provider must not use the NUMO Brand on its own behalf, whether in connection with Program Service or otherwise. The Service Provider must not create an impression that the Service Provider is a Member or a representative of the National Scheme Operator. A Service Provider must not create an impression that the National Scheme Operator in any way endorses the Service Provider or the Program Service that the Service Provider performs.

A Service Provider has the right to use one or more of the Brand in connection with the Program Service it performs, provided:

1. The Brand is used in accordance with the Standards, including all current reproduction, usage and artwork Standards; and
2. The Brand is used according to the express written instructions of the Member; and
3. The Brand is used solely in connection with the provision of Program Service.

يجب على كل مقدم طرف ثالث إخطار مشغل شبكة الدفع المحلية كتابةً على الفور عندما:

1. يبدأ في أداء، أو التوقف عن أداء خدمة برنامج العضو، وعلى أساس مستمر، إخطار مشغل شبكة الدفع المحلية بجميع أرقام تعريف العضو المتعلقة بأداء خدمات أي برنامج.
2. يخضع لتغيير الاسم أو نقل الملكية أو التحكم.
3. يفشل أو يرفض سداد المدفوعات في سياق العمل العادي.
4. يجعل التنازل لصالح الدائنين.
5. يسعى للحماية من الإفلاس أو حماية مماثلة.

يجب ألا يتلقى العضو خدمة البرنامج من أي كيان أو شخص آخر ما لم ينص على خلاف ذلك في المعايير.

45.1 الإفصاح عن المعايير

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

قبل أن يقترح العضو جهةً ليتم تسجيلها كمقدم خدمة من قبل مشغل شبكة الدفع المحلية، يجب عليه التحقق من أن مقدم الخدمة المقترح لديه حق الوصول إلى المعايير التي تنطبق في الواقع على مقدمي الخدمة وخدمة البرنامج، المتوقع أن يقوم مقدم الخدمة المقترح بأدائها بعد التسجيل ، ويجب كذلك على العضو تقديم أو ضمان إخطار مقدم الخدمة بأي تغيير في المعايير المطبقة على خدمة البرنامج.

46.1 نقطة اتصال العضو

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على مقدم الخدمة أن يقدم على الفور اسمًا ولقبًا ورقم هاتف لأحد موظفي العضو، بناءً على طلب حامل البطاقة، أو إذا كان مقدم الخدمة غير قادر أو غير راغب في الرد على سؤال يرضي حامل البطاقة.

47.1 استخدام العلامة التجارية

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب ألا يستخدم مقدم الخدمة علامة نمو التجارية نيابة عنه، سواء فيما يتعلق بخدمة البرنامج أو غير ذلك. ويجب ألا يترك مقدم الخدمة انطباعًا بأن مقدم الخدمة عضو أو ممثل لمشغل شبكة الدفع المحلية.

يجب ألا يترك مقدم الخدمة انطباعًا بأن مشغل شبكة الدفع المحلية يؤيد بأي شكل من الأشكال مقدم الخدمة أو خدمة البرنامج التي يؤديها مقدم الخدمة.

يحق لمقدم الخدمة استخدام علامة تجارية واحدة أو أكثر فيما يتعلق بخدمة البرنامج التي يؤديها، شريطة:

1. يتم استخدام العلامة التجارية وفقًا للمعايير، بما في ذلك جميع معايير النسخ والاستخدام والأعمال الفنية الحالية.
2. يتم استخدام العلامة التجارية وفقًا للتعليمات المكتوبة الصريحة للعضو.
3. تُستخدم العلامة التجارية فقط فيما يتعلق بتوفير خدمة البرنامج.

1.48 Service Provider Identification on a Card

(Category A as referenced in Book 1 Chapter 1)

The name of a non-Member Service Provider is permitted on a Card only if that Service Provider does not perform acquiring Program Service in connection with any Member Program.

1.49 Program Materials

(Category A as referenced in Book 1 Chapter 1)

A Member must approve all Program documents before distribution by a Service Provider. The Program materials must not imply that the Service Provider is participating in any activity not permitted by the Standards. Program materials include, by way of example, Card applications, , Cardholder agreements, Cardholder statements, marketing materials, and Cardholder Communications, including Solicitations.

1.50 Fees

(Category A as referenced in Book 1 Chapter 1)

The Service Provider must not attempt to collect any fee associated with the Member's Program without the prior written approval of the Member. Any fee must be clearly disclosed in writing to the Merchant or Card applicant prior to any request for payment of the fee.

1.51 Settlement Failure Obligation

(Category A as referenced in Book 1 Chapter 1)

A Service Provider that becomes aware of a settlement failure by the Members for which the Service Provider performs Program Service must promptly, and in no event later than 24 hours after becoming aware of such failure, notify the National Scheme Operator in writing of such failure.

1.52 Data Security

(Category A as referenced in Book 1 Chapter 1)

A Service Provider must comply with all Standards pertaining to the storage, safeguarding, and/or transmission of Account and Transaction data.

If a Service Provider reasonably believes that an unauthorized person accessed or might have accessed Account, Cardholder, or Transaction data in the possession or control of the Service Provider or any other third party, the Service Provider must promptly notify each Member for which it provides Program Service in writing of such belief and the Member must promptly notify the National Scheme Operator in writing of such belief.

1.53 Access to Merchant Account

(Category A as referenced in Book 1 Chapter 1)

A Service Provider must not have access to any account for funds due to a Merchant or withheld from a Merchant for chargebacks, with the exception of Payment Service Providers, as set forth above. A Member must not assign or transfer to a Service Provider an obligation to pay or reimburse a Merchant if the obligation arises from Activity.

48.1 تحديد هوية مقدم الخدمة على البطاقة

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

لا يُسمح بوضع اسم مقدم الخدمة غير العضو على البطاقة إلا إذا لم يقدم مقدم الخدمة هذا بالحصول على خدمة البرنامج فيما يتعلق بأي برنامج عضو.

49.1 مواد البرنامج

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب أن يوافق العضو على جميع مستندات البرنامج قبل التوزيع من قبل مقدم الخدمة. ويجب ألا تشير مواد البرنامج إلى أن مقدم الخدمة يشارك في نشاط لا تسمح به المعايير. وتشمل مواد البرنامج، على سبيل المثال، تطبيقات البطاقات، واتفاقيات حامل البطاقة، وبيانات حامل البطاقة، والمواد التسويقية، واتصالات حامل البطاقة، بما في ذلك العطاءات.

50.1 الرسوم

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب ألا يحاول مقدم الخدمة تحصيل أي رسوم مرتبطة ببرنامج العضو دون الحصول على الموافقة المكتوبة المسبقة من العضو. ويجب الإفصاح عن أي رسوم بطريقة مكتوبة وواضحة للتاجر أو مقدم طلب البطاقة قبل أي طلب لدفع الرسوم.

51.1 فشل التسوية

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على مقدم الخدمة الذي يدرك فشل التسوية من قبل الأعضاء الذين يؤدي مقدم الخدمة من أجلهم خدمة البرنامج على الفور، وفي موعد لا يتجاوز 24 ساعة بعد علمه بهذا الفشل، إخطار مشغل شبكة الدفع المحلية كتابيًا بهذا الفشل.

52.1 أمن البيانات

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على مقدم الخدمة الامتثال لجميع المعايير المتعلقة بتخزين و/أو حماية و/أو نقل بيانات الحساب والمعاملات.

إذا كان مقدم الخدمة يشتبه بشكل معقول أن شخصًا غير مصرح له، قد تمكن من الوصول إلى بيانات الحساب أو حامل البطاقة أو المعاملة أو يكون قد تمكن من الوصول إليها في حوزة أو سيطرة مقدم الخدمة أو أي طرف ثالث، فيجب على مقدم الخدمة أن يقوم بطريقة كتابية على الفور بإخطار كل عضو يقدم البرنامج نيابة عنه بحالة الاشتباه، ويجب على العضو إخطار مشغل شبكة الدفع المحلية كتابيًا على الفور بهذا الاشتباه.

53.1 الوصول إلى حساب التاجر

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب ألا يكون لدى مقدم الخدمة حق الوصول إلى حسابات الأموال المستحقة للتاجر أو تم حجبها من التاجر لرد المبالغ المدفوعة، باستثناء مقدمي خدمة الدفع، على النحو المبين أعلاه. ويجب على العضو ألا يكلف أو ينقل إلى مقدم الخدمة التزامًا بالدفع أو التعويض للتاجر إذا نشأ الالتزام عن النشاط.

1.54 Acquiring Programs

Only the National Scheme operator within its' license and given rights, has the right to perform the acquiring services. Except for the Merchant agreement that will be the responsibility of the acquirer as a delegated service.

Acquiring functions introduced by the National Scheme Operator covers POS acceptance as well as Electronic Commerce services include operating the payment gateway, and any digital money acceptance services, all eCommerce and digital services are covered in “Book 3 Technical Operational Standards Chapter 4 eCommerce & Digital Services”.

1.55 Merchant Agreement

(Category A as referenced in Book 1 Chapter 1)

The Merchant Agreement establishing the terms of an acquiring relationship between the Acquirer and a Merchant must:

1. Be signed by the Member with no separate or other agreement between the Service Provider and the Merchant regarding Activity. The Service Provider has the right to be a party to the Merchant Agreement, in which case the Merchant Agreement must contain the substance of all of the following:
 - a. For purposes of the Merchant Agreement and performance of the Merchant Agreement by the Service Provider, (i) the Service Provider is the exclusive Service Provider of the Member; (ii) the Member is entirely responsible for, and in control of, Service Provider performance; and (iii) the Member must approve, in advance, any fee payable to or obligation of the Merchant arising from or related to performance of the Merchant Agreement.
 - b. The Merchant Agreement is not effective and must not be modified in any respect without the express written agreement of the Member.
 - c. The Service Provider must not have access, directly or indirectly, to any account for funds or funds due to a Merchant and/or funds withheld from a Merchant for chargebacks arising from, or related to, performance of this Merchant Agreement. The Member must not assign or otherwise transfer an obligation to pay or reimburse a Merchant arising from, or related to, performance of the Merchant Agreement to a Service Provider.
 - d. The Service Provider must not subcontract, sublicense, assign, license, franchise, or in any manner extend or transfer to any third party, any right or obligation of the Service Provider set forth in the Merchant Agreement. The Member must not waive, forgive, release, assign, or fail to insist on strict performance of each requirement set forth in these parts 1 through 4.
2. Confirm the Member's responsibility for the Program and for the Merchant's Program participation and confirm that the Merchant Agreement does not contain any provision that could be deemed to limit such responsibility.
3. Not take effect or state or imply that it takes or has taken effect prior to being signed by the Member.
4. Disclose the Member's name and sufficient information to enable the Merchant to contact the Member directly by telephone or in writing.

54.1 قبول البرامج

يحق فقط لمشغل شبكة الدفع المحلية ضمن ترخيصه وحقوقه الممنوحة، أداء خدمات القبول. باستثناء عقد التاجر الذي سيكون من مسؤولية جهة القبول باعتبار هذه الخدمة مخولٌ بأدائها .

تغطي وظائف القبول التي يقدمها مشغل شبكة الدفع المحلية قبول نقاط البيع، بالإضافة إلى خدمات التجارة الإلكترونية التي تشمل إدارة بوابة الدفع وخدمات قبول نقود رقمية، وجميع خدمات التجارة الإلكترونية والخدمات الرقمية مشمولة في “الكتاب 3 معايير التشغيل التقنية ، الفصل 4 التجارة الإلكترونية والخدمات الرقمية”.

55.1 عقد (اتفاقية) التاجر

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

عقد التاجر الذي يحدد شروط علاقة القبول بين جهة القبول والتاجر يجب أن:

1. يتم التوقيع عليه من قبل العضو بدون أي عقد منفصل، أو عقد آخر بين مقدم الخدمة والتاجر فيما يتعلق بالنشاط. ويحق لمقدم الخدمة أن يكون طرفًا في عقد التاجر، وفي هذه الحالة يجب أن يحتوي عقد التاجر على كل ما يلي:
 - أ. لأغراض عقد التاجر وأداء عقد التاجر من قبل مقدم الخدمة: (1) مقدم الخدمة هو مقدم الخدمة الحصري للعضو. (2) يكون العضو مسؤولًا بالكامل عن أداء مقدم الخدمة والتحكم فيه. (3) يجب أن يوافق العضو مقدمًا على أي رسوم واجبة الدفع أو من التزام التاجر الناشئة عن أو المتعلقة بأداء عقد التاجر.
 - ب. عقد التاجر ليس ساري، ويجب عدم تعديله بأي شكل من الأشكال دون موافقة كتابية صريحة من العضو.
 - ت. يجب ألا يكون لمقدم الخدمة حق الوصول، بشكل مباشر أو غير مباشر، إلى أي حساب للأموال أو الأموال المستحقة للتاجر و/أو الأموال المحتجزة من التاجر لرد المبالغ المدفوعة الناشئة عن، أو المتعلقة بأداء عقد التاجر هذا. ويجب على العضو عدم النقل أو التنازل بأي طريقة عن التزام بالدفع أو التعويض للتاجر عن إلتزام ناشئ عن، أداء عقد التاجر، مع مقدم الخدمة.
 - ث. يجب ألا يقوم مقدم الخدمة بالتعاقد من الباطن أو الترخيص من الباطن أو التنازل أو الترخيص أو الامتياز، بأي شكل من الأشكال نقل الحق أو التزام لمقدم الخدمة منصوص عليه في عقد التاجر إلى أي طرف ثالث. ويجب على العضو ألا يتنازل أو يعفو عن أو يطلق أو يعين أو يتوانى في التشديد على الأداء الصارم لكل مطلب منصوص عليه في هذه الأجزاء من 1 إلى 4.

2. تأكيد مسؤولية العضو عن البرنامج، ومشاركة برنامج التاجر وتأكيد أن عقد التاجر لا يحتوي على أي بند يمكن اعتباره يحد من المسؤولية.
3. لا يدخل حيز التنفيذ ولا يذكر أو يشير ضمناً إلى أنه ساري المفعول أو أصبح ساري المفعول قبل أن يوقعها العضو.
4. الإفصاح عن اسم العضو والمعلومات الكافية، لتمكين التاجر من الاتصال بالعضو مباشرة بواسطة الهاتف أو في مراسلة مكتوبة.

1.56 Collection of Funds from a Merchant

(Category A as referenced in Book 1 Chapter 1)

Discount rates (or similar charges called by other terms) due to a Member from a Merchant must be collected directly by the Member and not by a Service Provider.

1.57 Access to Documentation

(Category A as referenced in Book 1 Chapter 1)

The Member at all times must maintain prompt and unrestricted physical access to all original, executed Merchant Agreements and ATM Owner Agreements and to completed Merchant and ATM site inspection reports. The Member must forward true and complete copies of any one or more of these documents to the National Scheme Operator promptly upon request.

1.58 Authority to Terminate Merchant Agreement

(Category A as referenced in Book 1 Chapter 1)

A Member must not limit or in any manner condition its authority to terminate any Merchant Agreement or ATM Owner Agreement to accommodate a Service Provider or otherwise.

1.59 Issuing Programs

Each Member and each Service Provider that performs Program Service with respect to that Member's issuing Programs must comply with all of the following:

Card Application Approval

(Category A as referenced in Book 1 Chapter 1)

The Member itself, and not a Service Provider, must approve the application of a person to participate as a Cardholder in the Member's Card Program.

Cardholder Agreement

(Category B as referenced in Book 1 Chapter 1)

The Cardholder agreement must disclose the Member's name and sufficient information to enable the Cardholder to contact the Member directly by telephone or in writing. The Service Provider must not be a party to the Cardholder agreement.

Program Payments

(Category A as referenced in Book 1 Chapter 1)

All Program payments other than Card application fees paid by prospective Cardholders must be collected directly by the Member and not by the Service Provider.

Program Receivables

A Service Provider is permitted to own Program receivables or participate in a financing vehicle involving such receivables so long as the National Scheme Operator determines that the Member continues to own and control the Program. Ownership of such receivables by the Service Provider does not in any way limit the Member's obligation to comply with the Standards.

56.1 تحصيل الأموال من التاجر

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب أن يتم تحصيل معدلات الخصم (أو الرسوم المماثلة التي تسمى بمصطلحات أخرى) المستحقة للعضو من التاجر مباشرة، من قبل العضو، وليس بواسطة مقدم الخدمة.

57.1 الوصول إلى الوثائق

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على العضو وفي جميع الأوقات الالتزام بالحفاظ على الوصول المادي الفوري وغير المقيد إلى جميع اتفاقيات التاجر الأصلية والمنفذة، واتفاقيات مالك أجهزة الصراف الآلي وتقارير فحص موقع التاجر وأجهزة الصراف الآلي المكتملة. ويجب على العضو إرسال نسخ صحيحة وكاملة إلى مشغل شبكة الدفع المحلية على الفور عند الطلب.

58.1 سلطة إنهاء عقد (اتفاقية) التاجر

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على العضو عدم تقييد سلطته، أو تعليقها على شرط بأي شكل من الأشكال لإنهاء أي عقد أي تاجر، أو اتفاقية مع مالك ماكينة الصراف الآلي لاستيعاب مقدم الخدمة أو غير ذلك.

59.1 إصدار البرامج

يجب على كل عضو، وكل مقدم خدمة يؤدي خدمة البرنامج فيما يتعلق ببرامج إصدار ذلك العضو الامتثال لجميع ما يلي:

الموافقة على طلب البطاقة

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على العضو نفسه، وليس مقدم الخدمة، الموافقة على طلب شخص، للمشاركة كحامل بطاقة في برنامج بطاقة العضو.

عقد (اتفاقية) حامل البطاقة

(الفئة ب كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب أن يكشف عقد حامل البطاقة عن اسم العضو، والمعلومات الكافية لتمكين حامل البطاقة من الاتصال بالعضو مباشرة، عبر الهاتف أو كتابيًا. ويجب ألا يكون مقدم الخدمة طرفًا في عقد حامل البطاقة.

مدفوعات البرنامج

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب تحصيل جميع مدفوعات البرنامج، بخلاف رسوم طلب البطاقة التي يدفعها حاملو البطاقات المحتملون مباشرة من قبل العضو، وليس بواسطة مقدم الخدمة.

ذمم البرنامج

يُسمح لمقدم الخدمة بامتلاك مستحقات البرنامج، أو المشاركة في وسيلة تمويل تتضمن مثل هذه المستحقات، طالما أن مشغل شبكة الدفع المحلية يقرر أن العضو لا يزال يمتلك البرنامج ويتحكم فيه. إن ملكية هذه المستحقات من قبل مقدم الخدمة لا يحد بأي شكل من الأشكال من التزام العضو بالامتثال للمعايير.

1.60 Registration Requirements for Payment Service Providers

(Category A as referenced in Book 1 Chapter 1)

To propose a Service Provider for registration as a Payment Service Provider, the Acquirer must be a Member in good standing with the National Scheme Operator and meet any and all capital requirements imposed by the National Scheme Operator.

To register a Service Provider as a Payment Service Provider, the Acquirer must:

1. Submit all information and material required by the National Scheme Operator in connection with the proposed registration within 30 days of the registration application submission date; and
2. Ensure that the Payment Service Provider is compliant with the PCI Data Security Standard. For any proposed Payment Service Provider that is not compliant, the National Scheme Operator must be provided with, and approve of, a compliance action plan. The application of a Payment Service Provider will not be approved until such time as the Payment Service Provider becomes fully compliant with the requirements;
3. Pay any fee that the National Scheme Operator imposes.

The Acquirer must receive the National Scheme Operator’s written or email confirmation of the registration before the Acquirer submits Transactions from the Payment Service Provider or any of its Sub merchants into interchange. In its sole discretion, the National Scheme Operator has the right to approve or reject any application for the registration of a Payment Service Provider.

To maintain the registration of a Payment Service Provider, the Member must submit such information and material as is required by the National Scheme Operator from time to time, including but not limited to a copy of the agreement between the Acquirer and the Payment Service Provider. Any renewal fee then in effect must be paid. In its sole discretion, the National Scheme Operator has the right to decline to renew the registration of a Payment Service Provider.

If the Acquirer ceases to accept Sub merchant Transactions from or terminates a Payment Service Provider, the Acquirer must notify the National Scheme Operator of the date and reasons for such action within one week of the decision. In its sole discretion, the National Scheme Operator has the right to require an Acquirer to cease to accept Sub merchant Transactions from a Payment Service Provider at any time.

1.61 Registration Requirements for Token Service Providers

(Category A as referenced in Book 1 Chapter 1)

Each Principal, for itself and each of its Sponsored Participants must register a Token Service Provider (TSP). The following requirements apply:

1. The Member must submit all information and material required by the National Scheme Operator in connection with the proposed registration within 60 days of the registration application submission date.
2. The proposed TSP must successfully complete all certification and testing procedures required by the National Scheme Operator.
3. The National Scheme Operator collects the applicable fee then in effect from the Member that proposes the registration.

60.1 متطلبات التسجيل لمقدمي خدمات الدفع

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

لتسجيل مقدم الخدمة كمقدم خدمة دفع، يجب أن يكون القابل عضوًا في وضع جيد مع مشغل شبكة الدفع المحلية، وأن يفي بجميع متطلبات رأس المال التي يفرضها مشغل شبكة الدفع المحلية. ولتسجيل مقدم الخدمة، كمقدم خدمة الدفع، يجب على جهة القبول القيام بالخطوات التالية:

1. تقديم جميع المعلومات والمواد التي يطلبها مشغل شبكة الدفع المحلية فيما يتعلق بالتسجيل المقترح، خلال 30 يومًا من تاريخ تقديم طلب التسجيل.

2. التحقق من أن مقدم خدمة الدفع متوافق مع معيار أمان بيانات PCI. وإذا كان مقدم الخدمة المقترح غير متوافق مع هذا المعيار، فيجب أن تقدم لمشغل شبكة الدفع المحلية خطة عمل لامثال مقدم الخدمة، والموافقة عليها. ولن تتم الموافقة على طلب مقدم خدمة الدفع حتى يصبح مقدم خدمة الدفع متوافقًا تمامًا مع المتطلبات.

3. دفع الرسوم التي يفرضها مشغل شبكة الدفع المحلية.

يجب أن تتلقى جهة القبول تأكيدًا مكتوبًا، أو بالبريد الإلكتروني من مشغل شبكة الدفع المحلية للتسجيل، وذلك قبل أن تقدم جهة القبول المعاملات من مقدم خدمة الدفع أو من التجار من الباطن التابعين له للتبادل. وتخضع الموافقة على طلب التسجيل للسلطة التقديرية لمشغل شبكة الدفع المحلية. فله الموافقة على الطلب أو رفضه.

للحفاظ على تسجيل مقدم خدمة الدفع، يجب على العضو تقديم هذه المعلومات والمواد كما هو مطلوب من قبل مشغل شبكة الدفع المحلية من وقت لآخر، بما في ذلك على سبيل المثال: نسخة من الاتفاق بين جهة القبول ومقدم خدمة الدفع. ويجب دفع رسوم تجديد سارية المفعول . وفقًا لتقديره ، لمشغل شبكة الدفع المحلية الحق في رفض أو تجديد تسجيل مقدم خدمة الدفع.

إذا توقفت جهة القبول عن قبول معاملات التاجر من الباطن من مقدم خدمة الدفع أو إنهاؤها، فيجب على جهة القبول إخطار مشغل شبكة الدفع المحلية بتاريخ وأسباب هذا الإجراء خلال أسبوع واحد من القرار. وفقًا لتقديره ، يحق لمشغل شبكة الدفع المحلية أن يطلب من جهة القبول التوقف عن قبول معاملات التاجر من الباطن من مقدم خدمة الدفع في أي وقت.

61.1 متطلبات التسجيل لمقدمي خدمة الترميز

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

يجب على كل مسؤول، لنفسه ولكل من المشاركين المكفولين، تسجيل مقدم خدمة الترميز.و تطبيق المتطلبات التالية:

1. يجب على العضو تقديم جميع المعلومات، والمواد التي يطلبها مشغل شبكة الدفع المحلية فيما يتعلق بالتسجيل المقترح، خلال 60 يومًا من تاريخ تقديم طلب التسجيل.
2. يجب أن يستكمل مقدم خدمة الترميز المقترح بنجاح، جميع إجراءات التصديق والاختبار المطلوبة من قبل مشغل شبكة الدفع المحلية.
3. يقوم مشغل شبكة الدفع المحلية بتحصيل الرسوم المطبقة ثم السارية من العضو الذي يقترح التسجيل.

The Member must receive the National Scheme Operator's written confirmation of the registration before the Principal, or a Sponsored Participant receives Program Service from the proposed TSP or the proposed TSP commences performing such Program Service or represents itself to any person as authorized to provide such Program Service on behalf of the Principal, or a Sponsored Participant.

In its discretion, the National Scheme Operator has the right to approve or reject any application for the registration of a TSP.

To maintain the registration of a TSP, the Member must submit such information as is required by the National Scheme Operator. The registration renewal fee then in effect must be paid by the Member. In its discretion, the National Scheme Operator has the right to decline to renew the registration of a TSP.

If a Member terminates a TSP, the Member must notify the National Scheme Operator of the termination date and of the reasons for the termination. This notification must be received by the National Scheme Operator within one week of the decision to terminate. In its discretion, the National Scheme Operator has the right to require a Member to cease receiving TSP Program Service from a TSP at any time.

1.62 Audits

(Category A as referenced in Book 1 Chapter 1)

The National Scheme Operator or its designee has the right to conduct one or more regular or periodic financial and procedural audits of the Member, its Service Providers, or both, at any time and from time to time for the purpose of determining compliance with the Standards. The Member bears all costs of any such audit or audits. The Member and its Service Providers each must fully co-operate with and promptly supply the National Scheme Operator with all information and material upon request.

1.63 No Endorsement by the National Scheme Operator

In no event does compliance with these Service Provider Rules or enforcement or any lack of or delay in enforcement thereof or the registration of a Service Provider imply, suggest, or otherwise mean that the National Scheme Operator endorses any Service Provider or the nature or quality of Program Service or other performance or that the National Scheme Operator approves of, is a party to, or a participant in, any act or omission by a Service Provider or other entity acting for or on behalf of a Member.

يجب أن يتلقى العضو تأكيدًا كتابيًا من مشغل شبكة الدفع المحلية للتسجيل قبل المسؤول، أو أن يتلقى العضو المشارك المكفول خدمة البرنامج من مقدم خدمة الترميز المقترح، أو يبدأ مقدم خدمة الترميز المقترح في أداء خدمة البرنامج، أو يمثل نفسه لأي شخص مصرح له بتقديم خدمة البرنامج أو نيابة عن العضو المسؤول أو العضو المشارك المكفول.

لمشغل شبكة الدفع المحلية وطبقاً لسلطته التقديرية، الموافقة على طلب تسجيل مقدم خدمة الترميز، أو رفض طلب تسجيله.

للحفاظ على تسجيل مقدم خدمة الترميز، يجب على العضو تقديم هذه المعلومات كما هو مطلوب من قبل مشغل شبكة الدفع المحلية. يجب على العضو دفع رسوم تجديد التسجيل السارية المفعول، وتخضع الموافقة على طلب تجديد التسجيل للسلطة التقديرية لمشغل شبكة الدفع المحلية. فله الموافقة على الطلب أو رفضه.

إذا قام العضو بإنهاء مقدم خدمة الترميز، فيجب على العضو إخطار مشغل شبكة الدفع المحلية بتاريخ الإنهاء وأسباب الإنهاء. ويجب أن يستلم مشغل شبكة الدفع المحلية هذا الإخطار في خلال أسبوع واحد من قرار الإنهاء. وفقاً لسلطته التقديرية لمشغل شبكة الدفع المحلية أن يطلب من العضو التوقف عن تلقي خدمة برنامج مقدم خدمة الترميز من مقدم خدمة الترميز في أي وقت.

62.1 عمليات التدقيق

(الفئة أ كما هو مشار إليه في الكتاب 1 الفصل 1)

لمشغل شبكة الدفع المحلية أو من ينوب عنه إجراء عملية واحدة، أو أكثر من عمليات التدقيق المالية والإجرائية المنتظمة أو الدورية للعضو، أو مقدمي الخدمة أو كليهما، في جميع اللوقات، وذلك لغرض تحديد الامتثال للمعايير. ويتحمل العضو جميع تكاليف عملية التدقيق أو عمليات التدقيق. ويجب على كل من العضو ومقدمي الخدمة، أن يقدموا كافة أشكال المساعدة لمشغل شبكة الدفع المحلية، وأن يزودوه على الفور بجميع المعلومات والمواد عند الطلب.

63.1 عدم وجود مصادقة من قبل مشغل شبكة الدفع المحلية

لا يعني بأي حال من الأحوال ، الامتثال لقواعد مقدم الخدمة أو إنفاذها، أو أي نقص أو تأخير في إنفاذها، أو تسجيل مقدم الخدمة أن مشغل شبكة الدفع المحلية يؤيد مقدم الخدمة أو طبيعة أو جودة مقدم الخدمة أو أي أداء آخر يوافق عليه مشغل شبكة الدفع المحلية، أو يكون طرفاً، أو مشاركاً في، أي فعل أو إمتناع عن فعل من قبل مقدم الخدمة أو أي جهة أخرى تعمل لصالح العضو، أو نيابة عنه .

Regulatory Rules of The Libyan National Payment Scheme

Chapter 2 - NUMO Brand Usage

2.1 Right to Use National Scheme Brand “NUMO”

The right to use Libyan National Scheme brand can only be granted through a license given by the entity that is delegated from Central Bank of Libya. Any usage without obtaining the fore mentioned license is considered prohibited.

No additional benefits are granted with the usage permission of the National Payment Scheme brand. Licensee is responsible for all costs and liabilities arising from its use of the National Payment Scheme or associated exchange system logo.

The license is non-exclusive and non-transferable to a party other than the licensee. The licensee is allowed to use the brand of the National payment Scheme and can grant a sub-license to a licensed party to deal through the sub-license only, in accordance with the standards or with the clear written consent of the Payment Scheme Operator.

The Member or other authorized licensee to license the use of the NPS Logo of the sub-licensee shall, as long as the sub-license is in effect, ensure that the use of the National Payment Scheme Logo by the sub-licensee is in accordance with the Standards and/or other Additional Terms For this use required by the operator of the payment system.

The right to use the National Payment Scheme logo may not be granted without a license or assignment, whether through sale, consolidation, merging, merging, enforcement of law, or otherwise, without the prior written consent of the Payment Scheme Operator.

The Payment Scheme Operator makes no express or implied representations or warranties with respect to the National Payment Scheme Logo and the Payment Scheme Operator in particular, and rejects all such representations and warranties.

2.2 Brand Ownership, Reserving National Payment Scheme Rights

Reserving the rights of the National Payment Scheme brand is vital to the Central bank of Libya and delegates this right to NUMO, its members and other authorized persons. No use of the National Payment Scheme logo shall in any way degrade, devalue, defame, or cause damage or damage to the National Payment Scheme logo or the Payment Scheme Operator in any way.

By using the National Payment Scheme logo, each member and other licensee acknowledges that the Payment Scheme Operator is the exclusive owner and/or licensor of the National Payment Scheme logo, and agrees not to object to or assist others, either directly or indirectly, in objecting to the ownership of the Payment Scheme Operator alone for the National Payment Scheme logo, or to do or not to alert the Payment Scheme Operator of any action that may not be consistent with that property. Any use of the NPS logo will be of interest only to the Payment Scheme Operator.

القواعد التنظيمية لشبكة الدفع المحلية الليبية

الفصل 2 - استخدام علامة نمو التجارية 1.2 الحق في استخدام علامة شبكة الدفع المحلية نمو

لا يجوز منح الحق في استخدام علامة شبكة الدفع المحلية “نمو” إلا من خلال ترخيص يتم منحه من الجهة المفوضة من قبل مصرف ليبيا المركزي. ويُحظر استخدام العلامة دون الحصول على الترخيص المذكور.

لا يتم منح مزايا إضافية مع استخدام علامة شبكة الدفع المحلية “نمو”. ويعد المرخص له مسؤول عن جميع التكاليف، والالتزامات الناشئة عن استخدامه لشبكة الدفع المحلية، أو شعار نظام الصرف المرتبط به.

الترخيص غير حصري وغير قابل للتنازل أو النقل إلى طرف آخر عدا المرخص له. ويُسمح للمرخص له باستخدام علامة شبكة الدفع المحلية، ويجوز له منح ترخيص من الباطن لطرف مرخص للتعامل من خلال الترخيص من الباطن فقط، وفقاً للمعايير أو بعد الحصول على الموافقة الكتابية من مشغل شبكة الدفع المحلية.

يجب على العضو، أو المرخص له الآخر الذي يقوم بترخيص استخدام شعار شبكة الدفع المحلية للمرخص له من الباطن، طالما كان الترخيص من الباطن ساري المفعول، التحقق من أن استخدام علامة شبكة الدفع المحلية من قبل المرخص له من الباطن يتوافق مع المعايير والشروط الإضافية الأخرى لهذا الاستخدام المطلوب من قبل مشغل شبكة الدفع المحلية.

لا يجوز منح الحق في استخدام شعار شبكة الدفع المحلية، بدون الحصول على الترخيص أو التنازل، سواء من خلال البيع أو الدمج أو الإندماج أو إنفاذ القانون أو غير ذلك، دون الحصول على الموافقة الكتابية المسبقة من مشغل شبكة الدفع المحلية.

لا يقدم مشغل شبكة الدفع المحلية أي تعهدات أو ضمانات صريحة أو ضمنية، فيما يتعلق بشعار شبكة الدفع المحلية ومشغل شبكة الدفع المحلية على وجه الخصوص، ويرفض كل هذه التعهدات والضمانات.

2.2 ملكية العلامة التجارية، الاحتفاظ بحقوق شبكة الدفع المحلية

يعد الاحتفاظ بحقوق علامة شبكة الدفع المحلية أمراً ضرورياً بالنسبة لمصرف ليبيا المركزي، ويفوض هذا الحق لشبكة نمو وأعضائها والأشخاص المصرح لهم الآخرين. ولن يؤدي استخدام شعار شبكة الدفع المحلية بأي شكل من الأشكال، إلى التقليل من القيمة أو التشهير أو التسبب في تلف أو إتلاف شعار شبكة الدفع المحلية أو مشغل شبكة الدفع المحلية بأي شكل من الأشكال.

باستخدام شعار شبكة الدفع المحلية، يقر كل عضو والمرخص له الآخر بأن مشغل شبكة الدفع المحلية هو المالك الحصري و/أو المرخص لشعار شبكة الدفع المحلية، ويوافق على عدم الاعتراض على الآخرين أو مساعدتهم، سواء بشكل مباشر أو غير مباشر، في الاعتراض على ملكية مشغل شبكة الدفع المحلية وحده لشعار شبكة الدفع المحلية، أو القيام أو عدم تنبيه مشغل شبكة الدفع المحلية، بأي إجراء قد لا يكون متوافقاً مع تلك الملكية. سيكون أي استخدام لشعار شبكة الدفع المحلية ذا أهمية لمشغل شبكة الدفع المحلية فقط.

No member, licensee or other sub-licensee shall be permitted to register, or attempt to register, for the National Payment Scheme logo or to impose a provision which, in the opinion of the Payment scheme Operator, is derived from, similar to or in any way related to the National Payment Scheme logo. Specifically, the use of the National Payment Scheme logo on any card, device, or other application associated with a payment service that the Payment Scheme Operator and its representative considered to be a competition is not permitted.

In any way benefit from, but not limited to, the foregoing applies to the registration or use of the National Payment Scheme logo or an item containing references to otherwise that may be confused or associated with the National Payment Scheme logo currently or formerly licensed or sublicensed, or has been used by A member or an authorized or sublicensed member and its successors and affiliated parties, (including, without limitation, by merger or otherwise, bankruptcy or voluntary or involuntary liquidation).

The Central Bank of Libya is delegating his right to NUMO to determine, create and control the nature and quality of services rendered by its members under the emblem of the National Payment Scheme.

To preserve the integrity of the National Payment Scheme Logo and prevent irreparable harm to the Payment Scheme Operator, each Member agrees to stop using the National Payment Scheme Logo immediately upon receipt of a written request from the Payment System Operator, and agrees to introduce an injunction against its continued use.

If the Member is threatened with litigation or if sued in connection with any matter relating to the use of the National Payment Scheme logo, the Member shall immediately send written notice to the Payment Scheme Operator. The Payment Scheme Operator shall, in its sole discretion, have the right to defend, settle, or consent to the introduction of an injunction, judgment or ordinance to terminate any such litigation or permit such Member to do so.

2.3 Registration of a Card Design

A Member or other Licensee must not register or attempt to register any Card design that includes the National Payment Scheme Logo.

2.4 Misuse of the Brand

A Member or other Licensee must promptly notify the Payment Scheme Operator whenever the Member or other Licensee learns of any misuse of the brand or of any attempt to copy or infringe the brand.

2.5 Use or register similar logos, designs and names

A Member, Licensee, or Sub-licensee must not use or seek to register any logo, design, name, or decorative element that, in the opinion of the Payment Scheme Operator, is likely to cause confusion with, or create a false association, connection or affiliation with, or limit the features of the National Payment Scheme Mark or logo.

لا يجوز لأي عضو، أو مرخص له، أو غيره من المرخص لهم من الباطن التسجيل، أو محاولة التسجيل، في شعار شبكة الدفع المحلية، أو فرض شرط، يكون طبقاً للسلطة التقديرية لمشغل شبكة الدفع المحلية مشتق أو مشابه بأي طريقة لشعار شبكة الدفع المحلية. على وجه التحديد، لا يُسمح باستخدام شعار شبكة الدفع المحلية على أي بطاقة أو جهاز أو أي تطبيق آخر مرتبط بخدمة الدفع التي يعتبرها مشغل شبكة الدفع المحلية وممثلته منافسة.

الاستفادة بأي شكل من الأشكال، من التطبيقات السارية على التسجيل أو استخدام شعار شبكة الدفع المحلية أو أي عنصر يحتوي على إشارات قد يتم الخلط بينها أو ربطها بشعار شبكة الدفع المحلية حالياً أو مرخصاً سابقاً أو مرخصاً من الباطن، أو تم استخدامه من قبل عضو أو عضو مرخص له أو مرخص له من الباطن وخلفائه والأطراف التابعة له ، (بما في ذلك، على سبيل المثال لا الحصر، عن طريق الاندماج أو غير ذلك، الإفلاس أو التصفية الطوعية أو غير الطوعية).

يفوض مصرف ليبيا المركزي حقه في نمو لتحديد وإنشاء والتحكم في طبيعة وجودة الخدمات المقدمة من قبل أعضائه تحت شعار شبكة الدفع المحلية.

للمحافظة على سلامة شعار شبكة الدفع المحلية، ومنع حدوث ضرر لا يمكن إصلاحه لمشغل شبكة الدفع المحلية، يوافق كل عضو على التوقف عن استخدام شعار شبكة الدفع المحلية، فور استلام طلب كتابي من مشغل شبكة الدفع المحلية، ويوافق على إصدار أمر قضائي ضد استخدامه المستمر.

إذا تعرض العضو للتهديد بالتقاضي أو إذا تمت مقاضاته فيما يتعلق بأي مسألة تتعلق باستخدام شعار شبكة الدفع المحلية، فيجب على العضو إرسال إشعار كتابي على الفور إلى مشغل شبكة الدفع المحلية، ولمشغل شبكة الدفع المحلية، وفقاً لسلطته التقديرية، التدخل في الدعوى طبقاً للقواعد المنصوص عليها في قانون المرافعات، وله الحق في الدفاع أو طلب تسوية النزاع أو الموافقة على تقديم أمر قضائي أو (حكم مرسوم* تُلغى لعدم وجود مراسيم في ليبيا) لإنهاء أي دعوى قضائية من هذا القبيل أو السماح لهذا العضو بالقيام بذلك.

3.2 تسجيل تصميم البطاقة

يجب على العضو أو المرخص له الآخر عدم تسجيل، أو محاولة تسجيل أي تصميم لبطاقة يتضمن شعار شبكة الدفع المحلية.

4.2 إساءة استخدام العلامة التجارية

يجب على العضو أو المرخص له الآخر إخطار مشغل شبكة الدفع المحلية، على الفور متى علم العضو أو المرخص له الآخر بأي إساءة استخدام للعلامة التجارية أو أي محاولة لنسخ العلامة التجارية أو انتهاكها.

5.2 استخدام أو تسجيل شعارات وتصميمات وأسماء مماثلة

يجب على العضو أو المرخص له أو المرخص له من الباطن، عدم استخدام أو السعي إلى تسجيل أي علامة أو تصميم أو اسم أو عنصر زخرفي، يقدر مشغل شبكة الدفع المحلية أنه من المحتمل أن يسبب التباساً أو ينشئ رابطة أو ارتباطاً أو انتماءً مزيقاً، أو تقييد ميزات علامة أو شعار شبكة الدفع المحلية.

2.6 Terms and Conditions of Brand usage

We apply the following requirements to the use of the National Payment Scheme logo.

2.18 The use of the NPS logo is permitted only under license. This requirement applies, without limitation, to:

- Using the logo of the National Payment scheme for advertising or promotional purposes;
- Submit an application for the card balance or any other materials bearing the logo of the National Payment Scheme;
- Displaying the logo of the National Payment Scheme;
- Issuance of a card;
- the merchant's signature of a commercial agreement; And the
- Distribution or pasting of badges

Only the member or other licensee is allowed to use the logo of the National Payment Scheme to identify and promote the activity.

Any use of the NPS logo must comply with license terms and standards, including all standards for reproduction, use, and artwork of the National Scheme Operator relating to this mark.

The National Payments Scheme logo shall appear prominently in all advertising, marketing, promotional and side items promoting a program or service provided by the National Scheme Operator. The inclusion of the National Payment Scheme logo in the subheading or headline, or the prominent display of the National Payment Scheme logo on the first page of the solicitation satisfies this requirement. Each RFP must also include one or more of the following phrases, as applicable to the program or service being promoted: "National Payments Scheme" is the registered logo of [xxx].

2.7 Use of Multiple Logos

When promoting the National Payment Scheme Logo with another acceptance mark in any media to denote acceptance, no other acceptance mark, symbol or logo is permitted to be or appear to be larger or more important than or more welcomed than the National Payment Scheme Logo. No other acceptance mark is permitted to overlap or obscure the National Payment Scheme Logo in any way.

To maintain visual parity, the National Payment Scheme Logo must be at least as prominent as, and appear in at least the same frequency, size, and color treatment as, any other acceptance mark displayed. To maintain parity within written text, the National Payment Scheme Logo must be at least as prominent as, and appear at least as frequently as, any other acceptance mark mentioned.

2.8 Particular Uses of the National Payment Scheme Logo

A Member must comply with all of the following Standards regarding particular uses of the National Payment Scheme Logo.

6.2 شروط وأحكام استخدام العلامة التجارية

نطبق المتطلبات التالية على استخدام شعار شبكة الدفع المحلية.

18.2 يسمح باستخدام شعار شبكة الدفع المحلية فقط بموجب ترخيص. ينطبق هذا الشرط، على سبيل المثال لا الحصر، على:

- استخدام شعار شبكة الدفع المحلية لأغراض الدعاية أو الترويج.
- تقديم طلب للحصول على رصيد البطاقة أو أي مواد أخرى تحمل شعار شبكة الدفع المحلية.
- عرض شعار شبكة الدفع المحلية.
- إصدار بطاقة.
- توقيع التاجر لاتفاقية تجارية، و
- توزيع أو لصق الشارات.

يسمح فقط للعضو أو المرخص له باستخدام شعار شبكة الدفع المحلية لتحديد النشاط والترويج له.

أي استخدام لشعار شبكة الدفع المحلية يجب أن يمثل مع شروط ومعايير الترخيص، بما في ذلك جميع معايير النسخ والاستخدام والأعمال الفنية لمشغل شبكة الدفع المحلية المتعلقة بهذه العلامة.

يجب أن يظهر شعار شبكة الدفع المحلية بشكل بارز في جميع المواد الإعلانية والتسويقية والترويجية والجانبية التي تروج لبرنامج أو خدمة يقدمها مشغل شبكة الدفع المحلية. إن إدراج شعار شبكة الدفع المحلية في العنوان الفرعي أو العنوان الرئيسي، أو العرض البارز لشعار شبكة الدفع المحلية على الصفحة الأولى من الالتماس يفي بهذا المطلب. ويجب أن يتضمن كل RFP أيضًا واحدة أو أكثر من العبارات التالية، حسبما ينطبق على البرنامج أو الخدمة التي يتم الترويج لها: "شبكة المدفوعات المحلية" هو الشعار المسجل لـ [xxx].

7.2 استخدام شعارات (علامات) متعددة

عند الترويج لشعار شبكة الدفع المحلية بعلامة قبول أخرى في أي وسيط للإشارة إلى القبول، لا يُسمح أن تكون أي علامة قبول أو رمز أو شعار أخرى أو أن تظهر أكبر أو أكثر أهمية من شعار شبكة الدفع المحلية أو أكثر ترجيحًا بها. لا يُسمح لأي علامة قبول أخرى أن تتداخل أو تحجب شعار شبكة الدفع المحلية بأي شكل من الأشكال.

للحفاظ على التكافؤ البصري، يجب أن يكون شعار شبكة الدفع المحلية بارزًا على الأقل ويظهر بنفس التكرار والحجم ومعالجة الألوان على الأقل مثل أي علامة قبول أخرى معروضة. للحفاظ على التكافؤ في النص المكتوب، يجب أن يكون شعار شبكة الدفع المحلية بارزًا على الأقل مثل أي علامة قبول أخرى مذكورة، وأن يظهر على الأقل بشكل متكرر.

8.2 الإستخدامات المعينة لشعار شبكة الدفع المحلية

يجب على العضو الامتثال لجميع المعايير التالية فيما يتعلق بالإستخدامات المعينة لشعار شبكة الدفع المحلية.

2.8.1 Generic Use

A generic term, such as “bank card” or “payment card,” does not function as the Logo. Use of the National Payment Scheme Logo in a manner that would tend to genericize the National Payment Scheme Logo or otherwise result in the loss of trademark rights is prohibited.

2.8.2 Use of Modifiers

Subject to Payment System Operator approval, a Member is permitted to use its name or a geographical designation in conjunction with the National Payment Scheme Logo, such as “First Issuer National Payment Scheme card program” or “First Issuer National Payment Scheme Department.” The Payment System Operator has the right to prohibit the use of a modifier that it determines will impair the distinctiveness of the National Payment Scheme Logo or create any likelihood of confusion or reflect poorly on the Payment System Operator.

2.8.3 Use on Stationery

A Licensee is permitted to use the National Payment Scheme Logo on print or electronic stationery, letterhead, envelopes, and the like for the purpose of identifying its Program or service. If the National Payment Scheme Logo is used, the Licensee’s name must appear in close proximity to it, such as “National Bank National Payment Scheme® Department.”

2.8.4 Use of the National Payment Scheme Logo in Text

The National Payment Scheme Logo is permitted to be used as an adjective (as in “your National Payment Scheme card”) in the first or most prominent use subsequent to any use in the title, headline, signature, or cover page of an offering, unless:

1. The word “National Payment Scheme” is used as part of a Member’s Program name; or
2. Otherwise expressly approved in writing by the Payment System Operator.

Use of the word “National Payment Scheme” as a verb (“National Payment Scheme your gifts”), in plural (“National Payment Schemes”) or in possessive form (“National Payment Scheme’s”) is prohibited.

2.9 Use of Scheme Brand in Member Corporate Identity

The National Payment Scheme Logo must not be used as part of a legal, corporate, or business name, such as “National Payment Scheme® Center, Inc.” No Internet domain name is permitted to be registered that includes the word “National Payment Scheme,” except as expressly permitted in writing by the Payment System Operator.

2.10 Program Names

Each Program name, Solicitation, and service must be referred to by the full, legal name of the brand and include the appropriate registration notice.

2.11 Use of Product Branding

Product branding must not be used in a manner likely to create an impression that any product or service offered by a Licensee, Sub-licensee, or Merchant is sponsored, produced, offered, approved, sold by, or otherwise affiliated with the Payment System Operator. Each Licensee must ensure that each of its Sub-licensees, partners, Merchants, and other Program participants does not use the National Payment Scheme Logo to brand any product or service unless expressly authorized in writing by the Payment System Operator.

1.8.2 الاستخدام العام

المصطلح العام، مثل “بطاقة مصرفية” أو “بطاقة دفع”، لا يعمل كشعار. يُحظر استخدام شعار شبكة الدفع المحلية بطريقة تميل إلى تعميم شعار شبكة الدفع المحلية، أو تؤدي بطريقة أخرى إلى ضياع حقوق العلامة التجارية.

2.8.2 استخدام المعدلات

مع مراعاة “موافقة مشغل شبكة الدفع المحلية”، يُسمح للعضو باستخدام اسمه أو تعيينه الجغرافي جنبًا إلى جنب مع شعار شبكة الدفع المحلية ، مثل “برنامج بطاقة شبكة الدفع المحلية لجهة الإصدار الأولى” أو “إدارة شبكة الدفع المحلية لجهة الإصدار الأولى”. لمشغل شبكة الدفع المحلية حظر الاستخدام المُعدّل الذي يقرر أنه سيؤثر على تمييز شعار شبكة الدفع المحلية، أو يخلق أي احتمال للارتباك أو ينعكس بشكل سيء على مشغل شبكة الدفع المحلية.

3.8.2 استخدام القرطاسية

يُسمح للمرخص له باستخدام شعار شبكة الدفع المحلية على القرطاسية المطبوعة أو الإلكترونية والورق ذي الرأسية والأظرف وما شابه ذلك لغرض تحديد برنامج أو خدمته. في حالة استخدام شعار شبكة الدفع المحلية، يجب أن يظهر اسم المرخص له بالقرب منه، مثل “إدارة شبكة الدفع المحلية للمصرف المحلي”®

4.8.2 استخدام شعار شبكة الدفع المحلية في النص

يُسمح باستخدام شعار شبكة الدفع المحلية كصفة (كما هو الحال في “بطاقة شبكة الدفع المحلية الخاصة بك”) في الاستخدام الأول أو الأبرز بعد أي استخدام في العنوان أو العنوان الرئيسي أو التوقيع أو صفحة الغلاف للعرض، إلا إذا:

1. كلمة “شبكة الدفع المحلية” مستخدمة كجزء من اسم برنامج العضو.
 2. تمت الموافقة على خلاف ذلك صراحةً و كتابةً من قبل مشغل شبكة الدفع المحلية.
- يحظر استخدام كلمة “شبكة الدفع المحلية” في جملة فعلية (“شبكة الدفع المحلية الخاصة بك“)، أو بصيغة الجمع (“شبكات الدفع المحلية“) أو بصيغة الملكية (“شبكة دفعك المحلية“).

9.2 استخدام علامة الشبكة التجارية في هوية الشركة العضو

يجب عدم استخدام شعار شبكة الدفع المحلية كجزء من اسم قانوني أو شركة أو اسم تجاري، مثل “مركز شبكة الدفع المحلية Inc®” لا يُسمح بتسجيل أي اسم لمجال إنترنت يتضمن كلمة “شبكة الدفع المحلية“ ، باستثناء ما هو مسموح به صراحةً و كتابيًا بواسطة مشغل شبكة الدفع المحلية.

10.2 أسماء البرامج

يجب الإشارة إلى كل اسم برنامج، وطلبات الإلتماس، والخدمة بالاسم القانوني الكامل للعلامة التجارية مع تضمين إشعار التسجيل المناسب.

11.2 استخدام العلامة التجارية للمنتج

يجب عدم استخدام العلامة التجارية للمنتج، بطريقة تخلق انطباعًا بأن أي منتج أو خدمة يقدمها المرخص له أو المرخص له من الباطن أو التاجر يتم رعايتها أو إنتاجها أو عرضها أو الموافقة عليها أو بيعها أو الإنضمام إليها بأي شكل آخر مع مشغل شبكة الدفع المحلية. ويجب على كل مرخص له التحقق من أن كل من المرخص لهم من الباطن والشركاء والتجار والمشاركين الآخرين في البرنامج لا يستخدمون شعار شبكة الدفع المحلية، لوضع علامة على أي منتج أو خدمة ما لم يتم التصريح بذلك كتابيًا من قبل مشغل شبكة الدفع المحلية.

2.12 Use of the National Payment Scheme Logo

The National Payment Scheme logo must be reproduced as set forth in chapter 6 of these Standards.

2.13 Use of the National Payment Scheme Card Design in Cardholder Statement Enclosures

The National Payment Scheme Logo or the Card face design must be displayed on statement enclosures used to offer products or services to Cardholders through the use of a Member's National Payment Scheme Card.

2.14 Usage of other Scheme Corporate Names (Non-Scheme Brand)

Only the National Payment Scheme Logo and logo are permitted to be used to signify acceptance of National Payment Scheme Cards.

2.15 Scheme Corporate Identity

The corporate identity of the payment scheme is denoted by the National Payment Scheme Logo.

2.16 Primacy of Scheme Brand

The National Payment Scheme Logo must be the primary brand on National Payment Scheme Cards.

2.17 Use of Brand on Cards

Display of the brand on a Card must be in compliance with the Standards, including chapter 6 of this manual and any other Card design specifications that are established.

2.18 Brand Positioning

The brand must be positioned on the Card as set out in Book 6 of this manual.

2.19 General Card Design

General Card design requirements are found in chapter 6 of these Standards.

2.20 Multiple Brands on Cards

Other payment or non-payment brands are not permitted to reside on National Payment Scheme Cards, unless expressly agreed in writing by the Payment System Operator.

When permitted, the other brands on a Card must not be larger, brighter or more prominent than the National Payment Scheme brand.

2.21 Competitive Logos

A competitor's brand, logo, or name, whether registered or not, must not appear on a Card, nor is a payment application of any such competitor permitted to reside on the magnetic stripe or chip of a Card, unless expressly agreed in writing by the Payment System Operator.

12.2 استخدام شعار شبكة الدفع المحلية

يجب إعادة إنتاج شعار شبكة الدفع المحلية على النحو المنصوص عليه في الفصل 6 من هذه المعايير.

13.2 استخدام تصميم بطاقة شبكة الدفع المحلية في مرفقات بيان حامل البطاقة

يجب عرض شعار شبكة الدفع المحلية أو تصميم وجه البطاقة على مرفقات البيان المستخدمة لتقديم المنتجات أو الخدمات لحاملي البطاقات، من خلال استخدام بطاقة شبكة الدفع المحلية الخاصة بالعضو.

14.2 استخدام أسماء شركات الشبكة الأخرى (علامة تجارية غير نظامية)

يُسمح فقط باستخدام الشعار وشعار شبكة الدفع المحلية للإشارة إلى قبول بطاقات شبكة الدفع المحلية.

15.2 هوية شركة النظام

يُشار إلى هوية الشركة لنظام الدفع بشعار شبكة الدفع المحلية.

16.2 أولوية العلامة التجارية للنظام

يجب أن يكون شعار شبكة الدفع المحلية هو العلامة التجارية الأساسية على بطاقات شبكة الدفع المحلية.

17.2 استخدام العلامة التجارية على البطاقات

يجب أن يتوافق عرض العلامة التجارية على البطاقة مع المعايير، بما في ذلك الفصل 6 من هذا الدليل وأي مواصفات تصميم بطاقة أخرى يتم وضعها.

18.2 وضع العلامة التجارية

يجب وضع العلامة التجارية على البطاقة كما هو موضح في الكتاب 6 من هذا الدليل.

19.2 تصميم البطاقة العام

توجد متطلبات تصميم البطاقة العام في الفصل 6 من هذه المعايير.

20.2 علامات تجارية متعددة على البطاقات

لا يُسمح للعلامات التجارية الأخرى الخاصة بالدفع أو عدم الدفع بالتواجد على بطاقات شبكة الدفع المحلية، ما لم يتم الاتفاق صراحةً و كتابةً مع مشغل شبكة الدفع المحلية. وفي حال السماح بذلك ، فيجب ألا تكون العلامات التجارية الأخرى الموجودة على البطاقة أكبر أو أكثر وضوحاً أو بروزاً من علامة شبكة الدفع المحلية التجارية.

21.2 الشعارات التنافسية

يجب ألا تظهر العلامة التجارية أو الشعار أو الاسم الخاص بالمنافس، سواء كان مسجلاً أم لا، على البطاقة، كما لا يُسمح بوجود تطبيق الدفع لأي منافس من هذا القبيل على الشريط المغناطيسي أو شريحة البطاقة، ما لم يتم الاتفاق صراحةً و كتابةً مع مشغل شبكة الدفع المحلية.

2.22 Member Rights to Identification - General

The Issuer must be clearly identified on the Card.

2.23 Member Rights to Identification on Scheme Branded Products

An Issuer's name, mark or logo is permitted to be placed on the front or back of a Card, provided that it does not obscure the National Payment Scheme Logo. The Issuer's identifying elements must not be larger, brighter or more prominent than the National Payment Scheme Logo.

2.24 Non-Member Brands on Cards

In accordance with the Standards or with the prior written agreement with the Payment System Operator, non-Member brands may be displayed on Cards, for example in the case of a Co-Brand Card Program as described in the following section.

2.25 Co-Brand and Premium Card Program Requirements

A Card Program is permitted to be issued as a Co-Brand Card Program in partnership with a third party, such as a merchant. An Issuer is permitted to use the area on the Card reserved for the identification of the Issuer to instead or additionally identify the Co-brand Partner.

A premium Card may bear a specific legend or program name indicating that it is a premium Card. Premium Cards may also be identified by their color or other distinctive features.

2.26 High Value Consumer Segment Card Programs

A high value consumer Card may bear a specific legend or program name indicating that it is a high value consumer Card. High value consumer Cards may also be identified by their color or other distinctive features.

2.27 Scheme Brand on Payment Devices

A National Payment Scheme payment application loaded on a Mobile Payment Device or Access Device must be identified by the National Payment Scheme Logo in the user interface.

2.28 Card Acceptance at Point of Sale (POS) or Card Not Present (CNP)

A Member must comply with all of the following requirements for display of the National Payment Scheme Logo at Merchant locations:

The National Payment Scheme Logo must be displayed as set forth in the Standards.

1. The National Payment Scheme Logo must be afforded at least equal prominence and be at least as large as other acceptance marks displayed by the Merchant.
2. The National Payment Scheme Logo must not be combined with any other acceptance marks displayed on the same Terminal.
3. The National Payment Scheme Logo must not be placed on or near or otherwise be used to identify any acceptance device or website that does not accept National Payment Scheme Cards.
4. The National Payment Scheme Logo must be shown in full color according to the color specifications provided by the Payment System Operator.
5. The National Payment Scheme Logo must not be displayed in a false, deceptive, or misleading manner.

22.2 حقوق الأعضاء في التحديد - عام

يجب تحديد جهة الإصدار بوضوح على البطاقة.

23.2 حقوق الأعضاء في التحديد على المنتجات ذات علامة النظام التجارية

يُسمح بوضع اسم جهة الإصدار أو علامته أو شعاره على الجزء الأمامي أو الخلفي من البطاقة، بشرط ألا يجلب شعار شبكة الدفع المحلية. يجب ألا تكون عناصر تحديد هوية جهة الإصدار أكبر أو أكثر وضوحاً أو أكثر بروزاً من شعار شبكة الدفع المحلية.

24.2 العلامات التجارية غير الأعضاء على البطاقات

وفقاً للمعايير أو باتفاق مكتوب مسبقاً مع مشغل شبكة الدفع المحلية، قد يتم عرض العلامات التجارية غير الأعضاء على البطاقات، على سبيل المثال في حالة برنامج بطاقة العلامة التجارية المشتركة كما هو موضح في القسم التالي.

25.2 متطلبات برنامج العلامة التجارية المشتركة والبطاقة المميزة

يُسمح بإصدار برنامج البطاقة كبرنامج بطاقة ذات علامة تجارية مشتركة بالشاركة مع طرف ثالث، مثل التاجر. ويُسمح لجهة الإصدار باستخدام المنطقة المحجوزة على البطاقة لتحديد هوية جهة الإصدار من أجل تحديد شريك العلامة التجارية المشتركة بدلاً من ذلك، أو بشكل إضافي.

قد تحمل البطاقة المميزة، اسماً مميزاً أو اسم برنامج يشير إلى أنها بطاقة مميزة. ويمكن أيضاً التعرف على البطاقات المميزة من خلال لونها أو ميزاتها المميزة الأخرى.

26.2 برامج بطاقة شريحة المستهلك عالية القيمة

قد تحمل بطاقة المستهلك عالية القيمة رمزاً معيناً، أو اسم برنامج يشير إلى أنها بطاقة مستهلك عالية القيمة. ويمكن أيضاً التعرف على بطاقات المستهلك عالية القيمة من خلال لونها أو ميزاتها المميزة الأخرى.

27.2 العلامة التجارية للنظام على أجهزة الدفع

يجب تحديد تطبيق الدفع الخاص بشبكة الدفع المحلية، والذي تم تحميله على جهاز الدفع عبر الهاتف المحمول أو جهاز الوصول بواسطة شعار شبكة الدفع المحلية في واجهة المستخدم.

28.2 قبول البطاقة في نقاط البيع أو البطاقة غير الموجودة

يجب على العضو الامتثال لجميع المتطلبات التالية لعرض شعار شبكة الدفع المحلية في مواقع التاجر:

يجب عرض شعار شبكة الدفع المحلية على النحو المنصوص عليه في المعايير.

1. يجب أن يُمنح شعار شبكة الدفع المحلية أهمية متساوية على الأقل وأن يكون على الأقل بحجم علامات القبول الأخرى التي يعرضها التاجر.
2. يجب عدم دمج شعار شبكة الدفع المحلية، مع أي علامات قبول أخرى معروضة على نفس المحطة.
3. يجب عدم وضع شعار شبكة الدفع المحلية على، أو بالقرب من أو استخدامه بأي وسيلة أخرى لتحديد أي جهاز قبول أو موقع لا يقبل بطاقات شبكة الدفع المحلية.
4. يجب عدم وضع شعار مخطط الدفع الوطني على أو بالقرب من أو استخدام أي وسيلة أخرى لتحديد أي جهاز قبول أو موقع ويب لا يقبل بطاقات نظام الدفع الوطني.
5. يجب أن يظهر شعار شبكة الدفع المحلية بالألوان الكاملة، ووفقاً لمواصفات الألوان التي يوفرها مشغل شبكة الدفع المحلية.

لا يجوز عرض شعار شبكة الدفع المحلية بطريقة خاطئة، أو خادعة أو مضللة.

2.29 ATM Network Program Logos

National Payment Scheme is the brand used to denote the National Payment Scheme ATM Network.

The National Payment Scheme Logo must appear on or near the ATM and must be applied in such a way that Cardholders can immediately recognize that the Terminal is associated with the National Payment Scheme service.

The National Payment Scheme Logo must not be placed on or near, or otherwise used to identify any ATM, which does not accept National Payment Scheme Cards.

The National Payment Scheme Logo must be shown in full color according to the color specifications provided by the Payment System Operator.

The National Payment Scheme Logo must be more prominent than any other mark displayed.

2.30 Card Acceptance at ATM

The National Payment Scheme Logo must be displayed on an ATM that accepts National Payment Scheme Cards with at least equal prominence and be at least as large as other acceptance marks on the ATM.

2.31 Card Acceptance in International Points of Acceptance

Card acceptance under the National Payment Scheme brand is not supported outside of Egypt, unless otherwise agreed by the Payment System Operator.

2.32 General Use of Scheme Brands for Promotional Purposes

The Payment System Operator reserves the right to review samples and approve or refuse to approve any use of the brand for marketing or promotional purposes. Amended samples, if required as a result of this review, also must be forwarded to the Payment System Operator for review.

2.33 Use of a Card Design in Issuer Advertising and Promotional Material

An Issuer is permitted to depict a National Payment Scheme Card face for an advertising or marketing purpose, subject to the following requirements.

1. The proportions of the Card face design, including typestyle and relative positions of the legends, must not be altered or distorted.
2. The legend “VALID THRU” or the equivalent must be depicted on the Card face design, unless the Card face design contains an effective date and an expiration date, in which case the words “VALID DATES” must be depicted.
3. The Card face design must bear Account information (for example, the Primary Account Number (PAN), the effective date and/or expiration date) and all Card face design requirements set forth in the Card Design Standards. The first six digits of the Account number must be a BIN assigned to the Issuer by the Payment System Operator or an unassigned BIN which the Payment System Operator has set aside for Issuer use in advertising and marketing Card face designs.
4. The National Payment Scheme Logo must be completely visible on at least one Card face design depicted in the materials.

29.2 شعارات برنامج شبكة أجهزة الصراف الآلي

شبكة الدفع المحلية هي العلامة التجارية المستخدمة للإشارة إلى شبكة أجهزة الصراف الآلي لشبكة الدفع المحلية.

يجب أن يظهر شعار شبكة الدفع المحلية على أو بالقرب من جهاز الصراف الآلي، ويجب تطبيقه بطريقة تمكن حاملي البطاقات من التعرف على الفور بارتباط المحطة بخدمة شبكة الدفع المحلية.

يجب عدم وضع شعار شبكة الدفع المحلية على أو بالقرب من أو استخدامه بأي طريقة لتحديد أي جهاز صراف آلي لا يقبل بطاقات شبكة الدفع المحلية.

يجب أن يظهر شعار شبكة الدفع المحلية بالألوان الكاملة وفقًا لمواصفات الألوان التي يوفرها مشغل شبكة الدفع المحلية.

يجب أن يكون شعار شبكة الدفع المحلية أكثر وضوحًا من أي علامة أخرى معروضة.

30.2 قبول البطاقة في أجهزة الصراف الآلي

يجب عرض شعار شبكة الدفع المحلية على جهاز الصراف الآلي الذي يقبل بطاقات شبكة الدفع المحلية ذات الأهمية نفسها على الأقل، وتكون على الأقل بحجم علامات القبول الأخرى على أجهزة الصراف الآلي.

31.2 قبول البطاقة في نقاط القبول الدولية

قبول البطاقة بموجب علامة شبكة الدفع المحلية التجارية غير مدعوم خارج ليبيا ، ما لم يتم الموافقة على خلاف ذلك من قبل مشغل شبكة الدفع المحلية.

32.2 الاستخدام العام لعلامات النظام التجارية للأغراض الترويجية

لمشغل شبكة الدفع المحلية مراجعة العينات والموافقة أو رفض الموافقة على أي استخدام للعلامة التجارية لأغراض التسويق أو الترويج. ويجب أيضًا إرسال العينات المعدلة، إذا لزم الأمر نتيجة لهذه المراجعة، إلى مشغل شبكة الدفع المحلية للمراجعة.

33.2 استخدام تصميم البطاقة في إعلانات جهة الإصدار والمواد الترويجية

يُسمح لجهة الإصدار بتصوير وجه بطاقة شبكة الدفع المحلية لغرض إعلاني أو تسويقي، وفقًا للمتطلبات التالية.

1. يجب عدم تغيير أو تشويه نسب تصميم وجه البطاقة، بما في ذلك النمط والمواضع النسبية للأساطير.
2. يجب وصف وسيلة “صالحة من خلال” أو ما يعادلها على تصميم وجه البطاقة، ما لم يتضمن تصميم وجه البطاقة تاريخًا ساريًا وتاريخ انتهاء صلاحية، وفي هذه الحالة يجب وصف الكلمات “تواريخ صالحة”.
3. يجب أن يحمل تصميم وجه البطاقة معلومات الحساب (على سبيل المثال، رقم الحساب الأساسي والتاريخ الفعلي و/أو تاريخ انتهاء الصلاحية) وجميع متطلبات تصميم وجه البطاقة المنصوص عليها في معايير تصميم البطاقة، ويجب أن تكون الأرقام الستة الأولى من رقم الحساب عبارة عن رقم تعريف مصرفي يتم تعيينه لجهة الإصدار بواسطة مشغل شبكة الدفع المحلية، أو رقم تعريف مصرفي غير مُعين، والذي وضعه مشغل شبكة الدفع المحلية جانبًا لاستخدام جهة الإصدار في تصميمات وجه البطاقة الإعلانية والتسويقية.
4. يجب أن يكون شعار شبكة الدفع المحلية مرئيًا تمامًا على تصميم وجه بطاقة واحد على الأقل الموصوف في المواد.

2.34 Use of a Card Design in Merchant Advertising and Signage

A Merchant is prohibited from using a National Payment Scheme Card design to indicate acceptance in Merchant advertising or other signage, other than signage for a Co-Brand Program in which the Merchant is a Co-Brand Partner. A Merchant is permitted to display an Issuer-specific National Payment Scheme Card design in Merchant advertising and any other signage that is not used to signify acceptance.

2.35 Brand Usage for Promotion and Advertising Activities

The National Payment Scheme Logo must not be used on a promotional card or other card without the prior written consent of the Payment System Operator.

2.36 Member Sponsorships

Subject to prior written agreement with the Payment System Operator, the National Payment Scheme Logo may be used in Member sponsorship activities.

2.37 Sponsorships Usage Requirements

The requirements related to use of the National Payment Scheme Logo in Member sponsorship activities

Regulatory Rules of The Libyan National Payment Scheme

Book 2 Chapter 3 - NUMO Products Guide

3.1 Introduction

3.1.1 Overview

Purpose of this guide, is delivering a framework for issuers interested in developing and launching NUMO Debit and Prepaid Cards.

Through this guide issuers will be able to get familiar with the basic requirements and key features of NUMO cards and build their NUMO products. However, because each issuer and its systems are unique, systems specifications for each proprietary system or third-party processor will vary and, therefore, are not the concern of this reference.

This reference can also be used by acquirers to understand how they can accept NUMO cards using the technical path of NUMO acceptance brand.

3.1.2 Who Should Use This Book

The National Scheme Operator provides this guide for issuing banks, acquiring banks and their authorized service providers. The main audience is the card department of the banks planning to enrich their card portfolio with a NUMO card proposition. The present guide can also be used by the acquiring department of the bank to understand how to accept NUMO cards.

34.2 استخدام البطاقة في إعلانات التاجر واللافتات

يُحظر على التاجر استخدام تصميم بطاقة شبكة الدفع المحلية، للإشارة إلى القبول في إعلانات التاجر أو غيرها من اللافتات، بخلاف اللافتات الخاصة ببرنامج العلامة التجارية المشتركة الذي يكون التاجر فيها شريكًا لعلامة تجارية مشتركة. ويُسمح للتاجر بعرض تصميم بطاقة شبكة الدفع المحلية الخاصة بجهة الإصدار في إعلانات التاجر وأي لافتات أخرى لا تُستخدم للدلالة على القبول.

35.2 استخدام العلامة التجارية لأنشطة الترويج والإعلان

لا يجوز استخدام شعار شبكة الدفع المحلية على بطاقة ترويجية، أو بطاقة أخرى، دون الحصول على الموافقة المكتوبة المسبقة من مشغل شبكة الدفع المحلية.

36.2 رعاية الأعضاء

مع مراعاة الاتفاق الكتابي المسبق مع مشغل شبكة الدفع المحلية، يجوز استخدام شعار شبكة الدفع المحلية في أنشطة رعاية الأعضاء.

37.2 متطلبات استخدام الرعاية

يجب أن تكون المتطلبات المتعلقة باستخدام شعار شبكة الدفع المحلية في أنشطة كفالة\رعاية الأعضاء.

القواعد التنظيمية لشبكة الدفع المحلية الليبية الكتاب 2 الفصل 3 - دليل منتجات نمو

1.3 مقدمة

1.1.3 نظرة عامة

الغرض من هذا الدليل هو تقديم إطار عمل لجهات الإصدار المهتمة بتطوير وإطلاق بطاقات الخصم، وبطاقات الدفع المسبق الخاصة بنمو.

من خلال هذا الدليل، ستمكن جهات الإصدار من التعرف على المتطلبات الأساسية والميزات الرئيسية لبطاقات نمو وإصدار منتجات نمو الخاصة بهم. ومع ذلك، ونظرًا لأن كل جهة إصدار وأنظمتها فريدة من نوعها، فإن مواصفات الأنظمة لكل نظام مملوك أو معالج تابع لجهة خارجية ستختلف، وبالتالي، تخرج عن نطاق هذا الدليل.

يمكن أيضًا استخدام هذا الدليل من قبل جهات القبول لفهم كيف يمكنهم قبول بطاقات نمو باستخدام المسار التقني لعلامة قبول نمو التجارية.

2.1.3 من يجب أن يستخدم هذا الكتاب

يوفر مشغل شبكة الدفع المحلية هذا الدليل للمصارف المصدرة، والمصارف القابلة ومقدمي الخدمات المعتمدين. الجمهور الرئيسي هو قسم البطاقات في المصارف التي تخطط لإثراء محفظة بطاقاتهم باقتراح بطاقة نمو. ويمكن أيضًا استخدام هذا الدليل بواسطة القسم المختص بالتزويد في المصرف لفهم كيفية قبول بطاقات نمو.

3.2 Basic Requirements

NUMO Cards is an immediate payment method that leverages the NUMO brand mark. It offers a debit/prepaid card solution, enabling everyday payments. It is used for personal payments rather than business or corporate payments unless being stated otherwise.

With NUMO Cards, the customer can pay at any NUMO branded acceptance point both physical and online.

Issuers must enable the card for domestic acceptance wherever the NUMO brand marks appear. Transactions are debited from the cardholder's account or prepaid card balance without delay after the issuer receives them.

The Payment card type (Debit/Prepaid) wording may be printed on the front or back of the card. This is intended to allow consumers and merchants to visually identify that this is a Debit/prepaid NUMO product and to distinguish NUMO Card type (commercial, Consumer, prepaid or Debit cards).

NUMO cards need to support all payment channels from POS to ATM and e-commerce.

3.3 NUMO Debit Cards

3.3.1 Product Construct – Features and Benefits

The core value proposition of NUMO Debit card includes features that help to drive card usage by addressing consumers' needs for convenience and control.

The below principles are guidelines available to issuers, to enable them to create innovative customer value propositions.

General Debit Cards Strategy

(See appendix number 2)

- Issuers decide what should form part of the proposition based on how they wish to position the product and the target segment they wish to attract
- Issuers can choose Value added benefits that can enrich the customer value proposition. Issuers may offer Value added benefits that are not sourced from the National Scheme Operator.

While building benefits into value propositions, Issuers may carry out an internal assessment using the following criteria (Indicative)

(See appendix number 3)

3.3.2 Technical Considerations

A NUMO Debit Card has specific requirements in regard of BIN, product code, card design, and CVM, please check book 3 chapter 1 for more details.

for example. These are listed below.

2.3 المتطلبات الأساسية

تعد بطاقات نمو طريقة دفع فورية، تستفيد من علامة العلامة التجارية نمو. وتقدم حل بطاقة الخصم/ الدفع المسبق، مما يتيح المدفوعات اليومية. يتم استخدامه للمدفوعات الشخصية بدلاً من مدفوعات الأعمال أو الشركات ما لم يُذكر خلاف ذلك.

باستخدام بطاقات نمو، يمكن للعميل الدفع في أي نقطة قبول تحمل علامة نمو التجارية سواء بطريقة شخصية أو عبر الإنترنت.

يجب على جهات الإصدار تمكين البطاقة للقبول المحلي، أينما تظهر علامات العلامة التجارية نمو، ويتم خصم المعاملات من حساب حامل البطاقة، أو رصيد البطاقة المدفوعة مسبقاً دون تأخير بعد أن تستلمها جهة الإصدار.

يمكن طباعة صيغة نوع بطاقة الدفع (الخصم/الدفع المسبق) على الوجه الأمامي أو الخلفي للبطاقة. ويهدف هذا إلى السماح للمستهلكين والتجار بالتعرف بشكل مرئي على أن هذا هو منتج نمو خصم/ الدفع المسبق، وتمييز نوع بطاقة نمو سواء (بطاقة تجارية أو مستهلك أو الدفع المسبق أو خصم). تحتاج بطاقات نمو إلى دعم جميع قنوات الدفع، من نقاط البيع إلى أجهزة الصراف الآلي والتجارة الإلكترونية.

3.3 بطاقات خصم نمو

1.3.3 تكوين المنتج - الميزات والفوائد

يتضمن عرض القيمة الأساسية لبطاقة الخصم نمو ميزات تساعد على زيادة استخدام البطاقة من خلال تلبية احتياجات المستهلكين للملائمة والتحكم.

تشكل المبادئ التالية إرشادات متاحة لجهات الإصدار، لتمكينهم من إنشاء عروض قيمة مبتكرة للعملاء.

الإستراتيجية العامة لبطاقات الخصم

(انظر ملحق رقم 2)

- تقرر جهات الإصدار ما يجب أن يشكل جزءاً من العرض بناءً على كيفية رغبتهم في وضع المنتج والشريحة المستهدفة التي يرغبون في جذبها.
- يمكن لجهات الإصدار اختيار مزايا القيمة المضافة؛ التي يمكن أن تثري عرض قيمة العميل. قد تقدم جهات الإصدار مزايا ذات قيمة مضافة لا يتم الحصول عليها من مشغل شبكة الدفع المحلية.

أثناء تقرير الفوائد في عروض القيمة، قد تجري جهات الإصدار تقييماً داخلياً باستخدام المعايير التالية (إرشادية)

(انظر ملحق رقم 3)

2.3.3 الاعتبارات الفنية

تحتوي بطاقة الخصم نمو على متطلبات محددة فيما يتعلق برقم التعريف المصرفي، ورمز المنتج، وتصميم البطاقة، و CVM، يرجى مراجعة الكتاب الثالث، الفصل الأول للمزيد من التفاصيل.

على سبيل المثال. أنظر المذكور أدناه.

3.3.2.1 BINs and Product Codes

Customer banks planning to issue NUMO Debit Cards need to obtain a Debit Card BIN for the correct calculation of interchange fees. The BIN that has been provided by the National Scheme Operator needs to be set up in the National Scheme Operator’s authorization and settlement system and provided to acquirers through the BIN table.

3.3.2.2 Card Design Requirements

The NUMO Debit Card must comply with the specifications contained in Book 3 chapter 1- Card Design Standards and Specifications.
(See appendix number 4)

3.4 Prepaid Cards

3.4.1 Types of NUMO Prepaid Cards

There are 2 major types of NUMO Prepaid Cards

- Not-Personalized Prepaid Cards (Anonymous)
- Personalized Prepaid Cards

3.4.2 Technical Considerations

A NUMO Prepaid Card has specific requirements in regard of BIN, product code, card design, and CVM, for example. These are listed below.

3.4.2.1 BINs and Product Codes

Customer banks planning to issue NUMO Prepaid Cards need to obtain a Prepaid Card BIN for the correct calculation of interchange fees. The BIN that has been provided by the National Scheme Operator needs to be set up in the National Scheme Operator’s authorization and settlement system and provided to acquirers through the BIN table.

3.4.2.2 Card Design Requirements

The NUMO Prepaid Card must comply with the specifications contained in Book 6 – Card Design Standards and Specifications.

The Cardholder’s name for not-personalized cards is not required on the card. Cards will bear a generic program name.

All Not-Personalized Prepaid Cards must indicate “No Cash Access” on the back of the Card.

If the Program is a Gift Card Program, the word “Gift” must appear on card front or back

1.2.3.3 أرقام التعريف المصرفية، ورموز المنتجات

تحتاج مصارف العملاء التي تخطط لإصدار بطاقات خصم نمو إلى الحصول على رقم تعريف مصرفي لبطاقة الخصم، من أجل الحساب الصحيح لرسوم التبادل. ويجب إعداد رقم التعريف المصرفي الذي قدمه مشغل شبكة الدفع المحلية في نظام تفويض وتسوية مشغل شبكة الدفع المحلية وتقديمه إلى القابلين من خلال جدول رقم التعريف المصرفي.

2.2.3.3 متطلبات تصميم البطاقة

يجب أن تمثل بطاقة الخصم نمو للمواصفات الواردة في الفصل 1 من الكتاب 3 - معايير ومواصفات تصميم البطاقة.

(انظر ملحق رقم 4)

4.3 البطاقات مسبقة الدفع

1.4.3 أنواع بطاقات نمو مسبقة الدفع

هناك نوعان رئيسيان من بطاقات نمو مسبقة الدفع

- بطاقات دفع مسبق غير مخصصة (مجهولة المصدر)
- بطاقات دفع مسبق مخصصة

2.4.3 الاعتبارات الفنية

تحتوي بطاقة نمو مسبقة الدفع على متطلبات محددة فيما يتعلق برقم التعريف المصرفي، ورمز المنتج، وتصميم البطاقة، و CVM، على سبيل المثال. أنظر المذكورة أدناه.

1.2.4.3 أرقام التعريف المصرفية ورموز المنتجات

تحتاج مصارف العملاء التي تخطط لإصدار بطاقات نمو مسبقة الدفع للحصول على بطاقة رقم تعريف مصرفي مسبقة الدفع، من أجل الحساب الصحيح لرسوم التبادل. ويجب إعداد رقم التعريف المصرفي الذي قدمه مشغل شبكة الدفع المحلية في نظام تفويض وتسوية مشغل شبكة الدفع المحلية وتقديمه إلى القابلين من خلال جدول رقم التعريف المصرفي.

2.2.4.3 متطلبات تصميم البطاقة

يجب أن تتوافق بطاقة نمو مسبقة الدفع مع المواصفات الواردة في الكتاب 6 - معايير ومواصفات تصميم البطاقة.

اسم حامل البطاقة للبطاقات غير المخصصة، غير مطلوب على البطاقة. ستحمل البطاقات اسم برنامج عام.

يجب أن تشير جميع البطاقات مسبقة الدفع غير المخصصة إلى “لا يوجد وصول نقدي” على ظهر البطاقة.

إذا كان البرنامج عبارة عن برنامج بطاقة هدايا، فيجب أن تظهر كلمة “هدية” على مقدمة البطاقة أو خلفها

3.4.3 Not-Personalized Prepaid Product Specific Requirements

All not-personalized prepaid products must meet the basic requirements set out below and must adhere to the Standards.
(See appendix number 5)

3.4.3.1 Limitations on Loading and Use of Not-personalized Prepaid Cards

It is the issuer's responsibility according to its risk evaluation to specify the maximum limit and number/value of daily transactions processed with prepaid cards, subject to following parameters:

Reload Option: All not-personalized prepaid Cards are non-reloadable.

Maximum Amount for Card Balance is XXX LYD.

Daily Limit for use of a not-personalized prepaid card is XXX LYD.

Monthly Limit for use of a not-personalized prepaid card is XXX LYD.

Cash and ATM Access are not permitted.

Distribution Channel: Not-Personalized prepaid cards may be issued at a bank branch or sold in shops. The maximum value of a card issued at bank branch is XXX LYD. The maximum value of a card sold in a shop is XX LYD. The card may be purchased with cash. The maximum number of cards sold at any one time is [one].

3.4.3.2 Not-Personalized Prepaid Product Types

The different types of anonymous prepaid card programs are outlined below. These card types do not require the cardholder to be identified, must not provide cash or ATM access, and must be non-reloadable. According to the type of program, the issuer is permitted to restrict acceptance to a specific transaction type, or a specific merchant or group or merchants, for example by MCC.

The National Scheme Operator may develop other types of anonymous prepaid products in the future.

Prepaid Gift Card Program

The Prepaid Gift Card Program is a secure and convenient non-reloadable prepaid card that is an alternative to gift certificates and cash for gift giving occasions. Prepaid gift cards are fully anonymous cards. In addition to allowing an individual to immediately gain access to a Card, owing to the option of instant issuance, issuers are also able to upgrade consumers from anonymous to fully registered cardholders over stages, to build valuable long-term engagement.

Prepaid Incentive and Rewards Program

The Prepaid Incentive and Rewards Program is a commercial card program that provides an alternative to cash, checks, or product incentives for businesses who wish to provide non-cash incentives and rewards to customers without identifying them.

3.4.3 المتطلبات المحددة لمنتج مسبق الدفع غير المخصص

يجب أن تفي جميع المنتجات مسبقة الدفع غير المخصصة، بالمتطلبات الأساسية الموضحة أدناه، ويجب أن تلتزم بالمعايير.
(انظر ملحق رقم 5)

1.3.4.3 قيود شحن واستخدام البطاقات مسبقة الدفع غير المخصصة

تتحمل جهة الإصدار وفقًا لتقييم المخاطر الخاص بها؛ مسؤولية تحديد الحد الأقصى وعدد/قيمة المعاملات اليومية التي تتم معالجتها ببطاقات الدفع المسبق، وفقًا للمعايير التالية:
خيار إعادة الشحن: جميع بطاقات الدفع المسبق غير المخصصة غير قابلة لإعادة الشحن.

الحد الأقصى لمبلغ رصيد البطاقة هو XXX دينار ليبي.

الحد اليومي لاستخدام بطاقة الدفع المسبق غير المخصصة هو XXX دينار ليبي.

الحد الشهري لاستخدام بطاقة الدفع المسبق غير المخصصة هو XXX دينار ليبي.

لا يسمح بالوصول النقدي وأجهزة الصراف الآلي .

قناة التوزيع : قد يتم إصدار بطاقات الدفع المسبق غير المخصصة في فرع المصرف، أو بيعها في المتاجر. الحد الأقصى لقيمة البطاقة الصادرة في فرع المصرف هو XXX دينار ليبي. الحد الأقصى لقيمة البطاقة المباعة في المتجر هو XX دينار ليبي. يمكن شراء البطاقة نقدًا. الحد الأقصى لعدد البطاقات المباعة في أي وقت هو [واحد].

2.3.4.3 أنواع بطاقات الدفع المسبق غير المخصصة

الأنواع المختلفة من برامج بطاقات الدفع المسبق مجهولة المصدر موضحة أدناه. لا تتطلب أنواع هذه البطاقات تحديد هوية حامل البطاقة، ويجب ألا توفر إمكانية الوصول النقدي أو أجهزة الصراف الآلي، ويجب أن تكون غير قابلة لإعادة الشحن. وفقًا لنوع البرنامج، يُسمح لجهة الإصدار بتقييد القبول بنوع معاملة معين، أو تاجر أو مجموعة تاجر معينين، على سبيل المثال بواسطة MCC.

قد يقوم مشغل شبكة الدفع المحلية بتطوير أنواع أخرى من منتجات الدفع المسبق مجهولة المصدر في المستقبل.

برنامج بطاقة الهدايا مسبقة الدفع

برنامج بطاقة الهدايا مسبقة الدفع هو بطاقة مسبقة الدفع، آمنة ومريحة وغير قابلة لإعادة الشحن، وهي بديل لشهادات الهدايا والنقد لمناسبات تقديم الهدايا. بطاقات الهدايا مسبقة الدفع هي بطاقات مجهولة المصدر بالكامل. بالإضافة إلى السماح للفرد بالوصول الفوري إلى البطاقة، نظرًا لخيار الإصدار الفوري، يمكن لجهات الإصدار أيضًا ترقية المستهلكين من حاملي بطاقات مجهولين إلى حاملي بطاقات مسجلين بالكامل على مراحل، لبناء مشاركة قيمة طويلة الأجل.

برنامج الحوافز والمكافآت مسبقة الدفع

برنامج الحوافز والمكافآت مسبقة الدفع هو برنامج بطاقة تجارية يوفر بديلًا للنقد أو الصكوك أو حوافز المنتجات للشركات التي ترغب في تقديم حوافز ومكافآت غير نقدية للعملاء دون التعرف عليهم.

3.4.4 Personalized Prepaid Product Requirements

All personalized prepaid products must meet the basic requirements set out below and must adhere to the Standards.
(See appendix number 6)

3.4.4.1 Limitations on Loading and Use of personalized Prepaid Cards

It is the issuer's responsibility according to its risk evaluation to specify the maximum limit and number/value of daily transactions processed with prepaid cards, subject to following parameters:

- Maximum Amount for Card Balance is Subject to CBL regulations.
- Daily Limit for Withdrawal/Transfer/Purchases for one customer's cards issued from one bank is 10,000 LYD.
- Monthly Limit for Withdrawal/Transfer/Purchases for one customer's cards issued from one bank for natural persons is 50,000 LYD.
- A bank is permitted to issue only one prepaid card to any customer, while a customer is permitted to have prepaid cards from several banks.

3.4.5 Recommended Features – personalized Prepaid Products

1. Zero Liability
2. Hybrid Dual Interface (Recommended)
3. Transaction alerts

Issuers will decide which recommended features should form part of the proposition based on how they wish to position the product and the target segment they wish to attract. Issuers can also provide value added benefits that enrich the customer value proposition. Issuers have the right to offer value added benefits that are not sourced from the National Scheme Operator.

3.4.6 Personalized Prepaid Product Types

The different types of personalized prepaid card programs are outlined below. According to the type of program, the issuer is permitted to restrict acceptance to a specific transaction type, or a specific merchant or group or merchants, for example by MCC.

The National Scheme Operator may develop other types of personalized prepaid products in the future.

1. Prepaid Consumer Reloadable Program

The Prepaid Consumer Reloadable Program provides an alternative to cash and checks for consumers who cannot or prefer not to use credit or a debit cards for all or some of their payment activities. These cards are useful for mail, phone, or internet-based commerce.

2. Prepaid Humanitarian Card Program

The Prepaid Humanitarian card is prepaid card that can be used in the immediate aftermath of a humanitarian crisis to distribute humanitarian assistance. The solution can be used to support the needs of humanitarian agencies to quickly respond to humanitarian disasters.

4.4.3 متطلبات منتجات الدفع المسبق المخصصة

يجب أن تفي جميع منتجات الدفع المسبق المخصصة بالمتطلبات الأساسية الموضحة أدناه ويجب أن تلتزم بالمعايير.
(انظر ملحق رقم 6)

1.4.4.3 قيود شحن واستخدام بطاقات الدفع المسبق المخصصة

تتحمل جهة الإصدار وفقًا لتقييم المخاطر الخاص بها، مسؤولية تحديد الحد الأقصى وعدد/ قيمة المعاملات اليومية التي تتم معالجتها ببطاقات الدفع المسبق، وفقًا للمعايير التالية:

- الحد الأقصى لمبلغ رصيد البطاقة يخضع لقواعد مصرف ليبيا المركزي.
- الحد اليومي للسحب/التحويل/المشتريات لبطاقات عميل واحد الصادرة من مصرف واحد هو 10.000 دينار ليبي.
- الحد الشهري للسحب/التحويل/المشتريات لبطاقات عميل واحد الصادرة من مصرف واحد للأشخاص الطبيعيين هو 50.000 دينار ليبي.
- يُسمح للمصرف بإصدار بطاقة دفع مسبق واحدة فقط لأي عميل، بينما يُسمح للعميل بالحصول على بطاقات الدفع المسبق من عدة مصارف.

5.4.3 الميزات الموصى بها - منتجات الدفع المسبق المخصصة

1. المسؤولية الصفرية\عدم وجود مسؤولية
 2. واجهة مزدوجة هجينة (موصى بها)
 3. تنبيهات المعاملات
- ستقرر جهات الإصدار الميزات الموصى بها، والتي يجب أن تشكل جزءًا من العرض بناءً على كيفية رغبتهم في وضع البطاقة والشريحة المستهدفة التي يرغبون في جذبها. يمكن لجهات الإصدار أيضًا توفير فوائد ذات قيمة مضافة تثيري عرض قيمة العميل. لجهات الإصدار الحق في تقديم فوائد ذات قيمة مضافة لا يتم الحصول عليها من مشغل شبكة الدفع المحلية.

6.4.3 أنواع منتجات الدفع المسبق المخصصة

الأنواع المختلفة لبرامج بطاقات الدفع المسبق المخصصة موضحة أدناه. وفقًا لنوع البرنامج، يُسمح لجهة الإصدار بتقييد القبول لنوع معاملة معين، أو تاجر أو مجموعة تاجر معينين، على سبيل المثال بواسطة MCC.

قد يقوم مشغل شبكة الدفع المحلية بتطوير أنواع أخرى من بطاقات الدفع المسبق المخصصة في المستقبل.

برنامج بطاقة المستهلك مسبقة الدفع القابلة لإعادة الشحن

1. يوفر برنامج بطاقة المستهلك مسبقة الدفع القابلة لإعادة الشحن بديلًا للنقد والصكوك للمستهلكين الذين لا يستطيعون أو يفضلون عدم استخدام بطاقات الائتمان أو الخصم لجميع أو بعض أنشطة الدفع الخاصة بهم. هذه البطاقات مفيدة للبريد أو الهاتف أو التجارة عبر الإنترنت.

2. برنامج البطاقة الإنسانية مسبقة الدفع

البطاقة الإنسانية مسبقة الدفع هي بطاقة مسبقة الدفع يمكن استخدامها في أعقاب أزمة إنسانية مباشرة لتوزيع المساعدة الإنسانية. يمكن استخدام الحل لدعم احتياجات الوكالات الإنسانية للاستجابة السريعة للكوارث الإنسانية.

The Prepaid Humanitarian card can only be reloaded by humanitarian agencies (for example, United Nations agencies, non-governmental organizations with a humanitarian remit, or other humanitarian agencies), and includes a cash access feature under certain conditions. The product offers material benefits for humanitarian programs targeting refugees, internally displaced persons, and other humanitarian aid recipients.

The product is intended for short-term relief programs in the immediate aftermath of humanitarian crises, when local issuance is not an immediately viable option. The product is not intended for long-term resilience programs.

3. Prepaid Incentive and Rewards Program

The Prepaid Incentive and Rewards Program is a commercial card program that provides an alternative to cash, checks, or product incentives for businesses who wish to provide incentives and rewards to employees, contractors, or customers. The cards are either reloadable or non-reloadable.

4. Prepaid Healthcare Program

The Prepaid Healthcare Program is designed to support payment for healthcare expenses through a prepaid, reloadable card given to an employee by the employer or health insurance provider.

The card is to be used only at designated healthcare merchant category codes (MCCs) and only for eligible healthcare expenses.

5. Prepaid Payroll Program

The Prepaid Payroll Program is a secure and convenient alternative to paying employees, contractors, or agents with cash or checks. It can be used for any form of compensation, but is not generally used for bonus or incentive payments (please see Prepaid Incentive and Rewards Program above). With direct deposit, online bill payment, instant access to balance information and greater security and balance recovery for lost or stolen cards, employees also benefit from the Program.

6. Prepaid Meal and Food Voucher Program

The Prepaid Meal and Food Voucher Program is designed to support payment for tax-advantaged meal or food benefits through a prepaid Card given to an employee by their employer abiding by local law and regulatory guidelines for meal and food programs. The Program is limited for use at designated meal or food merchant category codes (MCCs) and can be used only for meal and food expenses. A Meal and Food Voucher Card may support additional types of tax-advantaged benefits in accordance with applicable regulations.

7. Prepaid Business Program

The Prepaid Business Program is a card solution that can be used to pay a range of business related expenses:

- Business travel and entertainment
- Purchasing of goods and services
- Replacement for petty cash
- Business meetings and functions

لا يمكن إعادة شحن البطاقة الإنسانية مسبقة الدفع إلا من قبل الوكالات الإنسانية (على سبيل المثال، وكالات الأمم المتحدة، أو المنظمات غير الحكومية ذات الاختصاصات الإنسانية، أو الوكالات الإنسانية الأخرى)، وتتضمن ميزة الوصول النقدي في أحوال معينة. يقدم المنتج فوائد مادية للبرامج الإنسانية التي تستهدف اللاجئين والأشخاص المشردين داخلياً وغيرهم من متلقي المساعدات الإنسانية.

هذه البطاقة مخصصة لبرامج الإغاثة قصيرة المدى في أعقاب الأزمات الإنسانية المباشرة، عندما لا يكون الإصدار المحلي خياراً قابلاً للتطبيق على الفور. هذه البطاقة غير مخصصة لبرامج المرونة طويلة المدى.

3. برنامج بطاقة الحوافز والمكافآت مسبقة الدفع

برنامج بطاقة الحوافز والمكافآت مسبقة الدفع هو برنامج بطاقة تجارية يوفر بديلاً للنقد أو الصكوك أو حوافز المنتجات للشركات التي ترغب في تقديم حوافز ومكافآت للموظفين أو المقاولين أو العملاء. البطاقات إما قابلة لإعادة الشحن أو غير قابلة لإعادة الشحن.

4. برنامج بطاقة الرعاية الصحية مسبقة الدفع

تم تصميم برنامج بطاقة الرعاية الصحية مسبقة الدفع لدعم مدفوعات نفقات الرعاية الصحية من خلال بطاقة مسبقة الدفع، قابلة لإعادة الشحن يمنحها صاحب العمل أو مقدم التأمين الصحي للموظف. يجب استخدام البطاقة فقط في رموز فئة تاجر الرعاية الصحية المحددة (MCC) وفقط لتغطية نفقات الرعاية الصحية المؤهلة.

5. برنامج بطاقة الرواتب مسبقة الدفع

يعد برنامج بطاقة الرواتب مسبقة الدفع بديلاً آمناً ومريحاً للدفع للموظفين أو المقاولين أو الوكلاء نقدًا أو بصكوك. يمكن استخدامه لأي شكل من أشكال التعويض، ولكنه لا يستخدم بشكل عام للمكافآت أو مدفوعات الحوافز (يرجى الاطلاع على برنامج الحوافز والمكافآت مسبقة الدفع أعلاه). من خلال الإيداع المباشر ودفع الفواتير عبر الإنترنت والوصول الفوري إلى معلومات الرصيد والمزيد من الأمان واسترداد الرصيد للبطاقات المفقودة أو المسروقة، يستفيد الموظفون أيضاً من البرنامج.

6. برنامج بطاقة الوجبات وقسائم الطعام مسبقة الدفع

تم تصميم برنامج بطاقة الوجبات وقسائم الطعام مسبقة الدفع لدعم الدفع مقابل المزايا الضريبية للوجبات و الأطعمة من خلال بطاقة مسبقة الدفع يمنحها صاحب العمل للموظف وفقاً للقانون المحلي والإرشادات التنظيمية لبرامج الوجبات والأطعمة. البرنامج محدود للاستخدام في رموز فئة تاجر الوجبات أو الأطعمة المحددة (MCCs) ويمكن استخدامه فقط لمصاريف الوجبات والأطعمة. قد تدعم بطاقة قسيمة الوجبات والأطعمة أنواعاً إضافية من المزايا الضريبية وفقاً للوائح المعمول بها.

7. برنامج بطاقة الأعمال مسبقة الدفع

برنامج بطاقة الأعمال مسبقة الدفع هو حل بطاقة يمكن استخدامه لدفع مجموعة من النفقات المتعلقة بالعمل:

- سفر الأعمال والترفيه.
- شراء السلع والخدمات.
- استبدال المصروفات النقدية.
- اجتماعات ووظائف العمل.

- Expenditures specific to projects
- Invitation travel
- Per diem for consultants and temporary employees

The Prepaid Business Card can be used as a standalone program or to supplement a commercial charge card, credit card or debit card program. It is funded by the business entity or small business owner that is the issuer’s customer (the “Company”) and the funds are owned by the Company.

Implementing a prepaid business card program is suitable when the Company wants a cost-effective method for paying business expenses, and an employee does not meet the Company’s criteria to receive a charge, or credit or debit card.

8. Prepaid Emergency Relief Program

The Prepaid Emergency Relief Program is designed to distribute emergency disaster relief funds to first responders (government or NGO personnel and/or volunteers) as well as beneficiaries designated by the government or NGO. The solution is designed to be deployed effectively and efficiently in response to a disaster within 24 hours of request from the entity responsible for program administration. The card includes features that make it an effective tool (for example, Instant Issued non-personalized card) for short term emergency payments.

9. Prepaid Government & Public Sector Program

The Prepaid Government and Public Sector Program is a card solution targeted at national, state and local governments and agencies. The purpose of the card is to:

1. Migrate social benefits disbursements from paper/cash/debit to electronic payments
2. Enable stricter fund management and allocation
3. Better manage distribution of multiple benefits to a single individual
4. Increase the convenience, security, and timeliness of payment delivery

10. Prepaid Youth Card Program

The Prepaid Youth Card Program is designed to provide a reloadable prepaid card to young persons who are at least [16] years of age. The card may be reloaded by the young person or via the account of a parent or other responsible adult. The card issuer will apply appropriate restrictions on the use of the card, for example, limiting cash access, setting parameters on how often the card can be reloaded, and maximum load amounts.

3.5 General Implementation Considerations

3.5.1 Guidelines to Issuers

(See appendix number 7)

3.5.2 Guidelines to Acquirers

(See appendix number 8)

- المصروفات الخاصة بالمشاريع.

- دعوة سفر.

- بدل يومي للاستشاريين والموظفين المؤقتين.

يمكن استخدام بطاقة الأعمال مسبقة الدفع كبرنامج مستقل أو لتكملة ملف بطاقة الائتمان التجارية أو بطاقة الائتمان أو برنامج بطاقة الخصم. يتم تمويله من قبل مؤسسة تجارية أو صاحب عمل (صغير) يكون هو عميل جهة الإصدار (“الشركة”) وتكون الأموال مملوكة للشركة.

يعد تنفيذ برنامج بطاقة الأعمال مسبقة الدفع مناسبًا عندما ترغب الشركة في طريقة فعالة من حيث التكلفة لدفع نفقات العمل، ولا يفي الموظف بمعايير الشركة لتلقي رسوم أو بطاقة ائتمان أو خصم.

8. برنامج بطاقة الإغاثة في حالات الطوارئ مسبقة الدفع

تم تصميم برنامج بطاقة الإغاثة في حالات الطوارئ مسبقة الدفع لتوزيع أموال الإغاثة في حالات الكوارث لأول المستجيبين (موظفي الحكومة أو المنظمات غير الحكومية و/ أو المتطوعين) وكذلك المستفيدين المعيّنين من قبل الحكومة أو المنظمات غير الحكومية. الحل مصمم ليتم نشره بفعالية وكفاءة للاستجابة للكوارث خلال 24 ساعة من الطلب من الجهة المسؤولة عن إدارة البرنامج. تتضمن البطاقة ميزات تجعلها أداة فعالة (على سبيل المثال، إصدار فوري للبطاقة غير المخصصة) لمدفوعات الطوارئ على المدى القصير.

9. برنامج بطاقة الحكومة والقطاع العام مسبقة الدفع:

برنامج بطاقة الحكومة والقطاع العام مسبقة الدفع هو حلول بطاقةية يستهدف الحكومات والوكالات الوطنية و المحلية. الغرض من البطاقة هو:

- ترحيل مدفوعات المنافع الاجتماعية من مدفوعات ورقية/ نقدية/ خصم إلى مدفوعات إلكترونية
- تفعيل إدارة الأموال وتخصيصها بشكل أكثر صرامة.
- إدارة أفضل لتوزيع الفوائد المتعددة على الفرد الواحد.
- زيادة الراحة والأمان والالتزام بمواعيد تسليم المدفوعات

10. برنامج بطاقة الشباب مسبقة الدفع:

تم تصميم برنامج بطاقة الشباب مسبقة الدفع لتوفير بطاقة مسبقة الدفع قابلة لإعادة الشحن للشباب الذين لا تقل أعمارهم عن [16] عامًا. قد يتم إعادة شحن البطاقة من قبل الشاب أو عبر حساب أحد الوالدين أو أي شخص بالغ مسؤول. ستطبق جهة إصدار البطاقة قيودًا مناسبة على استخدام البطاقة، على سبيل المثال، تقييد الوصول إلى النقود، وتعيين معلمات حول عدد المرات التي يمكن فيها إعادة شحن البطاقة، والحد الأقصى لمبالغ الشحن.

5.3 اعتبارات التنفيذ العامة

1.5.3 إرشادات لجهات الإصدار

(انظر الملحق رقم 7)

2.5.3 إرشادات للقابليين

(انظر الملحق رقم 8)

Appendix Number 1

If the entity performs any ser- vices identified as...	An entity is categorized as a...
Independent Sales Organization (ISO)	ISO Program Service
Third Party Processor (TPP)	TPP Program Service
Data Storage Entity (DSE)	DSE Program Service
Payment Service Provider (PSP)	PSP Program Service
Staged Digital Wallet Operator (SDWO)	SDWO Program Service
Digital Activity Service Provider (DASP)	DASP Program Service
Token Service Provider (TSP)	TSP Program Service
Merchant Monitoring Program (MPP)	MMP Program Service
Terminal Servicer (TS)	TS Program Service
3-D Secure Service Provider (3-DSSP)	3-D Secure Program Service

Appendix Number 2

General Debit Cards Strategy	
A. Foundational Layer: Core requirements The core requirements are mandatory and include: 1. Card-present payments 2. Zero Liability 3. Dual Interface Contact/Contactless (recommended) 4. Transaction alerts (recommended) 5. E-Commerce payments 6. Non face to face transactions (Manual entry)	
B. Value Added Benefits- These are points based benefits for individual product segments	Illustrative Value Added Benefits - Extended warranty - Spend alerts and control - Concierge services - T & E - Airport experiences (e.g. lounge privileges) - Travel Insurance - Mobile Phone Insurance - Car Rental - Rewards Programme (will be declared once available)

Appendix Number 3

Benefits description	A detailed description of what the service is
Supplier	Who is the provider? Is the benefit in-house or third party?
Issuer cost per year	What is the cost for providing the service?
Perceived cost by the cardholder	What would the cardholder pay on the open market?
Customer demographic	How does this benefit fit the user demographic and complement the associated product tier?

(الملحق رقم 1)

قيم رمز الخدمة

إذا نفذت الجهة أي خدمات محددة ك...	أن الجهة مصنفة ك...
منظمة المبيعات مستقلة (ISO)	خدمة برنامج منظمة المبيعات المستقلة
معالج الطرف الثالث (TPP)	خدمة برنامج معالج الطرف الثالث
جهة تخزين البيانات (DSE)	خدمة برنامج جهة تخزين البيانات
مقدم خدمة الدفع (PSP)	خدمة برنامج مقدم خدمة الدفع
مشغل المحفظة الرقمية المرحلية (SDWO)	خدمة برنامج مشغل المحفظة الرقمية المرحلية
مقدم خدمة النشاط الرقمي (DASP)	خدمة برنامج مقدم خدمة النشاط الرقمي
مقدم خدمة الترميز (TSP)	خدمة برنامج مقدم خدمة الترميز
برنامج مراقبة التاجر	خدمة برنامج مراقبة التاجر
خدمة المحطة (TS)	خدمة برنامج المحطة
مقدم الخدمة الآمنة ثلاثية الأبعاد (3-DSSP)	خدمة برنامج مقدم الخدمة الآمنة ثلاثية الأبعاد

(الملحق رقم 2)

الإستراتيجية العامة لبطاقات الخصم	
أ. الطبقة التأسيسية: المتطلبات الأساسية المتطلبات الأساسية إلزامية وتشمل: 1. مدفوعات البطاقة الموجودة 2. المسؤولية الصفرية\عدم تحمل المسؤولية 3. جهة اتصال مزدوجة / بدون اتصال (موصى بها) 4. تنبيهات المعاملات (موصى بها) 5. مدفوعات التجارة الإلكترونية 6. المعاملات غير المباشرة (الإدخال اليدوي)	
ب. فوائد القيمة المضافة هذه هي الفوائد القائمة على النقاط لقطاعات المنتجات الفردية	فوائد القيمة المضافة التوضيحية - ضمان ممدد - تنبيهات الإنفاق والتحكم - خدمات الاستقبال والإرشاد - T & E - تجارب المطار (مثل امتيازات الصالة) - تأمين السفر - تأمين الهاتف المحمول - تاجير سيارة - برنامج المكافآت (سيتم الإعلان عنه بمجرد توفره)

(الملحق رقم 3)

الإستراتيجية العامة لبطاقات الخصم

وصف الفوائد	وصف مفصل لماهية الخدمة
المورد	من هو المقدم؟ هل المنفعة داخلية أم طرف ثالث؟
تكلفة جهة الإصدار في السنة	ما هي تكلفة تقديم الخدمة؟
التكلفة المتصورة من قبل حامل البطاقة	ماذا سيدفع حامل البطاقة في السوق المفتوح؟
التوزيع السكاني للعملاء	كيف تتناسب هذه الفائدة مع التوزيع السكاني المستخدم وتكمل طبقة المنتج ذات الصلة؟

Appendix Number 4

Technical Requirements	
BIN	Specific Debit BIN Range(s)
Card Parameters	Mag-stripe with PIN Chip and PIN
PAN Length	16 or 19 digits
Card Technology	Mag-Stripe Hybrid Cards (EMV Chip and magnetic stripe both present) Dual Interface Chip Contact and Contactless
Mobile Payment Applications	A Debit PAN may be loaded in a mobile wallet (Digitized)
Cardholder Verification Method	Mag-Stripe only with Mandatory PIN Online PIN for contact chip transactions, and for contactless transactions above the CVM Limit
Acceptance	POS –purchases refunds, deposits ATM - ATM cash withdrawal using online authorization with PIN verification, refunds and depos- its E-commerce – online purchases, with authentication of the cardholder and refunds
Digital & Security Options	- EMV 3DS 2.0 - Biometric Authentication - Transaction alerts - Risk based authentication - Card-based controls (E.g. Card Freeze/Unfreeze, Budget Control, Channel Control) - Issuer support of ATM Transactions on Contactless Cards and Payment Devices

Appendix Number 5

Program Attributes	Explanation
Cardholder Terms & Conditions	Must explain how the Cardholder can access account balance information and the expiry date, and disclose all Cardholder fees, usage conditions and limitations as well as any other disclosures and information required under applicable law or regulation
Cardholder Access to Account Information	Must provide access to balance inquiry and transaction history through the Internet, a call center, or other methods as chosen by the issuer
Selective Authorization Options	Limitations on acceptance apply
Anti-Money Laundering Program	Must adhere to the applicable Anti-Money Laundering requirements

Appendix Number 6

Program Attributes	Explanation
Cardholder Terms & Conditions	Must explain how the Cardholder can access account balance information and the expiry date, and disclose all Cardholder fees, usage conditions and limitations as well as any other disclosures and information required under applicable law or regulation
Cardholder Access to Account Information	Must provide access to balance inquiry and transaction history through the Internet, a call center, or other methods as chosen by the issuer
Lost/Stolen Reporting	Limitations on acceptance apply
Customer Service	Must provide access to live customer service
Selective Authorization Options	Limitations on acceptance permitted according to the product type
Anti-Money Laundering Program	Must adhere to the applicable Anti-Money Laundering requirements

(الملحق رقم 4)

متطلبات تقنية	
رقم التعريف المصرفي	نطاق (نطاقات) رقم التعريف المصرفي للخصم المحدد
معلومات البطاقة	الشريط المغناطيسي مع شريحة رقم التعريف الشخصي ورقم التعريف الشخصي
طول رقم الحساب الأساسي	16 أو 19 رقمًا
تقنية البطاقة	الشريط المغناطيسي البطاقات الهجينة (شريحة EMV والشريط المغناطيسي موجودان) شريحة واجهة اتصال مزدوجة وبدون اتصال
تطبيقات الدفع بواسطة الهاتف المحمول	يمكن تحميل رقم الحساب الأساسي الخصم في محفظة الهاتف المحمول (رقمي)
طريقة التحقق من حامل البطاقة	الشريط المغناطيسي فقط مع رقم التعريف الشخصي الإلزامي رقم التعريف الشخصي عبر الإنترنت لمعاملات شريحة الاتصال، وللمعاملات بدون اتصال فوق حد CVM
القبول	نقاط البيع - استرداد المشتريات والودائع جهاز الصراف الآلي - السحب النقدي من أجهزة الصراف الآلي باستخدام التفويض عبر الإنترنت مع التحقق من رقم التعريف الشخصي، والمبالغ المستردة والودائع التجارة الإلكترونية - عمليات الشراء عبر الإنترنت ، مع مصادقة حامل البطاقة والمبالغ المستردة
الخيارات الرقمية و الأمنية	- EMV 3DS 2.0.0 - المصادقة البيومترية - تنبيهات المعاملات - المصادقة على أساس المخاطر - الضوابط المستندة إلى البطاقة (على سبيل المثال ، تجميد/ إلغاء تجميد البطاقة، التحكم في الميزانية، التحكم في القناة)
	دعم جهات الإصدار لمعاملات أجهزة الصراف الآلي على بطاقات بدون الإتصال وأجهزة الدفع

(الملحق رقم 5)

سمات البرنامج	التوضيح
شروط وأحكام حامل البطاقة	يجب توضيح كيف يمكن لحامل البطاقة الوصول إلى معلومات رصيد الحساب وتاريخ انتهاء الصلاحية، والإفصاح عن جميع رسوم حامل البطاقة وشروط وقيود الاستخدام بالإضافة إلى أي إفصاحات ومعلومات أخرى مطلوبة بموجب القانون أو اللوائح المعمول بها
وصول حامل البطاقة إلى معلومات الحساب	يجب أن يوفر إمكانية الوصول للاستعلام عن الرصيد، وسجل المعاملات عبر الإنترنت أو مركز الاتصال أو أي طرق أخرى حسبما تختاره جهة الإصدار
خيارات التفويض الانتقائية	تنطبق القيود على القبول
برنامج مكافحة غسيل الأموال	يجب الالتزام بمتطلبات مكافحة غسيل الأموال المعمول بها

(الملحق رقم 6)

سمات البرنامج	التوضيح
شروط وأحكام حامل البطاقة	يجب توضيح كيف يمكن لحامل البطاقة الوصول إلى معلومات رصيد الحساب وتاريخ انتهاء الصلاحية، والإفصاح عن جميع رسوم حامل البطاقة وشروط وقيود الاستخدام بالإضافة إلى أي إفصاحات ومعلومات أخرى مطلوبة بموجب القانون أو اللوائح المعمول بها
وصول حامل البطاقة إلى معلومات الحساب	يجب أن يوفر إمكانية الوصول إلى الاستعلام عن الرصيد وسجل المعاملات عبر الإنترنت أو مركز الاتصال أو أي طرق أخرى حسبما تختاره جهة الإصدار
الإبلاغ عن الفقدان/السرقه	يجب تقديم تقارير الفقدان/السرقه إلى جهة الإصدار
خدمة العملاء	يجب توفير إمكانية الوصول إلى خدمة العملاء المباشرة
خيارات التفويض الانتقائية	يسمح بالقيود على القبول وفقًا لنوع المنتج
برنامج مكافحة غسيل الأموال	يجب التقيد بمتطلبات مكافحة غسيل الأموال المعمول بها

Appendix Number 7

A. Licensing
- Receiving NUMO network package which includes: (Bin Request Form, Operating Procedures, Card Design Specifications, Processing Regulations, Tech. Specification for clearing & settlement files, Chargeback Rule Book, List of authorized Cards Manufacturers card suppliers) - Submit BIN Request Form to the National Scheme Operator - Open an Implementation Project to put the new BIN live - Switch the issuer to live operations for specific BINs - Sign licensing agreement and become a member in NUMO network
B. Card Production
Card Design - Before issuing cards bearing any NUMO brand mark, go through the Card Design Approval Process to make sure the Card complies with the card design requirements. - Create card design in compliance with network requirements. - Send card Artwork Digital Form for the suggested design, to get the network approval Card type approval and Personalization Validation test (PVT): - Prepare coding keys including (AC KEYS – SMI – SMC – PVK – CVK1 – CVK2) to be used in Card Personalization Process. - Order Chip Cards from authorized vendors by NUMO in addition to (EMV Letter of Approval) for those chips to confirm its compatibility with National Payment Scheme approved chips. - Request for (Certification Request) to be used upon personalizing test cards. - Provide the National Scheme Operator with 4 white plastic test cards to be tested by the network to pass the Personalization Validation test. - Contact National Scheme Operator to reserve test slot for (Host Certification) to test Bank Host technical readiness to integrate with the network and to pass all required test cases. - Contact National Scheme Operator to reserve test slot for (Clearing Certification) to test Bank’s technical readiness to receive Clearing Files and to pass all required test cases.
C. Production Set-up
- Verify that your issuer host systems are correctly processing NUMO Card transactions. If not supported, you will need to plan and execute system testing. - Carry out end-to-end validation that cards and all systems under the control of the issuer (e.g. authorization system, network interface, clearing interface, etc.) function correctly - Send a “Production Certificate Request “to the network to be signed by Certificate Authority. - Provide the National Scheme Operator with 4 cards issued on the bank’s production environment with the approved design to be tested by the network to pass the “Personalization Validation test” and approve the production artwork. - Highly recommended to perform a pilot and evaluate results prior to mass roll-out. This phase should be used to validate internal processes, cardholder experiences and acceptance.

Appendix Number 8

Contracting
- Define objectives and set-up Project Team - Put in place merchant agreements for NUMO Card acceptance and train your merchants - Use NUMO Card branding kit across all designated POI related to Acquirer
Production Set-up
- Verify that your acquirer host systems are correctly processing NUMO Cards transactions. If not supported, you will need to plan and execute system testing - Check your terminal infrastructure and, if an EMV kernel change is needed for activation of the debit product, perform chip terminal testing (Terminal Integration Test) through National Scheme Operator - Highly recommended to perform a pilot and evaluate results prior to starting full scale roll-out.

(الملحق رقم 7)

أ. الترخيص
- استلام حزمة شبكة نمو والتي تتضمن: (نموذج طلب رقم التعريف المصرفي، إجراءات التشغيل ، مواصفات تصميم البطاقة ، لوائح المعالجة ، المواصفات الفنية لملفات المقاصة والتسوية، دفتر قواعد رد المبالغ المدفوعة ، قائمة مصنعي البطاقات المعتمدين، موردي بطاقات) - تقديم نموذج طلب رقم التعريف المصرفي إلى مشغل شبكة الدفع المحلية - افتتاح مشروع تنفيذ لبدء تشغيل رقم التعريف المصرفي الجديد - تحويل جهة الإصدار إلى العمليات المباشرة لأرقام التعريف المصرفية المحددة - توقيع اتفاقية الترخيص لكي تصبح عضوًا في شبكة نمو.
ب. إنتاج البطاقة
تصميم البطاقة - قبل إصدار البطاقات التي تحمل علامة نموالتجارية، انتقل إلى عملية الموافقة على تصميم البطاقة للتحقق من توافق البطاقة مع متطلبات تصميم البطاقة. - أشئ تصميم بطاقة يتوافق مع متطلبات الشبكة. - أرسل نموذج عمل فني رقمي للبطاقة للتصميم المقترح، للحصول على موافقة الشبكة الموافقة على نوع البطاقة واختبار التحقق من التخصيص (PVT): - قم بإعداد مفاتيح الترميز بما في ذلك (AC KEYS - SMI - SMC - PVK - CVK1 - CVK2) لاستخدامها في عملية تخصيص البطاقة. - اطلب بطاقات الشرائح من البائعين المعتمدين من قبل نمو بالإضافة إلى (خطاب اعتماد EMV لتلك الشرائح لتأكيد توافقها مع الشرائح المعتمدة من شبكة الدفع المحلية. - اطلب استخدام (طلب الشهادة) عند تخصيص بطاقات الاختبار. - قم بتزويد مشغل شبكة الدفع المحلية بأربع بطاقات اختبار بلاستيكية بيضاء ليتم اختبارها من قبل الشبكة لاجتياز اختبار التحقق من صحة التخصيص. - اتصل بمشغل شبكة الدفع المحلية لحجز فتحة اختبار لـ (شهادة المضيف) لاختبار الاستعداد الفني للمصرف المضيف للتكامل مع الشبكة واجتياز جميع حالات الاختبار المطلوبة. - اتصل بمشغل شبكة الدفع المحلية لحجز فتحة اختبار لـ (شهادة المقاصة) لاختبار استعداد المصرف الفني لاستلام ملفات المقاصة واجتياز جميع حالات الاختبار المطلوبة.
ج. إعداد الإنتاج
- تحقق من أن أنظمة مضيف جهة الإصدار الخاصة بك تقوم بمعالجة معاملات بطاقة نمو بشكل صحيح. إذا لم تكن مدعومة ، فستحتاج إلى تخطيط اختبار النظام وتنفيذه. - قم بإجراء تحقق شامل من أن البطاقات وجميع الأنظمة الخاضعة لسيطرة جهة الإصدار (مثل نظام التفويض وواجهة الشبكة وواجهة المقاصة وما إلى ذلك) تعمل بشكل صحيح. - أرسل "طلب شهادة إنتاج" إلى الشبكة ليتم توقيعه من قبل المرجع المصدق. - قم بتزويد مشغل شبكة الدفع المحلية بأربع بطاقات صادرة حول بيئة الإنتاج بالمصرف مع التصميم المعتمد ليتم اختباره من قبل الشبكة لاجتياز"اختبار التحقق من التخصيص" والموافقة على العمل الفني للإنتاج. - يوصى بشدة إجراء تجربة وتقييم النتائج قبل النشر الشامل. يجب استخدام هذه المرحلة للتحقق من صحة العمليات الداخلية وتجارب حامل البطاقة والقبول.

(الملحق رقم 8)

المقاولات/التعاقد
- قم بتحديد الأهداف وأشئ فريق مشروع - قم بإبرام اتفاقيات التاجر لقبول بطاقة نمو وقم بتدريب التجار - استخدم مجموعة العلامات التجارية الخاصة ببطاقة نمو عبر جميع نقاط الاهتمام المحددة والمتعلقة بالقابل
إعداد الإنتاج
- تحقق من أن أنظمة مضيف القابل الخاصة بك تقوم بمعالجة معاملات بطاقة نمو بشكل صحيح. إذا لم تكن مدعومة ، فستحتاج إلى تخطيط اختبار النظام وتنفيذه. - تحقق من البنية التحتية للمحطة الخاصة بك ، وإذا كان تغيير EMV kernel مطلوبًا لتنشيط منتج الخصم، فقم بإجراء اختبار المحطة (اختبار تكامل المحطة) من خلال مشغل شبكة الدفع المحلية - يوصى بشدة بإجراء تجربة وتقييم النتائج قبل بدء النشر على نطاق واسع.

**BOOK 3
TECHNICAL
OPERATIONAL
STANDARDS**

كتاب 3
معايير التشغيل الفنية

Regulatory Rules of The Libyan National Payment Scheme

BOOK 3 TECHNICAL OPERATIONAL STANDARDS

Table of Contents

Chapter 1	547
CARD SPECIFICATIONS, TERMS, AND DESIGNING STANDARDS	547
Introduction for Card Design and Specifications	547
1.1 NUMO Logo	547
1.1.1 Unique Characteristics of NUMO logo	547
1.1.2 Printing on Cards	549
1.1.3 Logo Placement on the Card	549
1.1.4 Image Resolution	549
1.1.5 Coexistence of NUMO logo with other brands or logos	549
1.2 Card Specifications	551
1.2.1 Standardizations followed for the Card	551
1.2.2 Quality requirements	551
1.3 Signature Panel Specifications	551
1.3.1 Main Characteristics	551
1.3.2 Signature Panel Dimensions	551
1.3.3 Signature Panel Location on the Card	553
1.3.4 Card Verification Value CVV2	553
1.3.5 Main Characteristics	553
1.4 Magnetic-Stripe Specifications	553
1.4.1 Magstripe Requirements	553
1.4.2 Distortion on Magstripe surface	553
1.4.3 Positioning the Magstripe	555

القواعد التنظيمية لشبكة الدفع المحلية الليبية

كتاب 3 معايير التشغيل الفنية

جدول المحتويات

الفصل 1	546
مواصفات البطاقة وشروطها ومعايير التصميم	546
مقدمة لتصميم البطاقة ومواصفاتها	546
1.1 شعار نمو	546
1.1.1 الخصائص الفريدة لشعار نمو	546
2.1.1 الطباعة على البطاقات	548
3.1.1 موضع الشعار على البطاقة	548
4.1.1 دقة الصورة	548
5.1.1 تواجد شعار نمو مع العلامات التجارية أو الشعارات الأخرى	548
2.1 مواصفات البطاقة	550
1.2.1 المعايير المتبعة للبطاقة	550
2.2.1 متطلبات الجودة	550
3.1 مواصفات لوحة التوقيع	550
1.3.1 الخصائص الرئيسية	550
2.3.1 أبعاد لوحة التوقيع	550
3.3.1 موقع لوحة التوقيع على البطاقة	552
4.3.1 قيمة التحقق من البطاقة CVV2	552
5.3.1 الخصائص الرئيسية	552
4.1 مواصفات الشريط المغناطيسي	552
1.4.1 متطلبات الشريط المغناطيسي	552
2.4.1 التشويه على سطح الشريط المغناطيسي	552
3.4.1 وضع الشريط المغناطيسي	554

1.5 Card data specifications and characteristics	555
1.5.1 Personalization Techniques	555
1.5.1.1 Personalization Techniques for Embossed Cards	555
1.5.1.2 Personalization Techniques for Unembossed Cards	555
1.5.2 Bank Logo and Brand Name	555
1.5.3 Cardholder Name	555
1.5.4 Presentation of Numbers	557
1.5.5 Customer Service Contacts	557
1.5.6 Card Validity	557
1.5.7 Issuer Bank Name	557
1.5.8 PAN Presentment on Card	557
1.5.9 Contactless Cards	557
1.5.9.1 Main Characteristics	557
1.5.9.2 Restrictions	559
1.6 Applying Invisible Ink and Hologram	559
1.6.1 Possibility of Using the Invisible Ink	559
1.6.2 Securing and Printing NUMO logo with invisible INK	559
1.6.3 Characteristics of The Invisible Ink	559
1.6.4 Usage of Hologram for NUMO Cards	559
1.7 Issuer Bank Responsibilities	561
Chapter 2 - Chargeback Rules	561
2.1. Dispute Resolution Process Overview	561
2.1.1.Reason Codes	563
2.1.1.2Additional Codes to Pre-Arbitration Creation	563
2.1.1.2Additional Codes to Pre-Arbitration Creation	565
2.1.1.3Chargeback Rejection Codes	565
2.1.2. Time Frames	565
2.1.3. Required Documents	565
2.1.4. Required Comment	567
2.1.5. Disputed Amount	567
2.1.6. Settlement of dispute and exchange of funds	567
2.1.7. Chargebacks for Reissued Cards	567
2.2. Chargeback Creation and Rejection	569
2.2.1. Authorization Dispute Group	569
2.2.1.1 Expired Card	569
2.2.1.2 Chargeback Rejection Conditions	569
2.2.1.3 No Authorization / Declined Authorization	571

5.1 مواصفات وخصائص بيانات البطاقة	554
1.5.1 تقنيات التخصيص	554
1.1.5.1 تقنيات التخصيص للبطاقات المنقوشة	554
2.1.5.1 تقنيات التخصيص للبطاقات غير المنقوشة	554
2.5.1 شعار المصرف واسم العلامة التجارية	554
3.5.1 اسم حامل البطاقة	554
4.5.1 عرض الأرقام	556
5.5.1 جهات اتصال خدمة العملاء	556
6.5.1 صلاحية البطاقة	556
7.5.1 اسم مصرف جهة الإصدار	556
8.5.1 عرض رقم الحساب الأساسي على البطاقة	556
9.5.1 البطاقات غير المتصلة	556
1.9.5.1 الخصائص الرئيسية	556
2.9.5.1 القيود	558
6.1 تطبيق الحبر غير المرئي والهولوجرام	558
1.6.1 إمكانية استخدام الحبر غير المرئي	558
2.6.1 تأمين وطباعة شعار نمو بحبر غير مرئي	558
3.6.1 خصائص الحبر غير المرئي	558
4.6.1 استخدام الهولوجرام لبطاقات نمو	558
7.1 مسؤوليات المصرف المصدر	560
الفصل 2 – قواعد رد المبالغ المدفوعة	560
1.2 نظرة عامة حول عملية حل النزاعات	560
1.1.2 رموز السبب	562
1.1.1.2 رموز سبب إنشاء رد المبالغ المدفوعة	562
2.1.1.2 رموز إضافية لإنشاء ما قبل التحكيم	564
3.1.1.2 رموز رفض رد المبالغ المدفوعة	564
2.1.2 الأطر الزمنية	564
3.1.2 المستندات المطلوبة	564
4.1.2 التعليق المطلوب	566
5.1.2 المبلغ المتنازع عليه	566
6.1.2 تسوية المنازعات وتبادل الأموال	566
7.1.2 عمليات رد المبالغ المدفوعة للبطاقات المعاد إصدارها	566
2.2 إنشاء رد المبالغ المدفوعة ورفضها	568
1.2.2 مجموعة نزاعات التفويض	568
1.1.2.2 بطاقة منتهية الصلاحية	568
2.1.2.2 شروط رفض رد المبالغ المدفوعة	568
3.1.2.2 لا يوجد تفويض / تفويض مرفوض	570

2.2.1.4 Card Number Not Issued	577
2.2.2 Customer Claims Group	579
2.2.2.1 Goods or Services Were Either Not as Described or Defective	579
2.2.2.2 Requesting Goods or Services Not Received.....	585
2.2.2.3 Credit Not Received	593
2.2.2.4 Recurring Transaction.....	597
2.2.2.5 Subsequent Transaction Disputed.....	603
2.2.2.6 Lodging or Vehicle Rental “No-Show” Charged / Deposit Not Refunded	607
2.2.2.7 Transaction Did Not Complete	611
2.2.2.8 Credit Posted as a Purchase.....	615
2.2.3 Fraud Dispute Group	619
2.2.3.1 No Cardholder Authorization	619
2.2.3.2 Chip Processing Rules.....	627
2.2.3.3 Multiple Fraudulent Transactions	631
2.2.4 Point of Interaction Error	635
2.2.4.1 Cash Not Received	635
2.2.4.2 Paid twice with the same Card.....	639
2.2.4.3 Paid by Other Means	643
2.2.4.4 Transaction amount is different.....	645
2.2.4.5 Late Presentment.....	651
2.2.4.6 ATM deposit was not posted to Card balance	655
2.2.4.7 POS deposit was not posted to Card balance	659
2.3 Pre-Arbitration and Arbitration Case Filing	663
2.3.1 Overview	663
2.3.2 Issuer Submission of a Pre-Arbitration Case.....	663
2.3.2.1 Cardholder Dispute-Cardholder Reasserts Claim	663
2.3.2.2 Authorization Dispute Group – Invalid Chargeback Rejection	665
2.3.2.3 Cardholder Claims Group – Invalid Chargeback Rejection	667
2.3.2.4 No Cardholder Authorization – Invalid Chargeback Rejection	667
2.3.2.5 Chip Processing Rules – Invalid Chargeback Rejection.....	669
2.3.2.6 Point of Interaction Error – Invalid Chargeback Rejection	669
2.3.2.7 Required Rejection Documents were illegible/Unrelated/Incomplete.....	669
2.3.2.8 Required Rejection Documents were not received	669
2.3.2.9 Change of Chargeback Reason to an Authorization Dispute Group	669
2.3.2.10 Change of Chargeback Reason to a Customer Claims Group Chargeback	671
2.3.2.11 Change of Chargeback Reason to a No Cardholder Authorization Chargeback	671
2.3.2.12 Change of Chargeback Reason to a Processing Error Group Chargeback	673

4.1.2.2 رقم البطاقة غير صادر	576
2.2.2 مجموعة مطالبات العملاء	578
1.2.2.2 السلع أو الخدمات إما غير مطابقة للوصف أو معيبة	578
2.2.2.2 طلب بضائع أو خدمات لم يتم استلامها	584
3.2.2.2 لم يتم استلام الائتمان	592
4.2.2.2 معاملة متكررة	596
5.2.2.2 المعاملات اللاحقة المتنازع عليها	602
6.2.2.2 لم يتم رد ايداع رسوم الإقامة أو استئجار المركبات “عدم الحضور”/ الإيداع	606
7.2.2.2 المعاملة لم تكتمل	610
8.2.2.2 الائتمان منشور على أنه شراء	614
3.2.2 مجموعة منازعات الاحتيال	618
1.3.2.2 لا يوجد تصريح من حامل البطاقة	618
2.3.2.2 قواعد معالجة الشريحة	626
3.3.2.2 معاملات احتيالية متعددة	630
4.2.2 خطأ نقطة التفعيل (التفاعل)	634
1.4.2.2 لم يتم قبض النقود	634
2.4.2.2 تكرار عملية الدفع بنفس البطاقة	638
3.4.2.2 الدفع بوسائل أخرى	642
4.4.2.2 الاختلاف في مبلغ المعاملة.....	646
5.4.2.2 التقديم المتأخر	650
6.4.2.2 لم يتم ترحيل إيداع جهاز الصراف الآلي إلى رصيد البطاقة	654
7.4.2.2 لم يتم ترحيل إيداع نقاط البيع إلى رصيد البطاقة	658
3.2 رفع دعوى ما قبل التحكيم والتحكيم	662
1.3.2 نظرة عامة	662
2.3.2 تقديم جهة الإصدار لدعوى ما قبل التحكيم	662
1.2.3.2 نزاع حامل البطاقة - يعيد حامل البطاقة تأكيد المطالبة	662
2.2.3.2 مجموعة منازعات التفويض - رفض غير صالح لرد المبالغ المدفوعة	664
3.2.3.2 مجموعة مطالبات حامل البطاقة - رفض غير صالح لرد المبالغ المدفوعة	666
4.2.3.2 لا يوجد تصريح من حامل البطاقة - رفض غير صالح لرد المبالغ المدفوعة	666
5.2.3.2 قواعد معالجة الشريحة - رفض غير صالح لرد المبالغ المدفوعة	668
6.2.3.2 خطأ في نقطة التفاعل - رفض غير صالح لرد المبالغ المدفوعة.....	668
7.2.3.2 مستندات الرفض المطلوبة غير مقروءة / غير ذات صلة/ غير كاملة	668
8.2.3.2 لم يتم استلام مستندات الرفض المطلوبة	668
9.2.3.2 تغيير سبب رد المبالغ المدفوعة إلى مجموعة نزاعات التفويض	668
10.2.3.2 تغيير سبب رد المبالغ المدفوعة إلى مجموعة مطالبات العملاء المتعلقة برد المبالغ المدفوعة	670
11.2.3.2 تغيير سبب رد المبالغ المدفوعة إلى عدم تفويض حامل البطاقة لرد المبالغ المدفوعة	670
12.2.3.2 تغيير سبب رد المبالغ المدفوعة إلى مجموعة أخطاء في المعالجة.....	672

2.3.3 Acquirer Response to a Pre-Arbitration Case	673
2.3.4 Issuer Submission of a Pre-Arbitration Case	673
2.3.5 National Scheme Operator Review Process	673
2.4 Compliance / Non Compliance	675
2.4.1 Missing, Invalid or Inaccurate Authorization Data	675
2.4.2 Inaccurate Clearing Data that Restricts Chargeback Cycles	677
2.4.3 Interchange Reimbursement Fee	679
2.4.4 All Other Rules Violations	679
2.4.5 National Scheme Operator Review Process	681
Chapter 3 - Interchange and Pricing	681
3.1 Fee Types	681
3.2 INTERCHANGE AND SERVICE FEES	681
3.2.1 Interchange Reimbursement Fees – Overview	681
3.2.2 Scheme Determines Interchange Reimbursement Fees Rates	681
3.2.3 Cost Studies	683
3.2.4 Allocation of Expenses	683
3.2.5 Compliance with a Cost Study	683
3.3 Interchange Reimbursement Fees Overview	683
3.3.1 Fee Tiers	683
3.3.2 Fee Structure	685
3.4 General Interchange Reimbursement Fees Requirements	685
3.5 Interchange Reimbursement Fees Rates	685
3.6 Interchange Reimbursement Fees Programs	685
3.7 Interchange Reimbursement Fee Adjustments	685
3.8 Interchange Reimbursement Fee-related Fines	685
3.9 Member Fee Collection and Funds Disbursement	687
3.10 Fee Collection	687
3.11 SCHEME FEES	687
3.11.1 Scheme Fees – General	687
3.11.2 Taxes and Other Charges	689
3.11.3 Scheme Fees – Rates	689
3.11.4 Scheme Fee Collection and Funds Disbursement	689
3.11.5 Fee Assessment and Responsibility	689
Chapter 4 – eCommerce and Digital Services	691
PART I – eCommerce & related service	691
4.1 Introduction	691
4.2 eCommerce Considerations & Eco System Components	691

رد القابل على دعوى ما قبل التحكيم	672
تقديم جهة الإصدار لدعوى ما قبل التحكيم	672
عملية مراجعة مشغل شبكة الدفع المحلية	672
الامتثال / عدم الامتثال	674
بيانات التفويض مفقودة أو غير صحيحة أو غير دقيقة	674
بيانات المقاصة غير الدقيقة التي تقيد دورات رد المبالغ المدفوعة	676
رسوم السداد المتبادل	678
جميع انتهاكات القواعد الأخرى	678
عملية مراجعة مشغل شبكة الدفع المحلية	680
الفصل 3 – التبادل والتسعير	680
أنواع الرسوم	680
رسوم التبادل والخدمة	680
رسوم سداد التبادل - نظرة عامة	680
يحدد النظام معدلات رسوم السداد التبادلية	680
دراسات التكلفة	682
تخصيص المصروفات	682
الامتثال لدراسة التكلفة	682
نظرة عامة على رسوم سداد التبادل	682
مستويات الرسوم	682
هيكل الرسوم	684
المتطلبات العامة لسداد رسوم التبادل	684
معدلات رسوم سداد التبادل	684
برامج رسوم السداد التبادلية	684
تعديلات رسوم السداد التبادلية	684
الغرامات المتعلقة بدفع رسوم التبادل	684
تحصيل رسوم الأعضاء وصرف الأموال	686
تحصيل الرسوم	686
رسوم الشبكة	686
رسوم الشبكة – عام	686
الضرائب والرسوم الأخرى	688
رسوم الشبكة – الأسعار	688
تحصيل رسوم النظام وصرف الأموال	688
تقييم الرسوم والمسؤولية	688
الفصل 4 – التجارة الإلكترونية والخدمات الرقمية	690
الجزء الأول - التجارة الإلكترونية والخدمات ذات الصلة	690
مقدمة	690
اعتبارات التجارة الإلكترونية ومكونات النظام البيئي	690

4.2.1 eCommerce Considerations	691
4.2.2 Eco System Components	695
4.2.3 Acquirers and Merchants Obligations	697
PART II – Cards Digitization and Mobile Wallets	699
4.3 Mobile Payment Devices	699
4.3.1 Wallet Definition	699
4.3.2 Wallet enabled services	699
4.3.3 Wallet management server	701
4.3.4 Wallet service provider	701
4.3.5 Consumer Device Cardholder Verification Method (CDCVM)	701
4.3.6 Implementation Guidelines & Security Requirements	703
4.3.7 Issuer Banks Responsibilities	703
4.3.8 Acceptance of Digitized Payments	703
4.3.9 Acquirers Responsibilities	703
4.3.10 Recurring Payments & Card On File	703
PART III – QR Code	705
QR Code consolidated specs and definitions	705
QR Code Merchant presented	705
QR Code Consumer presented	707
QR Code various components	709
PART IV – Rules and Operation considerations	709
4.4 NSO Role for eCommerce & Digitized Payment Services	709
4.5 Compliance & Risk Factors	711
4.6 Generic Rules for Cards Tokenization	711
4.7 Clearing & Settlement for eCommerce & Digital Payment services	713
4.7.1 eCommerce clearing & Settlement	713
4.7.2 Mobile Digital payments clearing and settlement	713
4.8 Linked Value-added services	713
Appendix number (1)	716
Appendix number (2)	716
Appendix number (3)	716
Appendix number (4)	716
Appendix number (5)	716
Appendix number (6)	717
Appendix number (7)	717
Appendix number (8)	717
Appendix number (9)	717

1.2.4 اعتبارات التجارة الإلكترونية	690
2.2.4 مكونات النظام البيئي	694
3.2.4 التزامات القابلين والتجار	696
الجزء الثاني - رقمنة البطاقات والمحافظ المحمولة	698
3.4 أجهزة الدفع عبر الهاتف المحمول	698
1.3.4 تعريف المحفظة	698
2.3.4 الخدمات الممكنة للمحفظة	698
3.3.4 خادم إدارة المحفظة	700
4.3.4 مقدم خدمة المحفظة	700
5.3.4 طريقة التحقق من حامل بطاقة جهاز المستهلك (CDCVM)	700
6.3.4 إرشادات التنفيذ ومتطلبات الأمان	702
7.3.4 مسؤوليات المصارف المصدرة	702
8.3.4 قبول المدفوعات الرقمية	702
9.3.4 مسؤوليات القابلين	702
10.3.4 المدفوعات المتكررة والبطاقة في الملف	702
الجزء الثالث - رمز الاستجابة السريعة	704
المواصفات والتعاريف الموحدة لرمز الاستجابة السريعة	704
رمز الاستجابة السريعة للتاجر	704
رمز الاستجابة السريعة للمستهلك	706
مكونات مختلفة لرمز الاستجابة السريعة	708
الجزء الرابع - القواعد واعتبارات التشغيل	708
4.4 دور مشغل شبكة الدفع المحلية في التجارة الإلكترونية وخدمات الدفع الرقمية	708
5.4 الامتثال وعوامل الخطر	710
6.4 قواعد عامة لترميز البطاقات	710
7.4 المقاصة والتسوية للتجارة الإلكترونية وخدمات الدفع الرقمي	712
1.7.4 . مقاصة وتسوية التجارة الإلكترونية	712
2.7.4 . مقاصة وتسوية المدفوعات الرقمية المتنقلة	712
8.4 . خدمات القيمة المضافة المرتبطة	712
الملحق رقم (1)	716
الملحق رقم (2)	716
الملحق رقم (3)	716
الملحق رقم (4)	716
الملحق رقم (5)	716
الملحق رقم (6)	717
الملحق رقم (7)	717
الملحق رقم (8)	717
الملحق رقم (9)	717

Appendix number (10)	717
Appendix number (11)	718
Appendix number (12)	718
Appendix number (13)	718
Appendix number (14)	718
Appendix number (15)	719
Appendix number (16)	719
Appendix number (17)	719
Appendix number (18)	720
Appendix number (19)	720
Appendix number (20)	720
Appendix number (21)	721
Appendix number (22)	721
Appendix number (23)	721
Appendix number (24)	722
Appendix number (25)	722
Appendix number (26)	722
Appendix number (27)	722
Appendix number (28)	723

الملحق رقم (10)	717
الملحق رقم (11)	718
الملحق رقم (12)	718
الملحق رقم (13)	718
الملحق رقم (14)	718
الملحق رقم (15)	719
الملحق رقم (16)	719
الملحق رقم (17)	719
الملحق رقم (18)	720
الملحق رقم (19)	720
الملحق رقم (20)	720
الملحق رقم (21)	721
الملحق رقم (22)	721
الملحق رقم (23)	721
الملحق رقم (24)	722
الملحق رقم (25)	722
الملحق رقم (26)	722
الملحق رقم (27)	722
الملحق رقم (28)	723

Chapter 1 Membership CARD SPECIFICATIONS, TERMS, AND DESIGNING STANDARDS. Introduction for Card Design and Specifications

This Chapter covers the standards related to cards, technical specifications and conditions that must be met and verified for printing cards, as well as conditions or considerations for issuing through Issuer Banks.

The brand name and logo of “NUMO” are trademarks of the National Payments System. NUMO’s trademarks may not be used in connection with any product or service that does not belong to the State of Libya or by an entity other than its representative in the name of the National Scheme Operator in any way that would cause confusion among customers or in any way that disparages or discredits the National Scheme Operator in the state of Libya and its subsidiaries and affiliates.

The National Scheme Operator is the representative of the brand and the party responsible for setting the visible rules and conditions for the cards as well as the technical specifications and rules related to the issued cards.

This Chapter provides a detailed explanation of the conditions for issuance of magnetic stripe cards, as well as the technical conditions to be considered when issuing smart cards of all types (contact / contactless). As such the Chapter is identified as the main reference for card issuers as well as personalization centers issuing on behalf of issuer Banks.

Summary of Changes (See appendix number 1)

1.1 NUMO Logo

Product name has been extracted through the initials of National Scheme Operator represented in Arabic letters resulting in the name of (نمو), which gives in translation a continuous growing, and the reflected logo in linked circles should represent tying up the financial institutions through the National Scheme Operator.

1.1.1 Unique Characteristics for NUMO logo

- The Colored logo for all light backgrounds
(See appendix number 2)
- The black/white logo for all dark or mixed backgrounds
(See appendix number 3)
- Proportional dimensions while using the logo
(See appendix number 4)

الفصل 1 مواصفات البطاقة وشروطها ومعايير التصميم مقدمة لتصميم البطاقة ومواصفاتها

يغطي هذا الفصل المعايير المتعلقة بالبطاقات والمواصفات الفنية والشروط التي يجب استيفاؤها والتحقق منها لطباعة البطاقات، وكذلك شروط أو اعتبارات الإصدار من خلال بنوك جهة الإصدار.

اسم العلامة التجارية وشعار “نمو” هما علامتان تجاريتان لنظام المدفوعات المحلي. لا يجوز استخدام علامات نمو التجارية فيما يتعلق بأي منتج أو خدمة لا تنتمي إلى دولة ليبيا أو من قبل كيان آخر غير ممثلها باسم مشغل شبكة الدفع المحلية بأي طريقة من شأنها أن تسبب ارتباكًا بين العملاء أو بأي شكل من الأشكال تنتقص أو تشوه سمعة مشغل شبكة الدفع المحلية في دولة ليبيا والشركات الفرعية والشركات التابعة له.

مشغل شبكة الدفع المحلية هو ممثل العلامة التجارية والطرف المسؤول عن وضع القواعد والشروط المرئية للبطاقات وكذلك المواصفات الفنية والقواعد المتعلقة بالبطاقات الصادرة.

يقدم هذا الفصل شرحاً مفصلاً لشروط إصدار البطاقات ذات الشريط المغناطيسي، فضلاً عن الشروط الفنية التي يجب مراعاتها عند إصدار البطاقات الذكية بجميع أنواعها (المتصلة / غير المتصلة). على هذا النحو، تم تحديد هذا الفصل باعتباره المرجع الرئيسي لمصدري البطاقات بالإضافة إلى مراكز التخصيص التي تصدر نيابة عن بنوك جهة الإصدار.

ملخص التغييرات (انظر الملحق رقم 1)

1.1 شعار نمو

تم استخلاص اسم المنتج من خلال الأحرف الأولى لمشغل شبكة الدفع المحلية ممثلة بأحرف عربية مما ينتج عنه اسم نمو مما يعطي ترجمة نمواً مستمراً، والشعار المنعكس في الدوائر المرتبطة يجب أن يمثل ربط المؤسسات المالية من خلال مشغل شبكة الدفع المحلية .

1.1.1 الخصائص الفريدة لشعار نمو

- الشعار الملون لجميع الخلفيات الفاتحة
(انظر الملحق رقم 2)
- الشعار الأسود/ الأبيض لجميع الخلفيات الداكنة أو المختلطة
(انظر الملحق رقم 3)
- الأبعاد النسبية عند استخدام الشعار
(انظر الملحق رقم 4)

1.1.2 Printing on Cards

From the aforementioned, the symbol cannot be used in printing on cards except through the backgrounds and colors placed, which form a harmony according to the background used in the issued card.

The logo may not be shown in any of the following ways when printing:

Cannot be used diagonally.

(See appendix number 5)

Cannot change its' dimensions without consideration to the early set proportions.

(See appendix number 6)

The logo shape cannot be squeezed vertically without consideration to the early stated dimensions.

(See appendix number 7)

No other colors can be used other than the early stated colors.

1.1.3 Logo Placement on the Card

The below figure specifies logo placement on the card.

(See appendix number 8)

1. Dimensions must be considered during the logo placement to consider the edges to be set with a distance equivalent to the width of the logo divided by 8.

(See appendix number 9)

2. Logo must be represented in front right corner of the card with consideration to card edges or to be presented following the Issuer Bank name.

(See appendix number 10)

3. Example of Logo presentment

(See appendix number 11)

1.1.4 Image Resolution

Final resolution when creating artwork must not be less than 150 dpi@100% of final output size, and the resolution must be at 25%, but make sure that the resolutions are sufficient to be increased to 400%; this will avoid any pixilation of the image in case of low-resolution files.

Converting a low-resolution image to a higher resolution is not accepted as quality will decrease often dramatically; this will result in a poor-quality image. All images should be in CMYK format.

1.1.5 Coexistence of NUMO logo with other brands or logos

Any design that attaches another logo to any of the payment networks will not be accepted if it appears in a value or appearance that exceeds the “NUMO” logo.

In the event that approval is obtained for the presence of a logo for a payment network or a logo for a sponsor from the National Scheme Operator, the design must be taken into consideration so that the logo design is separated by a distance estimated at the size of the logo symbol, divided by 4.

During the displacement of any other logo accompanying the NUMO logo, the other logo must not precede the NUMO logo in presence on the card.

(See appendix number 12)

2.1.1 الطباعة على البطاقات

مما سبق لا يمكن استخدام الرمز في الطباعة على البطاقات إلا من خلال الخلفيات والألوان الموضوعة والتي تشكل تناغمًا حسب الخلفية المستخدمة في البطاقة الصادرة. قد لا يظهر الشعار بأي من الطرق التالية عند الطباعة:

لا يمكن استخدامه بشكل مائل.

(انظر الملحق رقم 5)

لا يمكن تغيير أبعاده دون النظر إلى النسب المحددة سابقاً.

(انظر الملحق رقم 6)

لا يمكن ضغط شكل الشعار عمودياً دون مراعاة الأبعاد المذكورة سابقاً.

(انظر الملحق رقم 7)

لا يمكن استخدام ألوان أخرى غير الألوان المذكورة سابقاً.

3.1.1 موضع الشعار على البطاقة

يوضح الشكل أدناه موضع الشعار على البطاقة.

(انظر الملحق رقم 8)

1. يجب مراعاة الأبعاد أثناء وضع الشعار للنظر في تعيين الحواف بمسافة تعادل عرض الشعار مقسومًا على 8.

(انظر الملحق رقم 9)

2. يجب تمثيل الشعار في الزاوية اليمنى الأمامية للبطاقة مع مراعاة حواف البطاقة أو تقديمه بعد اسم مصرف جهة الإصدار.

(انظر الملحق رقم 10)

3. مثال على عرض الشعار

(انظر الملحق رقم 11)

4.1.1 دقة الصورة

يجب ألا تقل الدقة النهائية عند إنشاء عمل فني عن 150 نقطة في البوصة @100% من حجم الإخراج النهائي، ويجب أن تكون الدقة عند 25%، ولكن يجب التأكد من أن الدقة كافية للزيادة إلى 400%؛ سيؤدي ذلك إلى تجنب أي تشوه للصورة في حالة وجود ملفات منخفضة الدقة. لا يُقبل تحويل صورة منخفضة الدقة إلى دقة أعلى لأن الجودة غالبًا ما تنخفض بشكل كبير؛ سينتج عن ذلك صورة ذات جودة رديئة. يجب أن تكون جميع الصور بتنسيق CMYK.

5.1.1 تواجد شعار نمو مع العلامات التجارية أو الشعارات الأخرى

لن يتم قبول أي تصميم يرفق شعارًا آخر بأي من شبكات الدفع إذا ظهر بقيمة أو مظهر يتجاوز شعار نمو.

في حالة الحصول على الموافقة لوجود شعار لشبكة دفع أو شعار لراعي من مشغل شبكة الدفع المحلية، يجب مراعاة التصميم بحيث يتم فصل تصميم الشعار بمسافة تقدر بحجم رمز الشعار مقسومًا على 4.

أثناء إزاحة أي شعار آخر مصاحب لشعار نمو، يجب ألا يسبق الشعار الآخر شعار نمو الموجود على البطاقة.

(انظر الملحق رقم 12)

1.2 Card Specifications

1.2.1 Standardizations followed for the Card

1. It is a must that card dimension is correspondent to International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 (Identification Cards-Physical characteristics).
2. It is a must that the placement of the chip on the card follows ISO/IEC 7816 (Identification Cards- Integrated circuit cards).If the card dimension figure below is not identical to ISO/IEC standards; the ISO/IEC standards have the superiority.
3. The chip on the card must meet the applicable EMV and/or contactless specifications.
4. In case of using other materials, constructions, and characters, nothing will be acceptable unless it follows the requirements of durability, quality and reliability of ISO/ IEC Standards.
5. The next figure shows the height, and thickness width of the card.
(See appendix number 13)
6. In the event that contactless card services are implemented using NFC technology, the rules established by ISO/IEC 14443 standards for this purpose must be followed and implementation scopes for Kernels should be applied after the review made by the National Scheme Operator.

1.2.2 Quality requirements

There must be commitment of the main quality demands, as shown in the next table.
(See appendix number 14)

1.3 Signature Panel Specifications

This part describes the parameters for NUMO card and specifies the requirements for signature panel on card. The signature panel is created for card owner signature.

1.3.1 Main Characteristics

The main characteristics of signature panels are:

- White and clear
- Tamper- evident and safe signature panel foil that meets the highest standards
- demanded by the bank card Industry. It would be accepted to be printed on the back
- side of the card along with card design as a transparent signature panel
- Designed to accept all types of ink signature
- Seeking the legibility of the cardholder’s signature, the issuer must ensure that the colours of NUMO signature panel provide sufficient contrast with black and blue ink.

1.3.2 Signature Panel Dimensions

The size of the signature panel is the responsibility of the issuer, but it is recommended that it is at least 26.0 mm wide and 7.0 mm high.

NUMO Signature Panel may include the extended tab as a part of it for printing the CVV2 Value.

(See appendix number 15)

2.1 مواصفات البطاقة

1.2.1 المعايير المتبعة للبطاقة

1. من الضروري أن يكون بُعد البطاقة متوافقًا مع المنظمة الدولية للتوحيد القياسي (ISO) اللجنة الكهروتقنية الدولية 7810 ((IEC) (بطاقات التعريف - الخصائص الفيزيائية).
2. من الضروري أن يكون موضع الشريحة على البطاقة يتبع ISO / IEC 7816 (بطاقات التعريف - بطاقات الدوائر المتكاملة) إذا كان رقم أبعاد البطاقة أدناه غير مطابق لمعايير ISO / IEC؛ فمعايير ISO / IEC لها الأفضلية.
3. يجب أن تلمي الشريحة الموجودة على البطاقة مواصفات EMV و/أو المواصفات غير المتصلة المطبقة.
4. في حالة استخدام مواد وإنشاءات وحروف أخرى، لن يكون أي شيء مقبولًا إلا إذا كان يتبع متطلبات المتانة والجودة والموثوقية لمعايير ISO / IEC.
5. يوضح الشكل التالي ارتفاع وسمك عرض البطاقة.
(انظر الملحق رقم 13)
6. في حالة تنفيذ خدمات البطاقات غير المتصلة باستخدام تقنية NFC، يجب اتباع القواعد الموضوعة بواسطة معايير ISO / IEC 14443 لهذا الغرض ويجب تطبيق نطاقات التنفيذ الخاصة بـ Kernels بعد مراجعة مشغل شبكة الدفع المحلية.

2.2.1 متطلبات الجودة

يجب أن يكون هناك التزام بمتطلبات الجودة الرئيسية، كما هو موضح في الجدول التالي.
(انظر الملحق رقم 14)

3.1 مواصفات لوحة التوقيع

يصف هذا الجزء معلومات بطاقة نمو ويحدد متطلبات لوحة التوقيع على البطاقة. يتم إنشاء لوحة التوقيع لتوقيع مالك البطاقة.

1.3.1 الخصائص الرئيسية

الخصائص الرئيسية للوحات التوقيع هي:

- أبيض وواضح
- رقائق لوحة التوقيع الواضحة والأمنة التي تلمي أعلى المعايير
- تطلبها صناعة البطاقات المصرفية. سيتم قبول طباعته على ظهره
- جانب البطاقة مع تصميم البطاقة كلوحة توقيع شفافة
- مصمم لقبول جميع أنواع توقيعات الحبر
- طلبًا لإمكانية قراءة توقيع حامل البطاقة ، يجب على جهة الإصدار التأكد من أن ألوان لوحة توقيع نمو توفر تباينًا كافيًا مع الحبر الأسود والأزرق.

2.3.1 أبعاد لوحة التوقيع

حجم لوحة التوقيع هو مسؤولية جهة الإصدار، و لكن يوصى بأن لا يقل عرضه عن 26.0 ملم وارتفاعه 7.0 ملم. قد تتضمن لوحة التوقيع نمو علامة التبويب الموسعة كجزء منها لطباعة قيمة CVV2.
(انظر الملحق رقم 15)

1.3.3 Signature Panel Location on the Card

The signature tape must be located on the back side of the card.

The issuer is responsible for identifying the exact location of the signature panel on the back side of the card, but it must not be placed over the chip safety area.

(See appendix number 16)

1.3.4 Card Verification Value CVV2

- It is a must that the three digits of the card validation number are located immediately right to the signature panel.
- If the card verification number is printed in the extended tab of the signature panel,
- The width of the extended tab must be at least 8.5 mm and the height must be at least 7.0 mm.
- If the card verification number is printed directly on the card, the extended tab must be removed and the area of printing must be at least 8.0 mm wide and 5.75 mm high.
- It is recommended that this area is separated from other texts with a thin line.
- CVV2 must be printed using a specialized indent-printing module that prints numbers 0 through 9 in reverse italics slanted to the left and at 14 characters per inch.

(See appendix number 17)

1.3.5 Main Characteristics

There are many features which have the signature panels as follows:

- Ease of release and sharp edge definition
- No cold flake shedding before or during application
- Solvents used to erase signature will also dissolve the signature panel.

1.4 Magnetic-Stripe Specifications

This part describes the characteristics of magnetic stripe specifications for NUMO branded card and requirements for a high coercivity magnetic stripe (including any protective overlay) on the card, the encoding technique and coded character sets.

1.4.1 Magstripe Requirements

It is a must that the magnetic stripe is a 2 track /3 track high coercivity tape following the standards of International Organizations for Standardization (ISO) /International Electrotechnical Commission (IEC) 7811-6- Identification cards – Recording technique – Magnetic Stripe – High coercivity.

The issuer is responsible for identifying the color of the magnetic stripe and any graphics that may appear on the magnetic stripe.

1.4.2 Distortion on Magstripe surface

There will be no surface distortions, irregularities or raised areas on both the front and the back of the card in the area shown in Figure 1 that might interfere with the contact between the chip and magnetic stripe.

(See appendix number 18)

3.3.1 موقع لوحة التوقيع على البطاقة

يجب وضع شريط التوقيع على الجانب الخلفي للبطاقة.

جهة الإصدار هي المسؤولة عن تحديد الموقع الدقيق للوحة التوقيع على الجانب الخلفي من البطاقة،

ولكن لا يجب وضعها فوق منطقة أمان الشريحة.

(انظر الملحق رقم 16)

4.3.1 قيمة التحقق من البطاقة CVV2

- يجب أن تكون الأرقام الثلاثة لرقم التحقق من صحة البطاقة موجودة مباشرة على لوحة التوقيع.
 - إذا تمت طباعة رقم التحقق من البطاقة في علامة التبويب الموسعة بلوحة التوقيع،
 - يجب ألا يقل عرض علامة التبويب الموسعة عن 8.5 ملم وأن لا يقل الارتفاع عن 7.0 ملم.
 - إذا تمت طباعة رقم التحقق من البطاقة مباشرة على البطاقة، فيجب إزالة علامة التبويب الموسعة ويجب أن تكون منطقة الطباعة بعرض 8.0 ملم على الأقل وارتفاع 5.75 ملم.
 - يوصى بفصل هذه المنطقة عن النصوص الأخرى بخط رفيع.
 - يجب طباعة CVV2 باستخدام وحدة طباعة بادئة متخصصة تطبع الأرقام من 0 إلى 9 بخط عكسي مائل إلى اليسار وبكثافة 14 حرفًا للبوصة.
- (انظر الملحق رقم 17)

5.3.1 الخصائص الرئيسية

هناك العديد من الميزات التي تحتوي على لوحات التوقيع على النحو التالي:

- سهولة التحرير وتحديد الحافة الحادة
- لا تتساقط القشور الباردة قبل أو أثناء التطبيق
- المذيبات المستخدمة في محو التوقيع سوف تذيب لوحة التوقيع أيضًا.

4.1 مواصفات الشريط المغناطيسي

يصف هذا الجزء خصائص مواصفات الشريط المغناطيسي للبطاقة التي تحمل علامة نمو التجارية ومتطلبات شريط مغناطيسي عالي الإكراه (بما في ذلك أي غطاء واقٍ) على البطاقة، وتقنية التشفير ومجموعات الأحرف المشفرة.

1.4.1 متطلبات الشريط المغناطيسي

من الضروري أن يكون الشريط المغناطيسي عبارة عن شريط ذي مسارين / 3 مسارات عالية الإكراه وفقًا لمعايير المنظمات الدولية للتوحيد القياسي (ISO) / اللجنة الكهروتقنية الدولية (-6-7811 IEC) بطاقات التعريف - تقنية التسجيل - شريط مغناطيسي - مرتفع القوة القهرية. جهة الإصدار مسؤولة عن تحديد لون الشريط المغناطيسي وأي رسومات قد تظهر على الشريط المغناطيسي.

2.4.1 التشويه على سطح الشريط المغناطيسي

لن يكون هناك تشوهات في السطح أو مخالفات أو مناطق مرتفعة على كل من الجزء الأمامي والخلفي للبطاقة في المنطقة الموضحة في الشكل 1 والتي قد تتداخل مع الإتصال بين الشريحة والشريط المغناطيسي (انظر الملحق رقم 18)

1.4.3 Positioning the Magstripe

The magnetic stripe area is located on the back of the card.
(See appendix number 19)

1.5 Card data specifications and characteristics

This part specifies the requirements for the card number, characters, and personal data on NUMO cards. Card number characters are intended to transmit data either by the use of print, visual, or machine-reading tools.

The purpose of this series is to provide card performance without regard to usage, if any, to the extent that the card has been tested upon printing prior to the testing phase by the National Scheme Operator.

1.5.1 Personalization Techniques

This section clarifies the specifications of both Embossed and Unembossed personalization techniques.

1.5.1.1 Personalization Techniques for Embossed Cards

The embossed data should only be on the front of the card. All printed data as the logo or anything graphic that is not part of the background of the card must be at least 4.0 mm from the logo. Only the last four digits of the PAN must be at least 2.0 mm away from the logo.

(See appendix number 20)

1.5.1.2 Personalization Techniques for Unembossed Cards

Below are recommended Unembossed methods:

- The durability of Unembossed objects must be assured through sufficient depth of indent printing. Laser printing should be through the laminate.
- The Unembossed account information must be away from the card edge with at least 3.0mm and from the brand mark with at least 2.0 mm
- The issuer has the right to identify the size of the PAN, but the height must be 3.0 mm at least.

1.5.2 Bank Logo and Brand Name

The Bank logo/Name must be marked on the front of the card as mentioned before and away from all elements that are not part of the back of the card except for the last four digits of the Primary Card Number (PAN) which are not less than 4.0 mm.

1.5.3 Cardholder Name

It is a must that the cardholder name is located on the front side of the card. If the cardholder name is embossed, it must be located on line 2, and /or line 3 and/or line 4 and must be set from the brand mark with 2.0 mm at least.

(See appendix number 21)

3.4.1 وضع الشريط المغناطيسي

تقع منطقة الشريط المغناطيسي على ظهر البطاقة.
(انظر الملحق رقم 19)

5.1 مواصفات وخصائص بيانات البطاقة

يحدد هذا الجزء متطلبات رقم البطاقة والأحرف والبيانات الشخصية على بطاقات نمو. تهدف أحرف رقم البطاقة إلى نقل البيانات إما عن طريق استخدام أدوات الطباعة أو المرئية أو أدوات القراءة الآلية.

الغرض من هذه السلسلة هو توفير أداء البطاقة بغض النظر عن الاستخدام، إن وجد، إلى الحد الذي تم فيه اختبار البطاقة عند الطباعة قبل مرحلة الاختبار بواسطة مشغل شبكة الدفع المحلية

1.5.1 تقنيات التخصيص

يوضح هذا القسم مواصفات كل من تقنيات التخصيص المنقوشة وغير المنقوشة.

1.1.5.1 تقنيات التخصيص للبطاقات المنقوشة

يجب أن تكون البيانات المنقوشة في مقدمة البطاقة فقط. و جميع البيانات المطبوعة كشعار أو أي رسم ليس جزءًا من خلفية البطاقة يجب أن تكون على الأقل 4.0 ملم من الشعار. الأرقام الأربعة الأخيرة فقط من رقم الحساب الأساسي يجب أن تكون على بعد 2.0 ملم على الأقل من الشعار.
(الملحق رقم 20)

2.1.5.1 تقنيات التخصيص للبطاقات غير المنقوشة

فيما يلي الأساليب غير المنقوشة الموصى بها:

- يجب ضمان متانة العناصر غير المنقوشة من خلال عمق كافٍ للطباعة البادئة. يجب أن تكون الطباعة بالليزر من خلال الصفائح.
- يجب أن تكون معلومات الحساب غير المنقوش بعيدة عن حافة البطاقة بمقدار 3.0 ملم على الأقل وعن العلامة التجارية بـ 2.0 مم على الأقل.
- يحق لجهة الإصدار تحديد حجم رقم الحساب الأساسي ، ولكن يجب ألا يقل الارتفاع عن 3.0 ملم.

2.5.1 شعار المصرف واسم العلامة التجارية

يجب وضع علامة على شعار/ اسم المصرف في مقدمة البطاقة كما هو مذكور سابقًا وبعيدًا عن جميع العناصر التي ليست جزءًا من ظهر البطاقة باستثناء الأرقام الأربعة الأخيرة من رقم البطاقة الأساسية (رقم الحساب الأساسي) والتي لا تقل عن 4.0 ملم.

3.5.1 اسم حامل البطاقة

يجب أن يكون اسم حامل البطاقة موجودًا على الجانب الأمامي من البطاقة. إذا كان اسم حامل البطاقة منقوشًا، فيجب أن يكون موجودًا في السطر 2 و/ أو السطر 3 و/ أو السطر 4 ويجب تعيينه من علامة العلامة التجارية بـ 2.0 مم على الأقل.
(انظر الملحق رقم 21)

1.5.4 Presentation of Numbers

(See appendix number 22)

1.5.5 Customer Service Contacts

It is a must that the customer service number is located on the backside of the card, printed under the laminate or using an Unembossed method as well as being clearly legible. The issuer has the right to identify the font, color, size, and location of the customer service number on the back side of the card.

1.5.6 Card Validity

The card's validity date must be printed and shown, specified in a month and year, provided that it is shown on the front of the card after the phrase "Valid Thru" and must be printed prominently or unobtrusively according to the method of printing the name and the card account number.

1.5.7 Issuer Bank Name

It is a must that the issuer name and/or logo are placed on the front side of the card and positioned from NUMO Brand Mark with 4.0 mm at least.

1.5.8 PAN Presentment on Card

The PAN must be printed on the front of the card and, according to ISO/IEC rules, position 1 on line 1. It should be divided into four groups of four digits with one space between each group for a total of 19 positions including spaces.

In the case of using 19-digit card numbers, the above is implemented with the last three single digits placed to the right.

(See appendix number 23)

1.5.9 Contactless Cards

EMVCO developed Contactless indicator to create a worldwide symbol of contactless symbol.

The contactless indicator is formed of four customized semicircles from the smallest to the largest in size. The contactless indicator should be located at the front side of the card on the chip line. The contactless indicator must always appear exactly as shown in the below image and never angled or oriented in any other fashion.

(See appendix number 24)

1.5.9.1 Main Characteristics

The main characteristics of contactless indicator are:

- Appear on a solid colour that contrasts with the colour of the back ground.
- Optimal colours for the contactless indicator include black, white, grey or other neutral colours.
- Be printed under the laminate or printed using an indent method
- Be with height at least 7.0mm
- Be away from any other element on the card with a space of at least 2.0mm

4.5.1 عرض الأرقام

(انظر الملحق رقم 22)

5.5.1 جهات اتصال خدمة العملاء

من الضروري أن يكون رقم خدمة العملاء موجودًا على الجانب الخلفي من البطاقة، ومطبوع أسفل الصفائح أو باستخدام أسلوب الغير منقوش بالإضافة إلى أن يكون مقروءًا بوضوح. لجهة الإصدار الحق في تحديد الخط واللون والحجم والموقع لرقم خدمة العملاء على الجانب الخلفي من البطاقة.

6.5.1 صلاحية البطاقة

يجب طباعة تاريخ صلاحية البطاقة وإظهاره، محددًا بالشهر والسنة، بشرط أن يظهر في مقدمة البطاقة بعد عبارة "صالحة من" ويجب طباعته بشكل بارز أو غير مخفي حسب طريقة طباعة الاسم ورقم حساب البطاقة.

7.5.1 اسم مصرف جهة الإصدار

من الضروري وضع اسم جهة الإصدار و/ أو الشعار على الجانب الأمامي للبطاقة ووضعهما من علامة العلامة التجارية نمو بـ 4.0 ملم على الأقل.

8.5.1 عرض رقم الحساب الأساسي على البطاقة

يجب طباعة رقم الحساب الأساسي على مقدمة البطاقة، ووفقًا لقواعد ISO / IEC ، الموضع 1 في السطر 1. يجب تقسيمها إلى أربع مجموعات من أربعة أرقام مع مسافة واحدة بين كل مجموعة ليصبح المجموع 19 موضعًا بما في ذلك المسافات.

في حالة استخدام أرقام البطاقات المكونة من 19 رقمًا، يتم تنفيذ ما سبق مع وضع آخر ثلاثة أرقام مفردة على اليمين.

(انظر الملحق رقم 23)

9.5.1 البطاقات غير المتصلة

طورت EMVCO المؤشر الغير تلامسي لإنشاء رمز عالمي للرمز الغير تلامسي.

يتكون المؤشر غير المتصل من أربعة دوائر نصف دائرة مخصصة من الأصغر إلى الأكبر حجمًا. يجب وضع المؤشر غير المتصل في الجانب الأمامي للبطاقة على خط الشريحة. يجب أن يظهر المؤشر غير المتصل دائمًا تمامًا كما هو موضح في الصورة أدناه وألا يكون مائلًا أو موجهًا بأي شكل آخر. (انظر الملحق رقم 24)

1.9.5.1 الخصائص الرئيسية

الخصائص الرئيسية للمؤشر غير المتصل هي:

- تظهر بلون خالص يتناقض مع لون الخلفية.
- الألوان المثالية لمؤشر غير المتصل تشمل الأسود، الأبيض، الرمادي أو الألوان المحايدة الأخرى.
- يمكن طباعتها تحت الصفائح أو طباعتها باستخدام طريقة المسافة البادئة
- تكون بارتفاع لا يقل عن 7.0 ملم
- تكون بعيدة عن أي عنصر آخر على البطاقة بمساحة لا تقل عن 2.0 ملم

- It is expected that the contactless indicator will appear at a size equal to the other brand imagery displayed.
 - The minimum clear space around all four sides of the indicator must be equal to the full height of the second semicircle from the left.
 - When the contactless indicator is embossed or debossed on a contactless Card, the ripples must provide sufficient contrast against the selected background to maintain good visibility of the mark.
 - The Contactless Indicator may be applied as a supplemental Indicator on a standard-sized payment card where there is an existing Indicator that meets the full size and clear space requirements present on the card. Where being applied as a supplemental Indicator, the Contactless Indicator must appear at a height no smaller than 4.5mm, with a minimum clear space around all four sides of the indicator of 1.7mm, and placement must be on the opposite side to the existing Indicator.
- (See appendix number 25)

1.5.9.2 Restrictions

The contactless indicator must never be broken apart or visually altered in anyway. There are some examples of unaccepted usage are as follows:
(See appendix number 26)

1.6 Applying Invisible Ink and Hologram

1.6.1 Possibility of Using the Invisible Ink

Invisible Ink Can be used subject to obtaining an approval through the National Scheme Operator

1.6.2 Securing and Printing NUMO logo with invisible INK

It is from the characteristics of the invisible ink that it appears only when an ultraviolet light is shed to appear to the explorer, provided that it is below the previously approved NUMO logo and appears in a monochromatic degree inclined to light blue, considering that it appears at an angle of inclination of 30 degrees and bears the same NUMO logo
(See appendix number 27)

1.6.3 Characteristics of The Invisible Ink

- It is invisible in daylight.
- It appears under UV Lamp (Under 400 nm.).
- It must be the blue colour as a UV Fluorescent Inks.
- Using the UV Offset inks is a must.
- The inks are suitable for printing onto synthetic materials.
- It must be guaranteed that the expiry date of the invisible ink is not less than six months on the date of card manufacture.

It must be ensured that the expiry date of the invisible ink is at least six months from the date of manufacture of the card.

1.6.4 Usage of Hologram for NUMO Cards

The proposed design must be reviewed by the National Scheme Operator to indicate the extent of compliance with the requirements of printing as well as the extent to which it conforms to the rules and standards of the cards set.

- من المتوقع أن يظهر المؤشر غير المتصل بحجم مساوٍ لصور العلامة التجارية الأخرى المعروضة.
- يجب أن يكون الحد الأدنى للمسافة الواضحة حول الجوانب الأربعة للمؤشر مساويًا للارتفاع الكامل لنصف الدائرة الثاني من اليسار.
- عندما يكون المؤشر غير المتصل منقوشًا أو غير منقوشًا على البطاقة غير المتصلة ، يجب أن توفر التموجات تباينًا كافيًا مع الخلفية المحددة للحفاظ على الرؤية الجيدة للعلامة.
- يمكن تطبيق المؤشر غير المتصل كمؤشر تكميلي على بطاقة الدفع ذات الحجم القياسي حيث يوجد مؤشر حالي يلبي الحجم الكامل والمساحة الخالية.
- المتطلبات الموجودة على البطاقة. عند تطبيقه كمؤشر تكميلي ، يجب أن يظهر المؤشر غير المتصل على ارتفاع لا يقل عن 4.5 ملم ، مع مساحة خالية من جميع الجوانب الأربعة للمؤشر تبلغ 1.7 ملم ، ويجب أن يكون الموضع على الجانب المقابل للمؤشر الحالي .
(انظر الملحق رقم 25)

2.9.5.1 القيود

يجب عدم كسر المؤشر غير المتصل أو تغييره بصريًا على أي حال.
فيما يلي بعض الأمثلة على الاستخدام غير المقبول:
(انظر الملحق رقم 26)

6.1 تطبيق الحبر غير المرئي والهولوغرام

1.6.1 إمكانية استخدام الحبر غير المرئي

يمكن استخدام الحبر غير المرئي بشرط الحصول على موافقة من مشغل شبكة الدفع المحلية.

2.6.1 تأمين وطباعة شعار نمو بحبر غير مرئي

من خصائص الحبر غير المرئي أنه يظهر فقط عند تسليط ضوء فوق بنفسجي ليظهر للمستكشف، بشرط أن يكون أسفل شعار نمو المعتمد مسبقًا ويظهر بدرجة أحادية اللون تميل إلى اللون الأزرق الفاتح ، مع الأخذ في الاعتبار أنه يظهر بزاوية ميل 30 درجة وتحمل نفس شعار نمو
(انظر الملحق رقم 27)

3.6.1 خصائص الحبر غير المرئي

- غير مرئي في وضح النهار.
- يظهر تحت مصباح الأشعة فوق البنفسجية (أقل من 400 نانومتر).
- يجب أن يكون باللون الأزرق كأخبار فلورية للأشعة فوق البنفسجية.
- استخدام أحبار تعويض للأشعة فوق البنفسجية أمر لا بد منه.
- الأحبار مناسبة للطباعة على المواد الاصطناعية.
- يجب التأكد من أن تاريخ انتهاء صلاحية الحبر غير المرئي لا يقل عن ستة أشهر من تاريخ صنع البطاقة.

4.6.1 استخدام الهولوغرام لبطاقات نمو

يجب أن يقوم مشغل شبكة الدفع المحلية بمراجعة التصميم المقترح من قبل للإشارة إلى مدى الامتثال لمتطلبات الطباعة بالإضافة إلى مدى مطابقته لقواعد ومعايير البطاقات المحددة.

1.7 Issuer Bank Responsibilities

The Issuer Bank is responsible for all changes applied to the issued card in addition to the following:

Obtaining the approvals to add any image as background for the card even if the background image belongs to a third-party supplier that the bank authorized to review and approve of the background image.

No card provider has the right to print any background image on a growth card unless this third party is approved by the National Scheme Operator.

To ensure that product identifiers such as debit cards and silver, gold or platinum cards are printed during card allocation and according to the card specifications mentioned in the issuer's terms Chapter.

- To ensure that there is a protective cover for each card image printed using the digital or thermal printing process as a kind of protection on the printed image.
- The National Scheme Operator has the right to request samples of the card for review as well as to contact the card manufacturer directly to request card samples.
- Cards sent to the National Scheme Operator – for the purpose of design review – must be clearly invalidated by scratching the magnetic strip to such an extent that the magnetic stripe is illegible and blank for printing in the signature panel and ensuring that the chip is not activated or turned on in the case of smart cards.

Regulatory Rules of The Libyan National Payment Scheme

Chapter 2 – Chargeback Rules

2.1 Dispute Resolution Process Overview

Process initiation is started by the Cardholder through a standard form filled by the cardholder stating the type of chargeback either through ATM or POS and the reason for such request, this form is found in Annex (A).

National Scheme Operator administers procedures set forth later in this Chapter that enable a Member to seek redress against another Member for failure to comply with the Standards applicable to a Transaction. Any filing by or on behalf of a Member related to an arbitration procedure (including any chargeback or re-presentment cycle) or pre-compliance or compliance procedure must be made in good faith and only after careful review of both the Standards and available information pertinent to the dispute.

After the presentment of a Transaction from the Acquirer to the Issuer, the Issuer may determine that, for a reason specified later in this Chapter, the Transaction may be disputed. The Issuer may then return the Transaction to the Acquirer as a chargeback for possible remedy.

7.1 مسؤوليات المصرف المصدر

يتحمل مصرف جهة الإصدار المسؤولية عن جميع التغييرات المطبقة على البطاقة الصادرة بالإضافة إلى ما يلي:

الحصول على الموافقات لإضافة أي صورة كخلفية للبطاقة حتى إذا كانت صورة الخلفية تخص موردًا خارجيًا مصرح له من قبل المصرف بمراجعة صورة الخلفية والموافقة عليها.

لا يحق لأي مقدم بطاقة طباعة أي صورة خلفية على بطاقة النمو ما لم يتم اعتماد هذا الطرف الثالث من قبل مشغل شبكة الدفع المحلية.

للتأكد من طباعة معرفات المنتجات مثل بطاقات الخصم والبطاقات الفضية والذهبية أو البلاتينية أثناء تخصيص البطاقة ووفقًا لمواصفات البطاقة المذكورة في فصل شروط جهة الإصدار.

- التأكد من وجود غطاء واقٍ لكل صورة بطاقة مطبوعة باستخدام عملية الطباعة الرقمية أو الحرارية كنوع من الحماية على الصورة المطبوعة.
- يحق لمشغل شبكة الدفع المحلية طلب عينات من البطاقة للمراجعة بالإضافة إلى الاتصال بجهة تصنيع البطاقة مباشرة لطلب عينات من البطاقة
- يجب إبطال البطاقات المرسلة إلى مشغل شبكة الدفع المحلية - لغرض مراجعة التصميم - بشكل واضح عن طريق خدش الشريط المغناطيسي إلى الحد الذي يجعل الشريط المغناطيسي غير مقروء وفارغ للطباعة في لوحة التوقيع والتأكد من أن الشريحة ليست فعالة أو مشغلة في حالة البطاقات الذكية.

القواعد التنظيمية لشبكة الدفع المحلية الليبية

الفصل 2 – قواعد رد المبالغ المدفوعة

1.2. نظرة عامة حول عملية حل النزاعات

تبدأ العملية من قبل حامل البطاقة من خلال نموذج قياسي يملأه حامل البطاقة يوضح نوع رد المبالغ المدفوعة إما من خلال أجهزة الصراف الآلي أو نقاط البيع والسبب لهذا الطلب، ويمكن العثور على هذا النموذج في الملحق (أ).

يدير مشغل شبكة الدفع المحلية الإجراءات المنصوص عليها لاحقًا في هذا الفصل والتي تمكن العضو من طلب التعويض ضد عضو آخر بسبب عدم امتثاله للمعايير المطبقة على المعاملة. يجب أن يتم أي تقديم من قبل عضو أو نيابة عنه فيما يتعلق بإجراءات التحكيم (بما في ذلك أي دورة لرد المبالغ المدفوعة أو إعادة التقديم) أو الامتثال المسبق أو إجراء الامتثال بحسن نية وفقط بعد مراجعة دقيقة لكل من المعايير والمعلومات المتاحة ذات الصلة للنزاع.

بعد تقديم المعاملة من الجهة القابلة إلى جهة الإصدار، يجوز لجهة الإصدار أن تقرر، لسبب محدد لاحقًا في هذا الفصل، أن المعاملة قد تكون محل نزاع. يجوز لجهة الإصدار عندئذٍ إعادة المعاملة إلى القابل على أنها رد المبالغ المدفوعة للحصول على تعويض محتمل.

In response to the chargeback, the Acquirer may (a) accept responsibility for the disputed Transaction, (b) obtain information from the Merchant that can remedy the dispute, or (c) determine the chargeback was improper. The Acquirer may return the chargeback to the Issuer as a chargeback rejection.

The Issuer reviews the Acquirer's chargeback rejection and if the Issuer chooses to continue the dispute, the Issuer would continue the dispute based on the chargeback reason code as a pre-arbitration case (which may later be escalated to an arbitration case). When an arbitration case is escalated and the dispute is unresolved, National Scheme Operator will decide responsibility for the dispute in an arbitration case filing. Before an arbitration case is filed, all steps of the chargeback process must have been completed.

When a Member does not perform a required action, that Member is accepting liability for the disputed Transaction. For example, an Acquirer that does not generate a chargeback rejection is liable for the disputed Transaction.

2.1.1Reason Codes

Following is a list of the codes used in the National Scheme Operator portal.

2.1.1.1Chargeback Creation Reason Codes

Following is a list of the codes used to identify the reason for creating a chargeback.

- CBCD01 Expired Card
- CBCD03 Recurring Transaction dispute
- CBCD04 Credit posted as a purchase
- CBCD06 Requested goods or services not received
- CBCD07 Requested goods or services not as described/defected
- CBCD08 Subsequent Transaction disputed
- CBCD09 Credit not received
- CBCD11 No Show/Deposit not refunded
- CBCD12 Incomplete Transaction was processed
- CBCD13 Not authorized by Member
- CBCD14 Duplicate amount
- CBCD15 Paid by other way
- CBCD16 Transaction amount is different
- CBCD17 Late process of Transaction
- CBCD21 Chip processing rules
- CBCD22 No Authorization/Declined Authorization
- CBCD23 Card number not issued
- CBCD24 Multiple fraudulent Transactions
- CBCD27 Deposit did not affect Card (ATM Deposit)
- CBCD28 Deposit did not affect Card (POS Deposit)
- CBCD29 ICT did not affect Card

ردًا على رد المبالغ المدفوعة، يجوز للقابل (أ) قبول المسؤولية عن المعاملة المتنازع عليها، أو (ب) الحصول على معلومات من التاجر يمكنها معالجة النزاع، أو (ج) تحديد أن رد المبالغ المدفوعة كان غير مناسب. قد يقوم القابل بإعادة المبالغ المدفوعة إلى جهة الإصدار كرفض لرد المبالغ المدفوعة.

تراجع جهة الإصدار رفض القابل لرد المبالغ المدفوعة وإذا اختارت جهة الإصدار مواصلة النزاع، فستواصل جهة الإصدار النزاع بناءً على رمز سبب رد المبالغ المدفوعة كدعوى ما قبل التحكيم (والتي قد يتم تصعيدها لاحقًا إلى دعوى تحكيم). عندما يتم تصعيد دعوى التحكيم ولم يتم حل النزاع، سيقرر مشغل شبكة الدفع المحلية المسؤولية عن النزاع في تقديم دعوى التحكيم. قبل رفع دعوى التحكيم، يجب إكمال جميع خطوات عملية رد المبالغ المدفوعة.

عندما لا يقوم العضو بتنفيذ الإجراء المطلوب، فإن هذا العضو يقبل المسؤولية عن المعاملة المتنازع عليها. على سبيل المثال، يكون القابل الذي لا ينشئ رفضًا لرد المبالغ المدفوعة مسؤولًا عن المعاملة المتنازع عليها.

1.1.2. رموز السبب

فيما يلي قائمة بالرموز المستخدمة في بوابة مشغل شبكة الدفع المحلية.

1.1.1.2. رموز سبب إنشاء رد المبالغ المدفوعة

فيما يلي قائمة بالرموز المستخدمة لتحديد سبب إنشاء رد المبالغ المدفوعة.

- CBCD01 بطاقة منتهية الصلاحية
- CBCD03 نزاع المعاملات المكررة
- CBCD04 نشر الإئتمان على أنه عملية شراء
- CBCD06 عدم استلام السلع أو الخدمات المطلوبة
- CBCD07 السلع أو الخدمات المطلوبة غير مطابقة للوصف / معيبة
- CBCD08 المعاملات اللاحقة متنازع عليها
- CBCD09 عدم استلام الإئتمان
- CBCD11 عدم الظهور / عدم رد الإيداع
- CBCD12 تمت معالجة المعاملة غير المكتملة
- CBCD13 غير مصرح به من قبل العضو
- CBCD14 مبلغ مكرر
- CBCD15 مدفوعة بطريقة أخرى
- CBCD16 مبلغ المعاملة مختلف
- CBCD17 عملية متأخرة للمعاملة
- CBCD21 قواعد معالجة الشريحة
- CBCD22 لا يوجد تفويض / تفويض مرفوض
- CBCD23 عدم إصدار رقم بطاقة
- CBCD24 معاملات احتيالية متعددة
- CBCD27 عدم تأثير الإيداع على البطاقة (إيداع جهاز الصراف الآلي)
- CBCD28 عدم تأثير الإيداع على البطاقة (إيداع نقاط البيع)
- CBCD29 عدم تأثير ICT على البطاقة

2.1.1.2 Additional Codes to Pre-Arbitration Creation

Following is a list of additional codes that may be used to identify the reason for a pre-arbitration.

- CBCD25 Required rejection documents were illegible/unrelated/incomplete
- CBCD26 Required rejection documents were not received

2.1.1.3 Chargeback Rejection Codes

Following is a list of the codes used to identify the reason for rejecting a chargeback.

- RSN01 Attached Documents and remedy
- RSN02 Credit already processed
- RSN03 Chargeback is invalid
- RSN04 Chargeback documents were illegible/unrelated/incomplete
- RSN05 Chargeback documents were not received
- RSN06 Previous authorization obtained
- RSN07 Duplicate chargeback
- RSN08 Chargeback out of time frame

2.1.2 Time Frames

The term “Time Frames” is used throughout this Chapter. Time frame is the number of days in which an action must be performed.

Unless otherwise stated, all days are business days, consequently weekends and national holidays as identified by the Central Bank of Libya are excluded from time frame calculations.

The time frames for a dispute are as follows:

- An Issuer may submit a chargeback creation within the time frame specified in each chargeback creation section. The Transaction processing date is day zero.
- The Acquirer may reject the chargeback within 20 business days (10 business days for cash disputes) starting from the processing date of the chargeback. The processing date of the chargeback is day zero.
- The Issuer may submit a pre-arbitration within 20 business days (10 business days for cash disputes) starting from the processing date of the chargeback rejection. The processing date of the chargeback rejection is day zero.
- Acquirer may respond to pre-arbitration within 10 business days (5 business days for cash disputes) starting from the processing date of the pre-arbitration. The processing date of the pre-arbitration is day zero.
- If the Acquirer did not accept the pre-arbitration request within the above time frame, the Issuer may file the case for arbitration in the next 7 business days (5 business days for cash disputes) from the above time frame.
- National Scheme Operator will review the case and provide both Members with a ruling decision.

2.1.3 Required Documents

The term “Required Documents” is used throughout this Chapter. Required documents are written documents that must be provided by either the Cardholder or the Merchant in order to process the dispute and which provide information regarding the disputed Transaction.

2.1.1.2 رموز إضافية لإنشاء ما قبل التحكيم

فيما يلي قائمة بالرموز الإضافية التي يمكن استخدامها لتحديد سبب التحكيم المسبق.

- CBCD25 مستندات الرفض المطلوبة كانت غير مقروءة/ ذات غير صلة/ غير كاملة
- CBCD26 لم يتم استلام مستندات الرفض المطلوبة

3.1.1.2 رموز رفض رد المبالغ المدفوعة

فيما يلي قائمة بالرموز المستخدمة لتحديد سبب رفض رد المبالغ المدفوعة.

- RSN01 المستندات المرفقة وسبل المعالجة
- RSN02 تمت معالجة الإئتمان بالفعل
- RSN03 رد المبالغ المدفوعة غير صالح
- RSN04 إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة/ غير ذات صلة/ غير كاملة
- RSN05 لم يتم استلام مستندات رد المبالغ المدفوعة
- RSN06 - تم الحصول على التفويض المسبق
- RSN07 - تكرار رد المبالغ المدفوعة
- RSN08 رد المبالغ المدفوعة خارج الإطار الزمني

2.1.2 الأطر الزمنية

مصطلح “الأطر الزمنية” مستخدم في أنحاء هذا الفصل. الإطار الزمني هو عدد الأيام التي يجب فيها تنفيذ الإجراء.

ما لم يذكر خلاف ذلك، جميع الأيام هي أيام عمل، وبالتالي يتم استبعاد عطلات نهاية الأسبوع والأعياد الوطنية كما حددها مصرف ليبيا المركزي من حسابات الإطار الزمني.

الأطر الزمنية للنزاع هي كما يلي:

- يجوز لجهة الإصدار إرسال إنشاء رد المبالغ المدفوعة خلال الإطار الزمني المحدد في كل قسم من أقسام إنشاء رد المبالغ المدفوعة. تاريخ معالجة المعاملة هو اليوم صفر.
- يجوز للجهة القابلة رفض رد المبالغ المدفوعة في غضون 20 يوم عمل (10 أيام عمل للمنازعات النقدية) بدءًا من تاريخ معالجة رد المبالغ المدفوعة. تاريخ معالجة طلب رد المبالغ المدفوعة هو اليوم صفر.
- يجوز لجهة الإصدار تقديم التحكيم المسبق في غضون 20 يوم عمل (10 أيام عمل للمنازعات النقدية) بدءًا من تاريخ معالجة رفض رد المبالغ المدفوعة. تاريخ معالجة رفض رد المبالغ المدفوعة هو اليوم صفر.
- يجوز للقابل الرد على التحكيم المسبق في غضون 10 أيام عمل (5 أيام عمل للمنازعات النقدية) بدءًا من تاريخ معالجة التحكيم المسبق. تاريخ معالجة التحكيم المسبق هو اليوم صفر.
- إذا لم يقبل القابل طلب التحكيم المسبق خلال الإطار الزمني المذكور أعلاه، يجوز لجهة الإصدار رفع الدعوى للتحكيم في أيام العمل السبعة التالية (5 أيام عمل للمنازعات النقدية) من الإطار الزمني أعلاه.
- سيقوم مشغل شبكة الدفع المحلية بمراجعة الدعوى وتقديم قرار حكم لكل العضوين.

3.1.2 المستندات المطلوبة

يُستخدم مصطلح “المستندات المطلوبة” في أنحاء هذا الفصل. المستندات المطلوبة هي مستندات مكتوبة يجب أن يقدمها حامل البطاقة أو التاجر من أجل القيام بعملية المعالجة النزاع والتي توفر معلومات بشأن المعاملة المتنازع عليها.

Required documents must be in Arabic or English or both. Required documents must provide sufficient detail to enable all parties to understand the nature of the chargeback creation or rejection.

Required documents must be provided using the National Scheme Operator portal. Each Member is responsible for ensuring that legible copies of required documents have been entered into the portal.

Required documents to support a chargeback creation must come directly from the Cardholder or, in the case of a commercial Card, the corporate entity, and must be provided by email, letter, fax, and/or other message (including through the Issuer's password-protected website). Additionally, an Issuer's customer service representative may complete the applicable Dispute Form while on the telephone with a Cardholder or corporate entity representative. A Dispute Form may also accompany a Cardholder email, letter, fax/ and/or other message with additional detail provided by the Issuer.

Required documents to support a chargeback rejection must come directly from the Merchant and must be provided by the Merchant by email, letter, fax, and/or other message (including through the Acquirer's password-protected website). Acquirers should urge Merchants to provide all required documents in the rejection cycle to avoid extending disputes to further cycles.

Failure to submit required documents when required may cause that cycle to be invalid and may result in financial liability for the disputed Transaction.

A Member may submit documents even when the documents are not required; however, the documentation must be relevant to addressing or resolving the dispute.

2.1.4 Required Comment

The term "Required Comment" is used throughout this Chapter. A required comment is a phrase regarding the disputed Transaction which must be included in the National Scheme Operator portal.

5.1.2 Disputed Amount

The chargeback creation may dispute the total Transaction amount or a lesser amount. When a chargeback rejection, pre-arbitration, or arbitration is performed, the disputed amount must be for the same amount specified in the chargeback creation.

2.1.6 Settlement of dispute and exchange of funds

There is no financial impact to Members until the dispute is finalized. Funds will be moved according to each Members' liability to the disputed Transaction, and interchange fees will be settled as well.

7.1.2 Chargebacks for Reissued Cards

Upon reissuing a Card with the same primary account number (PAN) and a new expiration date, the Issuer must include the expiration date in all Transaction chargeback records.

يجب أن تكون المستندات المطلوبة باللغة العربية أو الإنجليزية أو كليهما. يجب أن توفر المستندات المطلوبة تفاصيل كافية لتمكين جميع الأطراف من فهم طبيعة إنشاء أو رفض رد المبالغ المدفوعة. يجب تقديم المستندات المطلوبة باستخدام بوابة مشغل شبكة الدفع المحلية. يتحمل كل عضو مسؤولية ضمان إدخال نسخ مقروءة من المستندات المطلوبة في البوابة.

يجب أن تأتي المستندات المطلوبة لدعم إنشاء رد المبالغ المدفوعة مباشرة من حامل البطاقة أو، في حالة البطاقة التجارية، من كيان الشركة، ويجب تقديمها عن طريق البريد الإلكتروني و /أو الخطاب و /أو الفاكس و /أو رسالة أخرى (بما في ذلك من خلال كلمة مرور جهة الإصدار- موقع محمي). بالإضافة إلى ذلك، يجوز لممثل خدمة العملاء لدى جهة الإصدار إكمال نموذج النزاع المعمول به أثناء الاتصال بالهاتف مع حامل البطاقة أو ممثل كيان الشركة. قد يرفق نموذج النزاع أيضًا بالبريد الإلكتروني لحامل البطاقة و /أو الخطاب و /أو الفاكس و /أو رسالة أخرى مع تفاصيل إضافية مقدمة من جهة الإصدار.

يجب أن تأتي المستندات المطلوبة لدعم رفض رد المبالغ المدفوعة مباشرة من التاجر ويجب أن يقدمها التاجر عن طريق البريد الإلكتروني و /أو الخطاب و /أو الفاكس و /أو رسالة أخرى (بما في ذلك من خلال موقع الويب المحمي بكلمة مرور الخاصة بالقابل). يجب على القابلين حث التاجر على تقديم جميع المستندات المطلوبة في دورة الرفض لتجنب توسيع النزاعات إلى دورات أخرى.

قد يؤدي عدم تقديم المستندات المطلوبة عند الطلب إلى عدم صلاحية هذه الدورة وقد يؤدي إلى تحمل المسؤولية المالية للمعاملة المتنازع عليها.

يجوز للعضو تقديم المستندات حتى عندما لا تكون المستندات مطلوبة؛ ومع ذلك، يجب أن تكون الوثائق ذات صلة بتحديد أو حل النزاع.

4.1.2 التعليق المطلوب

يُستخدم مصطلح "التعليق المطلوب" في أنحاء هذا الفصل. التعليق المطلوب هو عبارة تتعلق بالمعاملة المتنازع عليها والتي يجب تضمينها في بوابة مشغل شبكة الدفع المحلية.

5.1.2 المبلغ المتنازع عليه

قد يعترض إنشاء رد المبالغ المدفوعة على إجمالي مبلغ المعاملة أو مبلغ أقل. عند تنفيذ رفض رد المبالغ المدفوعة أو التحكيم المسبق أو التحكيم، يجب أن يكون المبلغ المتنازع عليه بنفس المبلغ المحدد في إنشاء رد المبالغ المدفوعة.

6.1.2 تسوية المنازعات وتبادل الأموال

لا يوجد أي تأثير مالي على الأعضاء حتى يتم إنهاء النزاع. سيتم نقل الأموال وفقًا لمسؤولية كل عضو تجاه المعاملة المتنازع عليها، وستتم تسوية رسوم التبادل أيضًا.

7.1.2 عمليات رد المبالغ المدفوعة للبطاقات المعاد إصدارها

عند إعادة إصدار بطاقة بنفس رقم الحساب الأساسي وتاريخ انتهاء صلاحية جديد، يجب على جهة الإصدار تضمين تاريخ انتهاء الصلاحية في جميع سجلات رد المبالغ المدفوعة الخاصة بالمعاملات.

2.2Chargeback Creation and Rejection

Disputes are grouped into four categories:

- Authorization Dispute Group
- Fraud Dispute Group
- Customer Claims Group
- Processing Error Group

The following sections provide detail information on terminology used through the chargeback creation and chargeback rejection process.

2.2.1 Authorization Dispute Group

An authorization-related chargeback may be submitted for one of the following reasons:

- The Card was expired
- An online authorization was not performed
- An online authorization was performed however the Transaction was declined
- The Card number is not valid

2.2.1.1 Expired Card

Reason Code. CBCD01-Expired Card Condition. An Issuer may use this reason code when all of the following conditions occurred:

- A Transaction occurred with an expired Card
- An online authorization was performed
- The Transaction was not approved by the Issuer

Time Frame. Within 60 calendar days of the Transaction processing date.

Required Documents. None

Required Comment. None

2.2.1.2 Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons. Refer to the corresponding subsections for complete details on each reason and its requirements.

- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN06-Previous authorization obtained
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN02-Credit previously issued

Condition. The Merchant processed a refund to the Card prior to receiving the chargeback.

Time Frame. Within 20 business days of the processing date of the chargeback

Required Documents. None

2.2. إنشاء رد المبالغ المدفوعة ورفضها

يتم تجميع النزاعات في أربع فئات:

- مجموعة نزاعات التفويض
- مجموعة منازعات الاحتيال
- مجموعة مطالبات العملاء
- مجموعة معالجة الأخطاء

توفر الأقسام التالية معلومات تفصيلية عن المصطلحات المستخدمة خلال إنشاء رد المبالغ المدفوعة وعملية رفض رد المبالغ المدفوعة.

1.2.2. مجموعة نزاعات التفويض

قد يتم إرسال رد المبالغ المدفوعة المرتبط بالتفويض لأحد الأسباب التالية:

- انتهت صلاحية البطاقة
- لم يتم إجراء التفويض عبر الإنترنت
- تم إجراء التفويض عبر الإنترنت ولكن تم رفض المعاملة
- رقم البطاقة غير صالح

1.1.2.2. بطاقة منتهية الصلاحية

رمز السبب. CBCD01 بطاقة منتهية الصلاحية.

شرط. يجوز لجهة الإصدار استخدام رمز السبب هذا عند حدوث جميع الشروط التالية:

- تم إجراء معاملة بطاقة منتهية الصلاحية.
- تم إجراء التفويض عبر الإنترنت.
- لم تتم الموافقة على المعاملة من قبل جهة الإصدار

إطار زمني. في غضون 60 يومًا تقويمياً من تاريخ معالجة المعاملة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

2.1.2.2. شروط رفض رد المبالغ المدفوعة

قد يرفض القابل رد المبالغ المدفوعة لأحد الأسباب التالية. راجع الأقسام الفرعية المقابلة للحصول

على تفاصيل كاملة عن كل سبب ومتطلباته.

- RSN02 - ائتمان تم إصداره مسبقًا.
- RSN03 - رد المبالغ المدفوعة غير صالح.
- RSN06 - تم الحصول على التفويض السابق.
- RSN07X - تكرار رد المبالغ المدفوعة.
- RSN08 رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا.

شرط. قام التاجر بمعالجة الإسترداد إلى البطاقة قبل استلام المبالغ المدفوعة.

إطار زمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

Required Comment. Both of the following:

- Date of the processed refund
- The Unique Clearing Reference Number of the refund.

Note. The Acquirer or Merchant must not process a refund after receiving a chargeback.

Reason Code. RSN03-Chargeback is invalid:

Condition. One the following:

- The Issuer did not meet the chargeback conditions
- Any of the chargeback data was invalid
- The Account PAN and Unique Clearing Reference Number fields in the chargeback creation record did not match any presentment record.

Time Frame. Within 20 business days of the processing date of the chargeback Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code. RSN06-Previous authorization obtained Condition. The Transaction was approved by the Issuer.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. All of the following:

- The Unique Reference Number (DE 57)
- Date of the original authorization
- Authorization number

Reason Code. RSN07-Duplicate Chargeback Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback. Required Documents. None

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame Condition. The chargeback was processed beyond the time frame specified for the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.1.3 No Authorization / Declined Authorization

The following subsections detail the conditions under which a chargeback may be created for one of the following reasons:

- Online authorization was not obtained for the Transaction.
- Online authorization was requested, and the Issuer declined the request.

التعليق المطلوب. كلا ما يلي:

- تاريخ معالجة الاسترداد
- الرقم المرجعي الفريد لمقاصة الاسترداد.

ملاحظة. يجب ألا يقوم القابل أو التاجر بمعالجة الاسترداد بعد استلام المبالغ المدفوعة.

رمز السبب. RSN03- رد المبالغ المدفوعة غير صالح:

شرط. واحد مما يلي:

- لم تف جهة الإصدار بشروط رد المبالغ المدفوعة.
- إذا كانت أي من بيانات رد المبالغ المدفوعة غير صالحة.
- عدم تطابق حقول رقم الحساب الأساسي والرقم المرجعي الفريد للمقاصة في سجل إنشاء رد المبالغ المدفوعة مع أي سجل عرض التقديم إطار زمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد.

التعليق المطلوب. الشرط الذي لم تستوفيه جهة الإصدار.

رمز السبب. RSN06- تم الحصول على التفويض المسبق شرط. تمت الموافقة على المعاملة من قبل جهة الإصدار.

إطار زمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد.

التعليق المطلوب. كل ما يلي:

- الرقم المرجعي الفريد (DE 57).
- تاريخ التفويض الأصلي.
- رقم التفويض.

رمز السبب. RSN07- تكرار رد المبالغ المدفوعة

شرط. تم التنازع على نفس المعاملة أكثر من مرة.

إطار زمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب . معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08- استعادة المبالغ المدفوعة خارج الإطار الزمني شرط. تمت معالجة عملية رد

المبالغ المدفوعة بعد الإطار الزمني المحدد لرمز سبب رد المبالغ المدفوعة.

إطار زمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

3.1.2.2 لا يوجد تفويض / تفويض مرفوض

توضح الأقسام الفرعية التالية الشروط التي يمكن بموجبها إنشاء رد المبالغ المدفوعة لأحد الأسباب التالية:

- لم يتم الحصول على التفويض عبر الإنترنت للمعاملة.
- تم طلب التفويض عبر الإنترنت، ورفضت جهة الإصدار الطلب.

- An online authorization was obtained but the cleared amount was greater than the approved amount

Reason Code. CBCD22

Chargeback Creation Condition. The Issuer may use this reason code when an online authorization was not performed for the Transaction.

Time Frame. Within 60 calendar days of the Transaction processing date.

Required Documents. None

Required Comment. No Authorization

Reason Code. CBCD22

Condition. The Issuer may use this reason code when an online authorization was obtained for the Transaction and the Issuer declined the request.

Time Frame. Within 60 calendar days of the Transaction processing date.

Required Documents. None

Required Comment. Declined Authorization

Reason Code. CBCD22

Condition. An Issuer may use this reason code when an online authorization was obtained but the cleared amount was greater than the approved amount.

Time Frame. Within 60 calendar days of the Transaction processing date.

Required Documents. None

Required Comment. Insufficient Authorization

Note. The Issuer may only charge back the difference between the approved and cleared amounts.

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN06-Previous authorization obtained
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy Chargeback Rejection Condition. One of the following Conditions:

Condition 1: Completion Transaction: The disputed Transaction was a completion Transaction corresponding to a pre-authorization

Condition 2: For Airline Tickets: The disputed Transaction was one of multiple clearing records corresponding to one approved authorization for the purchase of airline tickets and the total of the multiple clearing records did not exceed the approved amount.

Time Frame. Within 20 business days of the processing date of the chargeback.

- تم الحصول على تفويض عبر الإنترنت ولكن المبلغ الذي تمت تصفيته كان أكبر من المبلغ المعتمد.

رمز السبب. CBCD22

شرط إنشاء رد المبالغ المدفوعة. يجوز لجهة الإصدار استخدام رمز السبب هذا في حالة عدم إجراء تفويض عبر الإنترنت للمعاملة.

إطار زمني. في غضون 60 يومًا تقويمياً من تاريخ معالجة المعاملة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد تفويض.

رمز السبب. CBCD22

شرط. يجوز لجهة الإصدار استخدام رمز السبب هذا عند الحصول على تفويض عبر الإنترنت للمعاملة ورفضت جهة الإصدار الطلب.

إطار زمني. في غضون 60 يومًا تقويمياً من تاريخ معالجة المعاملة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. التفويض مرفوض.

رمز السبب. CBCD22

شرط. يجوز لجهة الإصدار استخدام رمز السبب هذا عند الحصول على تفويض عبر الإنترنت ولكن المبلغ الذي تمت تصفيته كان أكبر من المبلغ المعتمد.

إطار زمني. في غضون 60 يومًا تقويمياً من تاريخ معالجة المعاملة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. تفويض غير كافي

ملاحظة. يجوز لجهة الإصدار استرداد الفرق بين الموافقة والمبالغ المقاسة فقط.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقًا
- RSN03 - رد المبالغ المدفوعة غير صالح
- RSN06 - تم الحصول على التفويض السابق
- RSN07 - تكرار رد المبالغ المدفوعة
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شرط رفض رد المبالغ المدفوعة. أحد الشروط التالية:

الشرط 1: معاملة الإكتمال: كانت المعاملة المتنازع عليها عبارة عن معاملة إكتمال مقابلة لتفويض مسبق.

الشرط 2: بالنسبة لتذاكر الطيران: كانت المعاملة المتنازع عليها واحدة من سجلات المقاصة المتعددة المقابلة لتفويض واحد معتمد لشراء تذاكر الطيران ولم يتجاوز إجمالي سجلات المقاصة المتعددة المبلغ المعتمد.

إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.

Required Documents.

One of the following Conditions corresponding to the Chargeback Rejection Condition in this same subsection:

Condition 1: Completion Transactions: None

Condition 2: For Airline Tickets: Documents proving that the sum of the multiple clearing records did not exceed the approved authorization amount.

Required Comment. Unique Reference Number (DE 57) of the pre-authorization or authorization

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code. RSN06-Previous authorization obtained

Chargeback Rejection Condition. The Transaction was authorized by the Issuer.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The Unique Reference Number authorization number and date of the original authorization.

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Notes.

20% Tolerance. The 20% tolerance for gratuities does not apply to the following types of Transactions:

- Chip/PIN Transactions
- Contactless Transactions

المستندات المطلوبة. أحد الشروط التالية المقابلة لشرط رفض رد المبالغ المدفوعة في هذا القسم الفرعي نفسه:

الشرط : إتمام المعاملات: لا توجد

الشرط 2: بالنسبة لتذاكر الطيران: المستندات التي تثبت أن مجموع سجلات المقاصة المتعددة لا يتجاوز مبلغ التفويض المعتمد.

التعليق المطلوب. رقم مرجعي فريد (DE 57) للتفويض المسبق أو التفويض

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد الأموال إلى البطاقة

إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. تاريخ الاسترداد الذي تمت معالجته والرقم المرجعي الفريد لمقاصة للاسترداد

رمز السبب. -RSN03رد المبالغ المدفوعة غير صالح

شرط رفض رد المبالغ المدفوعة. لم تف جهة الإصدار بشروط رد المبالغ المدفوعة، أو أن أيًا من بيانات رد المبالغ المدفوعة كانت غير صالحة، أو أن حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. الشرط الذي لم تستوفه جهة الإصدار.

رمزالسبب. -RSN06تم الحصول على التفويض السابق

شرط رفض رد المبالغ المدفوعة. تمت الموافقة على المعاملة من قبل جهة الإصدار.

إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. رقم تفويض الرقم المرجعي الفريد وتاريخ التفويض الأصلي.

رمز السبب. -RSN07 تكرار رد المبالغ المدفوعة

شرط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. -RSN08رد المبالغ المدفوعة خارج الإطار الزمني

شرط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

ملاحظات. 20% تسامح. لا ينطبق التسامح البالغ 20% للإكراميات على الأنواع التالية من المعاملات:

- معاملات الشريحة/ رقم التعريف الشخصي
- المعاملات غير المتصلة

- Card-not-present Transactions

A 20% tolerance for gratuities will continue to apply to any other Transaction types.

2.2.1.4 Card Number Not Issued

The following subsection details the conditions under which a chargeback may be created to address an invalid card number.

Reason Code. CBCD23

Chargeback Creation Condition. An Issuer may use this reason code when the Issuer received a clearing record with a Card number that does not exist in the Issuer system. Time Frame. Within 60 calendar days of the Transaction processing date.

Required Documents. None

Required Comment. None

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN06-Previous authorization obtained
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code. RSN06-Previous authorization obtained

Chargeback Rejection Condition. The Transaction was authorized by the Issuer.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The Unique Reference Number (DE 57), Authorization number and Date of the original authorization.

- معاملات البطاقة غير الموجودة

سيستمر تطبيق التسامح بنسبة 20% للإكراميات على أي أنواع معاملات أخرى.

4.1.2.2 رقم البطاقة غير صادر

يوضح القسم الفرعي التالي بالتفصيل الشروط التي بموجبها يمكن إنشاء رد المبالغ المدفوعة لمعالجة رقم بطاقة غير صالح.

رمز الإِسبب. CBCD23

شرط إنشاء رد المبالغ المدفوعة. يجوز لجهة الإصدار استخدام رمز السبب هذا عندما تتلقى جهة الإصدار سجل مقاصة برقم بطاقة غير موجود في نظام جهة الإصدار.

إطار زمني. في غضون 60 يومًا تقويمياً من تاريخ معالجة المعاملة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. لا يوجد

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN02 - أئتمان تم إصداره مسبقًا
- RSN03 - رد المبالغ المدفوعة غير صالح
- RSN06 - تم الحصول على التفويض السابق
- RSN07 - تكرار رد المبالغ المدفوعة
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني

رمزالسبب. -RSN02 ائتمان تم إصداره مسبقًا

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

إطار زمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. تاريخ الاسترداد الذي تمت معالجته والرقم المرجعي للمقاصة الفريد للاسترداد

رمز السبب. -RSN03رد المبالغة المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. لم تف جهة الإصدار بشروط رد المبالغ المدفوعة، أو أن أيًا من بيانات رد المبالغ المدفوعة كانت غير صالحة ، أو أن حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. الشرط الذي لم تستوفه جهة الإصدار.

رمزالسبب. -RSN06تم الحصول على التفويض السابق

شرط رفض رد المبالغ المدفوعة. تمت الموافقة على المعاملة من قبل جهة الإصدار.

إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. الرقم المرجعي الفريد (DE 57) ورقم التفويض وتاريخ التفويض الأصلي.

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Creation Condition. The chargeback was processed out of the time frame of the chargeback reason code.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

2.2.2 Customer Claims Group

This section provides information in handling a Cardholder claim chargeback. Use of the Customer claim chargeback requires that the Cardholder engaged in the Transaction.
A Customer Claim chargeback may be submitted when the Cardholder contacted the Issuer alleging one of the following:

- Goods or services were either not as described or defective, including shipped merchandise was received damaged or not suitable for its intended purpose as well as the Merchant didn't honor the terms and conditions of a contract
- Goods or services were not provided
- Credit not processed
- Counterfeit goods alleged to be authentic were purchased
- Recurring Transaction canceled prior to billing
- Addendum dispute or "no-show" hotel charge was billed
- Purchase Transaction did not complete
- Credit posted as a purchase

A Customer Claim chargeback must not be submitted for an Instant Credit Transaction (ICT) Funding Transaction.

2.2.2.1 Goods or Services Were Either Not as Described or Defective

Reason Code. CBCD07

Chargeback Creation Condition. The Cardholder contacted the Issuer claiming all of the following occurred:

- The Cardholder engaged in the Transaction.
- The Cardholder contacted the Merchant, or attempted to contact the Merchant, to resolve the dispute.
- The Merchant refused to adjust the price, repair or replace the goods or other things of value, correct the service insufficiency, or issue a credit.
- For disputes involving goods: The Cardholder returned the goods or informed the Merchant the Cardholder was willing to return the goods.
- In order to process this chargeback, one of these three cases must have occurred in addition to the other bullets.

رمز السبب. -RSN07 تكرار رد المبالغ المدفوعة

شُروط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.
إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد
التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. -RSN08رد المبالغة المدفوعة خارج الإطار الزمني

شُروط إنشاء رد المبالغ المدفوعة. تمت معالجة عملية رد المبالغ المدفوعة خارج الإطار الزمني لرمز سبب رد المبالغ المدفوعة.
إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد
التعليق المطلوب. لا يوجد

2.2.2مجموعة مطالبات العملاء

يوفر هذا القسم معلومات في التعامل مع مطالبة حامل البطاقة برد المبالغ المدفوعة. يتطلب استخدام مطالبة العميل برد المبالغ المدفوعة أن يشارك حامل البطاقة في المعاملة.
يجوز تقديم مطالبة برد المبالغ المدفوعة للعميل عندما يتواصل حامل البطاقة بجهة الإصدار مدعيًا أحد الإجراءات التالية:

- كانت السلع أو الخدمات إما غير مطابقة للوصف أو معيبة، بما في ذلك البضائع المشحونة التي تم استلامها تالفة أو غير مناسبة للغرض المقصود منها وكذلك لم يحترم التاجر شروط وأحكام العقد
- لم يتم توفير السلع أو الخدمات
- لم تتم معالجة الائتمان
- تم شراء سلع مزورة يُزعم أنها أصلية
- تم إلغاء المعاملة المكررة قبل إعداد الفواتير
- تم احتساب نزاع الإضافة أو رسوم "عدم الحضور" الفندقية
- معاملة الشراء لم تكتمل
- نشر الائتمان كعملية شراء

يجب عدم تقديم مطالبة العميل برد المبالغ المدفوعة لمعاملة تمويل المعاملات الائتمانية الفورية (ICT).

1.2.2.2 السلع أو الخدمات إما غير مطابقة للوصف أو معيبة

رمز السبب. CBCD07

شُروط استرداد المبالغ المدفوعة. يجب على حامل البطاقة الاتصال بالجهة المصدرة في الحالات التالية:

- مشاركة حامل البطاقة في المعاملة.
- تواصل حامل البطاقة بالتاجر، أو محاول الاتصال بالتاجر لحل النزاع.
- رفض التاجر تعديل السعر، أو إصلاح أو استبدال البضائع أو الأشياء الأخرى ذات القيمة أو تصحيح عدم كفاية الخدمة أو إصدار ائتمان.
- بالنسبة للمنازعات المتعلقة بالبضائع: رد حامل البطاقة للبضائع، أو إعلام التاجر أنه على استعداد لرد البضائع.
- من أجل تسوية عملية رد المبالغ المدفوعة، يجب أن تكون إحدى هذه الحالات الثلاث قد وقعت، بالإضافة إلى الرموز النقطية الأخرى.

- When delivered from the Merchant, the goods arrived broken or could not be used for the intended purpose.
- Goods or services did not conform to their description. Examples include, but are not limited to:
 - The Cardholder claims that the quality or workmanship of the product is not as described.
 - The Cardholder claims that the specified color, size, or quantity is not as described.
 - The Merchant did not honor the terms and conditions of the contract with the Cardholder including, but not limited to, 100 percent money back guarantee, written promises, or return policy.

Time Frame. One of the following:

- Within 120 calendar days from when the services ceased with a maximum of 540 calendar days from the Transaction settlement date for issues of interruption of ongoing services.
- Within 120 calendar days from the delivery date of the goods or services.
- Within 120 calendar days from the Transaction processing date.

Required Documents. Cardholder email, letter, message, or completed Dispute Form-Cardholder Claims Group describing the Cardholder's complaint in sufficient detail to enable all parties to understand the dispute. This means that the Cardholder email, letter, or message must document how each point of the Chargeback Creation Conditions was met.

In addition:

- For Claims of Defective Shipped Merchandise or Not Suitable. The Cardholder email, letter, message of completed Dispute Form-Cardholder Claims Group must describe how the merchandise was broken, damaged, or otherwise unsuitable for the purpose sold. For example:
 - The cardholder ordered a table to be delivered. The table was delivered with a broken leg.
 - The cardholder received concert tickets after the concert date.
- For Claims of Goods and Services Did Not Conform to their Description. Both of the following:
 - The Cardholder email, letter, message of completed Dispute Form-Cardholder Claims Group must describe how the goods or services did not conform to the merchant's description, or the goods were of different quality, quantity, color, size or health of a plant or animal.

For example:

- The cardholder states that the quality or workmanship of the product is not as described as detailed by the merchant.
- A cardholder states that the specified color, size, or quantity is not as described as detailed by the merchant.
- The cardholder states that the goods were supposed to be genuine, but the cardholder claims that the goods were counterfeit.

The Cardholder may include any other documentation necessary to support the validity of the dispute; such documentation includes, but is not limited to, the original receipt, invoice, work order, brochure, contract, or appraisal.

- عند التسليم من التاجر، وصلت البضائع معيبة، أو لا يمكن استخدامها للغرض المقصود.
- السلع أو الخدمات غير مطابقة لموصفاتها. تشمل الأمثلة على سبيل المثال لا الحصر:
 - يدعي حامل البطاقة أن جودة المنتج أو صناعته، ليس كما هو موصوف.
 - يدعي حامل البطاقة أن اللون أو الحجم أو الكمية المحددة ليست كما هي موصوفة .
 - لم يلتزم التاجر بشروط وأحكام العقد المبرم مع حامل البطاقة بما في ذلك، على سبيل المثال لا الحصر، ضمان استرداد الأموال بنسبة 100% أو الوعود الخطية أو سياسة الاسترداد.

الإطار الزمني. واحد مما يلي:

- في غضون 120 يومًا تقويمياً من وقت توقف الخدمات، وبشرط أن لا يتجاوز 540 يومًا تقويمياً من تاريخ تسوية المعاملة بسبب مشاكل انقطاع الخدمات المستمرة.
- في غضون 120 يومًا من تاريخ تسليم البضائع أو الخدمات.
- في غضون 120 يومًا من تاريخ معالجة المعاملة.

المستندات المطلوبة. البريد الإلكتروني لحامل البطاقة، أو الخطاب أو الرسالة أو مجموعة مطالبات حامل البطاقة بنموذج النزاع المكتمل، بحيث يقوم حامل البطاقة بشرح شكواه بشكل دقيق حتى يتمكن جميع الأطراف من فهم موضوع النزاع.

هذا يعني أن البريد الإلكتروني أو الخطاب أو الرسالة لحامل البطاقة يجب أن يوثق كيفية استيفاء كل نقطة من شروط إنشاء رد المبالغ المدفوعة.

فضلاً عن ذلك يجب أن تتضمن:

- لمطالبات البضائع المشحونة المعيبة أو غير الصالحة للغرض المقصود. يجب أن يصف البريد الإلكتروني لحامل البطاقة أو الخطاب أو الرسالة الخاصة بمجموعة مطالبات حامل البطاقة بنموذج النزاع يصف عيوب البضائع أو تلفها أو عدم ملاءمتها للغرض الذي تم البيع من أجله. على سبيل المثال:
 - طلب حامل البطاقة تسليم طاولة لكن تم تسليم الطاولة بساق مكسورة.
 - استلام حامل البطاقة تذاكر الحفلة بعد تاريخ إقامتها.
 - لمطالبات السلع والخدمات التي لا تتوافق مع وصفها. كل مما يلي:
 - يجب أن يصف البريد الإلكتروني لحامل البطاقة، أو الخطاب أو الرسالة الخاصة بمطالبات حامل البطاقة بنموذج النزاع المكتمل كيف أن السلع أو الخدمات لا تتوافق مع وصف التاجر، أو أن البضائع كانت مختلفة في جودتها والكمية واللون والحجم أو الحالة الصحية للنبات أو الحيوان.

على سبيل المثال:

- يوضح حامل البطاقة أن جودة المنتج أو صناعته لم يتم وصفها كما هو موضح بالتفصيل من قبل التاجر.
 - يذكر حامل البطاقة أن اللون أو الحجم أو الكمية المحددة ليست كما هو موضح بالتفصيل من قبل التاجر.
 - يذكر حامل البطاقة أنه كان من المفترض أن تكون البضائع أصلية، ولكنها كانت بضائع مقلدة.
- يجوز لحامل البطاقة إضافة أي وثائق أخرى، يقدر إنها ضرورية لدعم صحة ادعاءاته؛ تتضمن هذه الوثائق، على سبيل المثال لا الحصر، الإيصال الأصلي أو الفاتورة أو أمر العمل أو الكتيب أو العقد أو التقييم الأصلي.

- Documentation from an expert or professional (on their business letterhead, with a business card attached, or validated by other information demonstrating that the opinion expressed is that of a qualified expert or professional) that supports the Cardholder’s dispute about the level of quality or misrepresentation.
- For Claims of Terms and Conditions of a Contract are Not as Described. The Cardholder email, letter, message of completed Dispute Form-Cardholder Claims Group must describe how the terms and conditions of the original contract or agreement were changed without the cardholder’s consent. For example: 100 percent money back guarantee, written promises, or return policy

Required Comment. None

Notes. This chargeback is not available when proper disclosure of the conditions of the goods is made at the time of the sale, such as when goods are sold in “as is” condition.

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove the goods or service were as described or not defective.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. Any relevant documents to support the Acquirer’s claim. An example includes, but is not limited to any correspondence with the Cardholder in which the Cardholder confirms receiving the described goods or service in good condition

Required Comment. None.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Both of the following:

- Date of the processed refund
- Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. One or more of the following:

- The Issuer did not meet the chargeback conditions
- Any of the chargeback data was invalid

- تقرير من خبير (على ورق الأعمال الخاص بهم، مع إرفاق بطاقة العمل، أو التحقق من صحتها من خلال معلومات أخرى توضح أن الرأي المعبر عنه هو رأي خبير) يؤيد ادعاء حامل البطاقة حول مستوى الجودة أو عيوبها.

- لمطالبات شروط و أحكام العقد ليست كما هي موصوفة. يجب أن يصف البريد الإلكتروني لحامل البطاقة والخطاب ورسالة مجموعة مطالبات حامل البطاقة بنموذج النزاع المكتمل كيف تم الخروج عن أحكام العقد أو الإتفاقية الأصلية دون موافقة حامل البطاقة. على سبيل المثال: ضمان استرداد الأموال بنسبة 100% أو الوعود المكتوبة أو سياسة الإرجاع.

التعليق المطلوب. لا يوجد.

ملاحظات. لا يجوز رد المبالغ المدفوعة، عندما يتم الإفصاح بشكل صحيح عن أوصاف البضائع في وقت البيع، مثل عندما يتم بيع البضائع في حالة “كما هي”.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 المستندات المرفقة وسبل المعالجة
- RSN02 ائتمان تم إصداره مسبقًا
- RSN03 رد المبالغ المدفوعة غير صالح
- RSN04 كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.
- RSN05 لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 تكرار رد المبالغ المدفوعة.
- RSN08 المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة .

شرط رفض رد المبالغ المدفوعة. يجوز للقابل إثبات أن السلع أو الخدمة كانت كما هي موصوفة، أو غير معيبة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. أي مستندات ذات صلة لدعم مطالبة القابل، على سبيل المثال، أية مراسلة مع حامل البطاقة التي يؤكد فيها استلام السلع أو الخدمة الموصوفة بحالة جيدة.

التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى حامل البطاقة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد.

التعليق المطلوب. كلا ما يلي:

- تاريخ الاسترداد الذي تمت معالجته.
- رقم مرجعي مميز للمقاصة للاسترداد.

رمز السببRSN03 . - رد المبالغ المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. واحد أو أكثر مما يلي:

- لم تف جهة الإصدار بشروط رد المبالغ المدفوعة.
- كانت أي من بيانات رد المبالغ المدفوعة غير صالحة.

- PAN and Unique Clearing Reference Number included in the chargeback did not match any presentment records.
-

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition: The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code: RSN05-Chargeback documents were not received)

Chargeback Rejection Condition: The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comments. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.2.2 Requesting Goods or Services Not Received

Reason Code. CBCD06

Chargeback Creation Condition. The Cardholder contacted the Issuer claiming all of the following occurred:

- The Cardholder participated in the disputed Transaction
- The merchandise/service was never provided
- The Cardholder contacted the Merchant, or attempted to contact the Merchant, to resolve the dispute
- The Cardholder and Merchant could not resolve the dispute

- لا يتطابق رقم الحساب الأساسي ورقم مرجع المقاصة الفريد والمضمن في طلب رد المبالغ المدفوعة مع سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. الشرط الذي لم تستوفه جهة الإصدار.

رمز السبب. RSN04 - كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.

شرط رفض رد المبالغ المدفوعة. كانت المستندات المطلوبة والتي قدمتها جهة الإصدار إما غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة، أو غير مكتملة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN05 لم يتم استلام مستندات رد المبالغ المدفوعة.

شرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. -RSN07 إعادة تحميل المبالغ المكررة.

شرط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليقات المطلوبة. معرف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. -RSN08 رد المبالغ المدفوعة خارج الإطار الزمني.

شرط رفض رد المبالغ المدفوعة. يجب أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

2.2.2.2 طلب بضائع أو خدمات لم يتم استلامها

رمز السبب. CBCD06

شرط إنشاء رد المبالغ المدفوعة. يجب أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مدعيًا حدوث كل ما يلي:

- شارك حامل البطاقة في المعاملة المتنازع عليها.
- لم يتم تقديم البضائع أو الخدمة.
- تواصل حامل البطاقة بالتاجر أو محاولة الاتصال بالتاجر لتسوية النزاع.
- لم يتمكن حامل البطاقة والتاجر من تسوية النزاع.

Time Frame.

- In cases involving delayed delivery of goods or services and the delivery or performance date was not specified by the Merchant: the Issuer must wait 30 calendar days from the Transaction date before submitting a chargeback and not to exceed 120 calendar days from the Transaction processing date.
- However, the Issuer may charge back the Transaction immediately (and not wait the 30 calendar days) upon learning the Merchant will not provide the goods or services because, for example, for the Merchant is no longer in business.
- In cases involving delayed delivery of goods or services and the delivery or performance date was specified by the Merchant and the latest anticipated delivery or performance date was specified by the Merchant has passed: within 120 calendar days of the latest anticipated delivery or performance date specified by the Merchant.
- However, the Issuer may charge back the Transaction immediately (and not wait until the latest anticipated delivery or performance date has passed) upon learning the Merchant will not provide the goods or services because, for example, for the Merchant is no longer in business.
- In cases involving interruption of ongoing services, within 120 calendar days of the date the Cardholder becomes aware that the service ceased. A chargeback must not be processed after 540 calendar days from the Transaction processing date.
- In all other cases: within 120 calendar days from the Transaction processing date.

Required Documents. A Cardholder letter, email, message, or completed Dispute Form-Cardholder Claims Group describing the Cardholder's complaint in sufficient detail to enable all parties to understand the dispute and a reasonably specific tokenization of the goods/services purchased.

Required Comment. None

Notes.

This chargeback applies when the Cardholder receives an empty box or a box containing worthless items, such as bricks or a stack of paper.

Interruption of ongoing services

The Issuer must only charge back an amount representing the services not received by the Cardholder.

When an end date was not defined, then the Issuer must calculate the prorated amount based upon 18 months.

For example, the Cardholder purchased a lifetime membership for LYD 1,000. The Merchant goes out of business after three months. The amount to be charged back is LYD 833 (LYD 1,000 divided by 18 months = LYD 55 per month. 18 months minus 3 months = 15. LYD 55 * 15 = LYD 833.)

الإطار الزمني.

- في الحالات التي يترتب عليها تأخير في تسليم البضائع أو الخدمات، ولم يتم تحديد تاريخ التسليم أو أداء الخدمة من قبل التاجر: يجب أن تنتظر جهة الإصدار 30 يومًا تقويميًا من تاريخ المعاملة قبل تقديم طلب رد المبالغ المدفوعة وألا يتجاوز 120 يومًا تقويميًا من تاريخ تسوية المعاملة.
- ومع ذلك، يجوز لجهة الإصدار استرداد قيمة المعاملة على الفور (وعدم الانتظار لمدة 30 يومًا تقويميًا) عند معرفة أن التاجر لن يقدم السلع أو الخدمات لأنه ، على سبيل المثال، لم يعد التاجر يمارس عمله.
- في الحالات التي يترتب عليها تأخير في تسليم البضائع أو الخدمات وتم تحديد تاريخ التسليم أو أداء الخدمة من قبل التاجر وتم انقضاء آخر موعد للتسليم أو الأداء المتوقع من قبل التاجر: في غضون 120 تقويميًا يومًا من آخر تسليم متوقع أو تاريخ أداء محدد بواسطة التاجر.
- ومع ذلك، قد تقوم جهة الإصدار بإعادة تحميل المعاملة على الفور (ولا تنتظر حتى انقضاء آخر موعد للتسليم أو الأداء المتوقع) عند معرفة أن التاجر لن يقدم السلع أو الخدمات، لأنه، على سبيل المثال، لم يعد يمارس عمله.
- في الحالات التي يترتب عليها انقطاع الخدمات بشكل مستمر، في غضون 120 يومًا تقويميًا من تاريخ علم حامل البطاقة بتوقف الخدمة. ويجب ألا تتم تسوية عملية رد المبالغ المدفوعة بعد انقضاء 540 يومًا تقويميًا من تاريخ تسوية المعاملة.
- في جميع الحالات الأخرى: في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة.

المستندات المطلوبة. خطاب حامل البطاقة أو بريد إلكتروني أو رسالة أو مجموعة مطالبات حامل البطاقة بنموذج نزاع مكتمل تصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع ووصف محدد بشكل معقول للسلع/ الخدمات المشتراة.

التعليق المطلوب. لا يوجد

ملاحظات.

تنطبق عملية رد المبالغ المدفوعة، عندما يتلقى حامل البطاقة صندوقًا فارغًا أو صندوقًا يحتوي على عناصر لا قيمة لها، مثل الطوب أو كومة من الورق.

انقطاع الخدمات الجارية

يجب على جهة الإصدار فقط، أن تقوم بخصم مبلغ يساوي قيمة الخدمات التي لم يتلقاها حامل البطاقة.

ويجب على جهة الإصدار، عندما لم يتم تحديد تاريخ الانتهاء أن تقوم بحساب المبلغ النسبي على أساس 18 شهرًا.

على سبيل المثال، اشترى حامل البطاقة، عضوية مدى الحياة مقابل 1000 دينار ليبي. توقف التاجر عن ممارسة نشاطه بعد ثلاثة أشهر. المبلغ المطلوب رده هو 833 دينارًا ليبيًا (1000 دينار ليبي مقسومًا على 18 شهرًا = 55 دينارًا ليبيًا في الشهر. 18 شهرًا ناقص 3 أشهر = 15. 55 دينارًا ليبيًا * 15 = 833 دينارًا ليبيًا).

This chargeback does not apply when

- The Cardholder has taken possession of the merchandise from the Merchant and subsequently decided to have the merchandise shipped by a third party.
- The goods are being held in customs for unpaid duty or customs fees. The Cardholder is obligated to pay the appropriate fees.
- The Merchant delivered the merchandise and the Cardholder refused to accept delivery.
- The Cardholder signed a waiver absolving the Merchant from responsibility when the merchandise is not received.
- For example: A Cardholder purchases vase and arranges with the Merchant to have the vases shipped to another country. At the time of purchase, the Cardholder signs a waiver form that states: “PROOF OF DISPATCH OF THE MERCHANDISE WILL BIND THE CARDHOLDER.” The vases never arrive, and the Cardholder contacts the Merchant. The Merchant provides documentation to show that the merchandise was shipped. By signing the waiver, the Cardholder absolved the Merchant of liability for merchandise that the Cardholder did not receive.
- The Cardholder declined insurance
- For example: The Merchant provides the Cardholder with an opportunity to purchase insurance on the merchandise to be delivered. Normally, such insurance stipulates that the Cardholder must initiate claims that limit the Merchant responsibility to the presenting documentation that verifies shipment or dispatch. The Merchant should provide a signed waiver of liability obtained from the Cardholder when the Cardholder declined to purchase insurance, along with documentation that shows that the Merchant shipped the merchandise.

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove:

- The Cardholder, or designated recipient, received the merchandise or service.
- The Acquirer can prove the Cardholder, or designated recipient, refused delivery of the merchandise or service.
- The Acquirer can prove the Cardholder, or designated recipient, waived the Merchant’s liability for delivering the merchandise or service.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. Any relevant documents to support the Acquirer’s claim. Examples include, but are not limited to, signed delivery receipt, any correspondences with the Cardholder in which the Cardholder confirms receiving the merchandise or service, documents proving the Cardholder used the service.

ولا تنطبق عملية رد المبالغ المدفوعة على الحالات التالية:

- استحواذ حامل البطاقة على البضائع من التاجر، وقرر بعد ذلك شحن البضائع من قبل طرف ثالث.
- إذا تم حجز البضائع في الجمارك مقابل رسوم جمركية أو رسوم جمركية غير مدفوعة. ويلتزم حامل البطاقة في هذه الحالة بدفع الرسوم المناسبة.
- إذا قام التاجر بتسليم البضائع، ورفض حامل البطاقة قبول التسليم.
- إذا وقع حامل البطاقة على تنازل يعفي التاجر من المسؤولية عند عدم استلام البضائع.
- على سبيل المثال: أن يشتري حامل البطاقة إناء ويرتب مع التاجر لشحن المزهريات إلى بلد آخر. في وقت الشراء، ويوقع حامل البطاقة على شرط تعاقد ي نص على: “إثبات إرسال البضاعة سيلزم حامل البطاقة”. لا تصل المزهريات أبدًا ويتواصل حامل البطاقة مع التاجر. ويقدم التاجر الوثائق لإثبات أنه تم شحن البضائع. من خلال التوقيع على التنازل، فإن حامل البطاقة يعفي التاجر من المسؤولية عن البضائع التي لم يستلمها حامل البطاقة.
- رفض حامل البطاقة التأمين
- على سبيل المثال: يمنح التاجر، لحامل البطاقة فرصة لقبول شرط التأمين على البضائع التي سيتم تسليمها. عادة، ينص شرط التأمين هذا على أنه؛ يجب على حامل البطاقة الشروع في مطالبات تقصر مسؤولية التاجر على تقديم المستندات التي تتحقق من الشحن أو الإرسال. ويجب أن يقدم التاجر تنازلًا موقّعًا عن المسؤولية تم الحصول عليه من حامل البطاقة عندما رفض حامل البطاقة شرط التأمين، إلى جانب المستندات التي توضح أن التاجر قام بشحن البضائع.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة.
- RSN02 - ائتمان تم إصداره مسبقًا.
- RSN03 - رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل الإنصاف

شرط رفض رد المبالغ المدفوعة. يجوز للقابل إثبات:

- أن حامل البطاقة، أو نائبه، قد استلم البضائع أو الخدمة.
- أن حامل البطاقة أو نائبه، رفض تسليم البضائع أو الخدمة.
- أن حامل البطاقة، أو نائبه، قد تنازل عن مسؤولية التاجر عن تسليم البضائع أو الخدمة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. أي مستندات ذات صلة لإثبات ادعاء القابل. مثال ذلك، إيصال التسليم الموقع، وأي مراسلات مع حامل البطاقة يؤكد فيها حامل البطاقة استلام البضائع أو مقدم الخدمة، والمستندات التي تثبت استخدام حامل البطاقة للخدمة.

بالنسبة لحالات رفض التسليم: المستندات التي تثبت مطالبة التاجر، على سبيل المثال: ملاحظات شركة التوصيل أو أي مراسلات بين التاجر وحامل البطاقة تفيد أن حامل البطاقة يرفض التسليم.

For cases of delivery refusal: Documents proving the Merchant's claim, for example: delivery company feedback or any correspondences between Merchant and Cardholder in which the Cardholder refuses delivery.

For case of waiver agreement: A copy of the agreement in which the Cardholder absolves the Merchant from responsibility should the merchandise not be received and any other relevant documents/details.

Required Comment. None.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents.

For all other cases: None

Required Comment. The condition the Issuer did not meet.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition: The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comments. None

Reason Code: RSN05-Chargeback documents were not received)

Chargeback Rejection Condition: The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comments. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comments. Chargeback ID of the previously received chargeback.

في حالة وجود اتفاقية التنازل: نسخة من الإتفاقية المتضمنة للشروط التي تعفي فيها حامل البطاقة التاجر من المسؤولية في حالة عدم استلام البضائع وأي مستندات/ تفاصيل أخرى ذات صلة. التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا.

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. تاريخ الاسترداد الذي تمت معالجته والرقم المرجعي الفريد للمقاصة للاسترداد.

رمز السبب. -RSN03 رد المبالغ المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. لم تفي جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد المبالغ المدفوعة غير صالح، أو أن حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة.

لجميع الحالات الأخرى: لا يوجد.

التعليق المطلوب. الشرط الذي لم تستوفيه جهة الإصدار.

رمز السبب. RSN04 - كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة

شرط رفض رد المبالغ المدفوعة: أن تكون المستندات المطلوبة التي قدمتها جهة الإصدار إما غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة، أو غير مكتملة.

الإطار زمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليقات المطلوبة. لا توجد.

رمز السبب: RSN05 لم يتم استلام مستندات رد المبالغ المدفوعة.

شرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة المطلوبة لرد المبالغ المدفوعة.

الإطار زمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليقات المطلوبة. لا توجد.

رمز السبب. -RSN07 إعادة تحميل المبالغ المكررة

شرط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار زمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليقات المطلوبة. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.2.3 Credit Not Received

Reason Code. CBCD09

Chargeback Creation Condition. The Cardholder contacted the Issuer claiming one of the following:

- The Merchant granted the Cardholder a refund but failed to process that same refund to the National Scheme Operator Card.
- The disputed Transaction was voided, the Cardholder has a sales receipt marked as voided by the Merchant, but the disputed Transaction was still processed.
- The Merchant posted a credit for a reduced amount without proper disclosure to the Cardholder.

Time Frame. One of the following:

- Between 15 and 120 calendar days from the date on the credit documentation, or the date the service was canceled, or the goods were returned.
- When waiting the 15 calendar days would cause the Issuer to exceed the 120 calendar day time frame, the Issuer may chargeback the Transaction earlier than 15 calendar days.
- When the credit documentation is dated, the 120-day chargeback time frame counts the date on the credit documentation as day zero.
- When the credit documentation is undated, the 120-day time frame counts the date on the Cardholder letter, email, or message as day zero.
- When the Cardholder letter is undated, the chargeback time frame counts the receipt date of the documentation by the Issuer as day zero.
- The Issuer can immediately charge back the Transaction upon receiving one of the following forms of credit documentation:
 - A letter from the Merchant advising the Issuer to obtain credit using a chargeback
 - A sales receipt marked as voided by the Merchant

Required Documents. One of the following:

- A Cardholder letter, email, message, or completed Dispute Form-Cardholder Claims Group describing the Cardholder's complaint in sufficient detail to enable all parties to understand the dispute. This means that the Cardholder email, letter, or message must document how the Chargeback Conditions was met.
- Merchant documentation to support a credit is due to the Cardholder.
- A letter from the Merchant advising the Issuer or the Cardholder to obtain credit using a chargeback
- A sales receipt marked as voided by the Merchant

رمز السبب. -RSN08 رد المبالغ المدفوعة خارج الإطار الزمني

شروط رفض رد المبالغ المدفوعة. تمت معالجة عملية رد المبالغ المدفوعة خارج الإطار الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. لا يوجد

3.2.2.2. لم يتم استلام الائتمان

رمز السبب. CBCD09

شروط إنشاء رد المبالغ المدفوعة. أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مطالباً بإحدى الحالات التالية:

- منح التاجر لحامل البطاقة استرداداً لكنه فشل في معالجة نفس المبلغ المسترد إلى بطاقة مشغل شبكة الدفع المحلية.
- إذا تم إلغاء المعاملة المتنازع عليها، وكان حامل البطاقة لديه إيصال مبيعات تم إلغاؤه من قبل التاجر، ولكن المعاملة المتنازع عليها لا تزال قيد التسوية.
- إذا منح التاجر ائتماناً بمبلغ مخفض دون الإفصاح المناسب لحامل البطاقة.

الإطار الزمني. واحدة من الحالات التالية:

- في غضون فترة زمنية ما بين 15 و 120 يومًا تقويمياً من التاريخ المدون على مستند الائتمان، أو تاريخ إلغاء الخدمة، أو إعادة البضائع.
- عندما يؤدي الانتظار لمدة 15 يومًا تقويمياً إلى تجاوز جهة الإصدار ميعاد 120 يومًا تقويمياً، فقد تقوم جهة الإصدار بإعادة تحميل المعاملة قبل 15 يومًا تقويمياً.
- عندما يتم تأريخ وثائق الائتمان، يكون الإطار الزمني لرد المبالغ المدفوعة في غضون مدة 120 يومًا تقويمياً، مع اعتبار أن التاريخ الموجود في مستندات الائتمان على أنه اليوم صفر.
- عندما تكون وثائق الائتمان غير مؤرخة، يحسب الإطار الزمني لمدة 120 يومًا تقويمياً، من التاريخ الموجود في خطاب حامل البطاقة أو البريد الإلكتروني أو الرسالة على أنه اليوم صفر.
- عندما يكون خطاب حامل البطاقة غير مؤرخ، يحسب الإطار الزمني لرد المبالغ المدفوعة من تاريخ استلام المستندات من قبل جهة الإصدار على أنه اليوم صفر.
- يمكن لجهة الإصدار استرداد قيمة المعاملة فوراً عند استلام أحد أشكال المستندات الائتمانية التالية:
 - خطاب من التاجر ينصح جهة الإصدار بالحصول على ائتمان باستخدام طريقة رد المبالغ المدفوعة.
 - إيصال مبيعات تم إلغاؤه من قبل التاجر.

المستندات المطلوبة. واحدة من الآتي:

- خطاب حامل البطاقة أو بريد إلكتروني أو رسالة أو مجموعة مطالبات حامل البطاقة بنموذج نزاع مكتمل تصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع. هذا يعني أن البريد الإلكتروني أو الخطاب أو الرسالة لحامل البطاقة يجب أن يوثق كيفية استيفاء شروط رد المبالغ المدفوعة.
- مستندات التاجر لدعم الائتمان المستحق لحامل البطاقة.
- خطاب من التاجر ينصح فيه جهة الإصدار أو حامل البطاقة بالحصول على ائتمان باستخدام ميزة رد المبالغ المدفوعة.
- إيصال مبيعات تم إلغاؤه من قبل التاجر.

Required Comment. None

Notes. When the Merchant informed the Cardholder of its refund policy at the time of purchase, the Cardholder must abide by that policy. For example, the Cardholder’s sales slip clearly indicates that the refund policy is “in-store credit only” or “no refunds.”

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. One of the following Conditions:

Condition 1. The Acquirer can prove the Merchant issued a refund to the Cardholder with another method, for example cash.

Condition 2. The Acquirer can prove the lesser credit amount was the correct amount due as a refund.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. Any relevant documents to support the Acquirer’s claim. An example includes, but is not limited to: a refund receipt signed by the Cardholder showing the alternate payment method.

Required Comment. None.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

التعليق المطلوب. لا يوجد.

ملاحظات: إذا أفصح التاجر لحامل البطاقة بسياسة الاسترداد الخاصة به وقت الشراء، يجب على حامل البطاقة الالتزام بهذه السياسة. على سبيل المثال ، تشير قسيمة مبيعات حامل البطاقة بوضوح إلى أن سياسة الاسترداد هي “رصيد في المتجر فقط” أو “لا يوجد رد أموال”.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقًا.
- RSN03 - رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة
- RSN07 - تكرار رد المبالغ المدفوعة
- RSN08 - إذا كان رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شرط رفض رد المبالغ المدفوعة. أحد الشروط التالية:

الشرط 1. يجوز للقابل إثبات أن التاجر قد رد الأموال لحامل البطاقة بطريقة أخرى، على سبيل المثال نقدًا.

الشرط 2. يجوز للقابل إثبات أن الحد الأدنى لمبلغ الائتمان، هو المبلغ الصحيح المستحق للرد.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. أي مستندات ذات صلة لإثبات ادعاء القابل، على سبيل المثال، إيصال استرداد موقع من قبل حامل البطاقة يوضح طريقة الدفع البديلة.

التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا.

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويته والرقم المرجعي الفريد للمقاصة للاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. لم تفي جهة الإصدار بشروط رد المبالغ المدفوعة، أو أن أيًا من بيانات رد المبالغ المدفوعة كانت غير صالحة، أو أن حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. الشرط الذي لم تستوفيه جهة الإصدار.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition: The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code: RSN05-Chargeback documents were not received)

Chargeback Rejection Condition: The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comments. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.2.4 Recurring Transaction

A recurring Transaction allows for continuous billing without a specified end date.

Chargeback Reason Code. CBCD03

Chargeback Creation Condition. The Cardholder contacted the Issuer claiming one of the following Conditions:

Condition 1: The Cardholder notified the Merchant to cancel the recurring Transaction and the Merchant continued to bill the Cardholder.

Condition 2: The Cardholder was not aware that the Cardholder was agreeing to a recurring Transaction.

In addition, the disputed recurring Transaction was a non-face-to-face Transaction.

Time Frame. Within 120 calendar days of the Transaction processing date.

Required Documents. One of the following Conditions corresponding to the Chargeback Rejection Condition in this same subsection:

رمز السبب: RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة

شرط رفض رد المبالغ المدفوعة: أن تكون المستندات المطلوبة والتي قدمتها جهة الإصدار إما غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة، أو غير مكتملة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN05 لم يتم استلام مستندات رد المبالغ المدفوعة.

شرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. -RSN07 إعادة تحميل المبالغ المكررة.

شرط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليقات المطلوبة. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. -RSN08 ردالمبالغ المدفوعة خارج الإطار الزمني

شرط رفض رد المبالغ المدفوعة. أن تكون عملية تسوية رد المبالغ المدفوعة قد تمت خارج الإطار

الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. لا يوجد

4.2.2.2. معاملة متكررة

تسمح المعاملة المتكررة بالفوترة المستمرة بدون تاريخ انتهاء محدد.

رمز سبب رد المبالغ المدفوعة. CBCD03

شرط إنشاء رد المبالغ المدفوعة. أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مطالباً بواحد من الشروط التالية:

الشرط 1: أن يقوم حامل البطاقة بإخطار التاجر بإلغاء المعاملة المتكررة واستمر التاجر في إصدار فاتورة لحامل البطاقة.

الشرط 2: أن يكون حامل البطاقة غير عالم بموافقة حامل البطاقة على إجراء معاملة متكررة.

بالإضافة إلى ذلك، إذا كانت المعاملة المتكررة المتنازع عليها هي معاملة غير تقابلية، أي إنها لم تتم (وجهًا لوجه).

الإطار الزمني. في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة.

المستندات المطلوبة. أحد الشروط التالية المقابلة لشرط رفض رد المبالغ المدفوعة في هذا القسم الفرعي نفسه:

Condition 1: A Cardholder letter, email, message, or completed Dispute Form-Cardholder Claims Group form describing how and when the Cardholder cancelled the recurring Transaction arrangement. Examples include, but are not limited to:

- A Cardholder summary of a telephone conversation between the Cardholder and the Merchant requesting cancellation of the recurring Transaction
- A copy of correspondence between the Cardholder and the Merchant requesting cancellation of the recurring Transaction.

Condition 2: A Cardholder letter, email, message, or completed Dispute Form-Cardholder Claims Group form stating that the Cardholder was not aware that the Cardholder was agreeing to a recurring Transaction.

Required Comment. None

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN06-Previous authorization obtained
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Chargeback Reason Code. RSN01-Attached Documents and Remedy

Chargeback Creation Condition. One of the following Conditions:

Condition 1: The Acquirer can prove the Cardholder never canceled the recurring Transaction and the recurring goods or services were provided until the chargeback date.

Condition 2: The Acquirer can prove the Cardholder was notified of the recurring nature of the Transaction, and the Cardholder agreed to the recurring Transaction.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. One of the following Conditions corresponding to the Chargeback Rejection Condition in this same subsection:

Condition 1: Any relevant documents to support the Acquirer's claim. Examples include, but are not limited to, recent correspondence with the Cardholder confirming the Cardholder did not cancel the recurring Transaction, reports of recent service used by Member.

Condition 2: Any relevant documents to support the Acquirer's claim. Examples include, but are not limited to, correspondence with the Cardholder confirming agreement with the recurring terms or signed contract.

Required Comment. None.

الشرط 1: خطاب لحامل البطاقة، أو بريد إلكتروني، أو رسالة، أو نموذج مجموعة مطالبات حامل البطاقة بنموذج نزاع كامل يصف كيف ومتى ألغى حامل البطاقة ترتيب المعاملة المتكررة. على سبيل المثال:

- ملخص حامل البطاقة لمحادثة هاتفية بين حامل البطاقة والتاجر يطلب إلغاء المعاملة المتكررة.
- نسخة من المراسلات بين حامل البطاقة والتاجر لطلب إلغاء المعاملة المتكررة.

الشرط 2: خطاب لحامل البطاقة أو بريد إلكتروني أو رسالة أو نموذج مجموعة مطالبات حامل البطاقة بنموذج نزاع كامل يوضح أن حامل البطاقة لم يكن على علم بموافقة حامل البطاقة على معاملة متكررة.

التعليق المطلوب. لا يوجد.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 المستندات المرفقة وسبل المعالجة
- RSN02 ائتمان تم إصداره مسبقاً.
- RSN03 رد المبالغ المدفوعة غير صالح.
- RSN04 إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة
- RSN05 إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN06 تم الحصول على التفويض السابق.
- RSN07 تكرار رد المبالغ المدفوعة.
- RSN08 رد المبالغ المدفوعة خارج الإطار الزمني.

رمز سبب رد المبالغ المدفوعة. - RSN01 المستندات المرفقة وسبل المعالجة .

شرط إنشاء رد المبالغ المدفوعة. أحد الشروط التالية:

الشرط 1: أن يقوم القابل بإثبات عدم قيام حامل البطاقة بإلغاء المعاملة المتكررة، وقد تم توفير السلع أو الخدمات المتكررة حتى تاريخ رد المبالغ المدفوعة.

الشرط 2: أن يقوم القابل بإثبات أن حامل البطاقة قد تم إخطاره بالطبيعة المتكررة للمعاملة، ووافق حامل البطاقة عليها.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. أحد الشروط التالية المقابلة لشرط رفض رد المبالغ المدفوعة في هذا القسم الفرعي نفسه:

الشرط 1: أي مستندات ذات صلة لإثبات ادعاء القابل. على سبيل المثال، المراسلات الأخيرة مع حامل البطاقة التي تؤكد أن حامل البطاقة لم يبلغ المعاملة المتكررة، وتقارير الخدمة الأخيرة التي استخدمها العضو.

الشرط 2: أي مستندات ذات صلة لإثبات ادعاء القابل. على سبيل المثال، المراسلات مع حامل البطاقة لتأكيد الاتفاق مع الشروط المتكررة أو العقد الموقع.

التعليق المطلوب. لا يوجد.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number (DE 57) fields in chargeback did not match any presentment records.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. The condition the Issuer did not meet.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition: The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

Reason Code: RSN05-Chargeback documents were not received)

Chargeback Rejection Condition: The Required Documents required for this chargeback were not received.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comments. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شُرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة
الإطار الزمني . في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد
التعليق المطلوب. تاريخ الاسترداد الذي تمت معالجته والرقم المرجعي الفريد للمقاصة للاسترداد

رمز السبب. -RSN03 رد المبالغ المدفوعة غير صالح:

شُرط رفض رد المبالغ المدفوعة. لم تف جهة الإصدار بشروط رد المبالغ المدفوعة ، أو أن أيًا من بيانات رد المبالغ المدفوعة غير صالح، أو أن حقل رقم الحساب الأساسي والرقم المرجعي الفريد للمقاصة (DE 57) في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد
التعليق المطلوب. الشرط الذي لم تستوفه جهة الإصدار.

رمز السبب. RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة

شُرط رفض رد المبالغ المدفوعة: أن تكون المستندات المطلوبة التي قدمتها جهة الإصدار إما غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة، أو غير مكتملة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد..

رمز السبب. RSN05 لم يتم استلام مستندات رد المبالغ المدفوعة.

شُرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

رمز السبب. -RSN07 إعادة تحميل المبالغ المكررة

شُرط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليقات المطلوبة. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب.. -RSN08 رد المبالغ المدفوعة خارج الإطار الزمني.

شُرط رفض رد المبالغ المدفوعة: أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار الزمني لرمز سبب رد المبالغ المدفوعة.
الإطار الزمني. في غضون 20 يوم عمل و تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

2.2.2.5 Subsequent Transaction Disputed

A subsequent Transaction dispute is the dispute of a separate Transaction that occurs after a valid Transaction involving the same Merchant and the same Cardholder.

Code: CBCD08

Chargeback Creation Condition. The Cardholder contacted the Issuer claiming all of the following:

- The Cardholder engaged in a valid Transaction with the Merchant.
- A subsequent Transaction (including for loss, theft, or damage) occurred with that same Merchant without the Cardholder's consent.
- The Cardholder contacted the Merchant, or attempted to contact the Merchant, to resolve the dispute.
- The Merchant refused to resolve the issue.

Time Frame. Within 120 calendar days of the processing date of the disputed subsequent Transaction.

Required Document. A Cardholder letter, email, message, or completed Dispute Form-Cardholder Claims Group describing the Cardholder's complaint in sufficient detail to enable all parties to understand the dispute. This means that the Cardholder email, letter, or message must document how each point of the Chargeback Creation Conditions was met. Required Comment. None

Notes. The right to charge back the disputed amount is not dependent on the method of payment for the original Transaction. For example, the Cardholder may have paid cash for the accepted Transaction, but the disputed subsequent Transaction was applied to the National Scheme Operator card because the Cardholder presented the National Scheme Operator Card to the Merchant to guarantee the service.

Cardholders are responsible for valid subsequent Transactions. Examples include, but are not limited to: meals that were signed for by the Cardholder but not included in the final hotel folio or for parking tickets/traffic fines issued while the vehicle was in the Cardholder's possession.

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove the Cardholder authorized the disputed Transaction or that the disputed Transaction was not a subsequent Transaction but an independent Transaction.

5.2.2.2. المعاملات اللاحقة المتنازع عليها

نزاع المعاملات اللاحقة هو ذلك النزاع الذي يتعلق بمعاملة منفصلة يحدث بعد معاملة صحيحة تتعلق بذات التاجر ونفس حامل البطاقة.

الرمز: CBCD08

شرط إنشاء رد المبالغ المدفوعة. أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مطالباً بكل ما يلي:

- أن تكون هناك معاملة صحيحة بين حامل البطاقة والتاجر.
- أن تكون المعاملة اللاحقة (بما في ذلك الخسائر أو السرقة أو التلف) قد حدثت مع ذات التاجر ودون الحصول على موافقة حامل البطاقة.
- أن يكون حامل البطاقة قد اتصل بالتاجر أو حاول الاتصال بالتاجر لتسوية النزاع.
- أن يكون التاجر قد رفض تسوية المنازعة.

الإطار الزمني. في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة المتنازع عليها اللاحقة.

المستندات المطلوبة خطاب حامل البطاقة أو بريد إلكتروني أو رسالة أو مجموعة مطالبات حامل البطاقة بنموذج نزاع مكتمل تصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع. هذا يعني أن البريد الإلكتروني أو الخطاب أو الرسالة لحامل البطاقة يجب أن يوثق كيفية استيفاء كل نقطة من شروط إنشاء رد المبالغ المدفوعة . التعليق المطلوب. لا يوجد.

ملاحظات: لا يعتمد الحق في استرداد المبلغ المتنازع عليه على طريقة الدفع للمعاملة الأصلية. على سبيل المثال، فقد يكون حامل البطاقة قد دفع نقدًا للمعاملة المقبولة، ولكن تم تطبيق المعاملة المتنازع عليها اللاحقة على بطاقة مشغل شبكة الدفع المحلية لأن حامل البطاقة قدم بطاقة مشغل شبكة الدفع المحلية إلى التاجر لضمان الخدمة.

يتحمل حاملو البطاقات مسؤولية المعاملات اللاحقة الصحيحة ، على سبيل المثال : الوجبات التي وقع عليها حامل البطاقة ولكنها غير مدرجة في سجل الفندق النهائي أو تذاكر وقوف السيارات / غرامات المرور الصادرة أثناء وجود السيارة في حوزة حامل البطاقة.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقًا
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة.

شرط رفض رد المبالغ المدفوعة. يجوز للقابل إثبات أن حامل البطاقة وافق على المعاملة المتنازع

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. Any relevant documents to support the Acquirer's claim. Examples include, but are not limited to, a sales receipt indicating the CVM used (when signature was the CVM then the sales receipt must include the Cardholder's signature). Note: Signature on file is not a valid CVM.

When the subsequent Transaction was related to a valid service that Cardholder received and was liable for according to contract/agreement between the Merchant and the Cardholder, the Acquirer must provide the contract supporting his claim and to prove that the disputed Transaction occurred during the contract/agreement time frame.

When the Merchant stated that the disputed Transaction is not a subsequent Transaction, the Acquirer must provide full details of the Transaction including, but not limited to, the sales receipt.

Required Comment. None.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition: The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code: RSN05-Chargeback documents were not received

Chargeback Rejection Condition: The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

عليها، أو أن المعاملة المتنازع عليها لم تكن معاملة لاحقة ولكنها كانت معاملة مستقلة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. أي مستندات ذات صلة لإثبات ادعاء القابل. على سبيل المثال، إيصال مبيعات يشير إلى CVM المستخدمة (عندما كان التوقيع هو CVM ، يجب أن يتضمن إيصال المبيعات توقيع حامل البطاقة). ملاحظة: التوقيع في الملف ليس CVM صالحًا.

إذا كانت المعاملة اللاحقة مرتبطة بخدمة صالحة حصل عليها حامل البطاقة وكان مسؤولاً عنها وفقًا للعقد/ الإيفاق المبرم بين التاجر وحامل البطاقة، فإنه يجب على القابل تقديم العقد الذي يدعم مطالبته، وإثبات أن المعاملة المتنازع عليها وقعت أثناء سريان العقد/ الإيفاق. وإذا أثبت التاجر أن المعاملة المتنازع عليها، ليست معاملة لاحقة، فإنه يجب على القابل تقديم التفاصيل الكاملة للمعاملة بما في ذلك ، على سبيل المثال إيصال المبيعات. التعليق المطلوب. لا يوجد.

رمز السبب. RSN02- ائتمان تم إصداره مسبقًا

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى حامل البطاقة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويته والرقم المرجعي الفريد لمقاصة الاسترداد

رمز السبب. RSN03 عدم صلاحية رد المبالغ المدفوعة.

شرط رفض رد المبالغ المدفوعة. لم تفي جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد المبالغ المدفوعة غير صحيحة، أو أن حقلي رقم الحساب الأساسي والرقم المرجعي الفريد للمقاصة في عملية رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. الشرط الذي لم تستوفه جهة الإصدار.

رمز السبب. RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة

شرط رفض رد المبالغ المدفوعة: أن تكون المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة، أو غير مكتملة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN05 لم يتم استلام مستندات رد المبالغ المدفوعة.

شرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.
Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.2.6 Lodging or Vehicle Rental “No-Show” Charged / Deposit Not Refunded

Code: CBCD11

Chargeback Condition. The Cardholder contacted the Issuer to dispute a “No-Show” deposit lodging or vehicle rental charge and claimed one of the following:

1. The Cardholder canceled the reservation and was charged a “No-Show” fee
2. The Cardholder properly canceled the reservation and the deposit Transaction was not refunded
3. The Cardholder used the accommodation or vehicle and was charged a “No-Show” fee
4. The Merchant provided alternate accommodations. For example, the Cardholder arrived at the hotel and no room was available. Although the hotel arranged for accommodations at another hotel, either the original Merchant billed the Cardholder or the Merchant providing the alternate accommodate billed the Cardholder.
5. The “No-Show” charge differed from the rate quoted to the Cardholder. Under these circumstances, only the difference between the two charges can be charged back.
6. The Merchant did not advise. the Cardholder that the Merchant would charge a “No-Show” fee.

Time Frame. Within 120 calendar days of the Transaction processing date.

Required Documents. A Cardholder letter, email, message, or completed Dispute Form-Cardholder Claims Group describing the Cardholder’s complaint in sufficient detail to enable all parties to understand the dispute and one of the following when applicable:

1. When available, cancellation number or other Merchant documentation confirmation cancellation
2. When the Cardholder paid for the alternative accommodation with an alternate form of payment, documentation of the payment method.
3. When the “No-Show” rate is being disputed or the Cardholder claims the Merchant did not disclose the “No-Show” policy or the reservation documents.

Required Comments. When the Cardholder paid for the alternative accommodation with a National Scheme Operator Card, the Unique Clearing Reference Number of the Transaction.

رمز السبب. -RSN07 إعادة تحميل المبالغ المكررة

شروط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. -RSN08 رد المبالغ المدفوعة خارج الإطار الزمني.

شروط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار

الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

6.2.2.2. لم يتم رد ايداع رسوم الإقامة أو استئجار المركبات “عدم الحضور” / الإيداع**الرمز: CBCD11**

شروط رد المبالغ المدفوعة. أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار للاعتراض على إيداع “عدم الحضور” أو رسوم استئجار السيارة، وقدم طلباً بأحد الحالات التالية:

1. قيام حامل البطاقة بإلغاء الحجز، وفرض عليه رسوم “عدم الحضور”.
2. قيام حامل البطاقة بإلغاء الحجز بشكل صحيح ولم يتم رد معاملة الإيداع.
3. استخدم حامل البطاقة مكان الإقامة أو السيارة وتم تحصيل رسوم “عدم الحضور”.
4. قدم التاجر، لحامل البطاقة، أماكن إقامة بديلة. على سبيل المثال ، وصل حامل البطاقة إلى الفندق وكانت غرف الفندق شاغرة. على الرغم من أن الفندق قام بترتيب أماكن الإقامة في فندق آخر، فإما ان يكون التاجر الأصلي قد أصدر فاتورة إلى حامل البطاقة أو ان التاجر الذي يقدم السكن البديل قد اصدر فواتير إلى حامل البطاقة
5. تختلف رسوم “عدم الحضور” عن السعر المعروض على حامل البطاقة. في ظل هذه الحالة ، لا يمكن استرداد سوى الفرق بين السعرين.
6. لم يقم التاجر بإخطار حامل البطاقة بأنه سيتقاضى رسوم “عدم الحضور”.

الإطار الزمني. في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة.

المستندات المطلوبة. خطاب حامل البطاقة أو بريد إلكتروني أو رسالة أو مجموعة مطالبات حامل البطاقة بنموذج نزاع مكتمل تصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع وواحد مما يلي عند الاقتضاء:

1. عند توفر رقم الإلغاء، أو إلغاء تأكيد التاجر الآخر.
2. عندما يدفع حامل البطاقة ثمن الإقامة البديل بطريقة دفع بديلة، توثيق طريقة الدفع.
3. عندما يكون معدل “عدم الحضور” محل نزاع، أو يدعي حامل البطاقة أن التاجر لم يفصح عن سياسة “عدم الحضور” او مستندات الحجز.

التعليقات المطلوبة. عندما دفع حامل البطاقة ثمن الإقامة البديلة باستخدام بطاقة مشغل شبكة الدفع المحلية، الرقم المرجعي الفريد لمقاصة المعاملة.

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. One of the following:

- The Merchant issued a refund to the Cardholder with another method, for example cash.
- The Transaction was not a “no-show” charge.
- The Merchant has no record of Cardholder cancellation and the Cardholder cannot provide a cancellation number. This condition is only permitted when the Merchant’s reservation program automatically generates correspondence (including but not limited to letter, email, or text) to the Cardholder with a cancellation number.
- The acquirer can provide documentation substantiating that the cardholder was advised before the date of the reservation that he would be billed a “No-Show” fee if the reservation was not cancelled before 18:00 (merchant’s local time) on the date of the reservation.
- For disputes involving the rate of the “No-Show” fee, the Acquirer can provide documentation proving that the Cardholder was notified of the rate before the date of the reservation.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. Any relevant documents to support the Acquirer’s claim.

Required Comment. None.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment.

For cases of delivery refusal: None

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقًا
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شروط رفض رد المبالغ المدفوعة. أحد الشروط التالية:

- أن يقوم التاجر برد أموال لحامل البطاقة بطريقة أخرى، على سبيل المثال نقدًا.
- المعاملة لم تكن رسوم “عدم الحضور”.
- إذا كان التاجر لا يمتلك سجل لإلغاء حامل البطاقة، ولا يمكن لحامل البطاقة تقديم رقم إلغاء. لا يُسمح بهذا الشرط إلا عندما يُنشئ برنامج حجز التاجر تلقائيًا مراسلات (بما في ذلك على سبيل المثال لا الحصر الخطاب أو البريد الإلكتروني أو الرسائل النصية) إلى حامل البطاقة برقم إلغاء.
- يمكن للقابل تقديم وثائق تثبت أن حامل البطاقة قد تم إخطاره قبل تاريخ الحجز بأنه سيتم محاسبته على رسوم “عدم الحضور” إذا لم يتم إلغاء الحجز قبل الساعة 18:00 (بالتوقيت المحلي للتاجر) في تاريخ الحجز .
- بالنسبة للنزاعات المتعلقة بمعدل رسوم “عدم الحضور” ، يجوز للقابل تقديم مستندات تثبت أن حامل البطاقة قد تم إخطاره بالسعر قبل تاريخ الحجز.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. أي مستندات ذات صلة لإثبات ادعاء القابل.

التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شروط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا يوجد.

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويته والرقم المرجعي الفريد لمقاصة الاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شروط رفض رد المبالغ المدفوعة. لم تف جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد المبالغ المدفوعة غير صحيحة، أو كان حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب:

في حالات رفض التسليم: لا يوجد.

For case of waiver agreement: None
For all other cases: The condition the Issuer did not meet.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition: The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

Reason Code: RSN05-Chargeback documents were not received

Chargeback Rejection Condition: The Required Documents required for this chargeback were not received.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

2.2.2.7 Transaction Did Not Complete

Code: CBCD12
Chargeback Creation Condition. The Cardholder contacted the Issuer claiming all of the following:

- The Cardholder engaged in the Transaction.
- The Cardholder claims the disputed Transaction failed to complete.
- The Cardholder did not use the goods or services.

In addition, the disputed recurring Transaction was not an Instant Credit Transaction (ICT) Funding Transaction.

Time Frame. Within 120 calendar days from the Transaction processing date.
Required Documents. Cardholder email, letter, message, or completed Dispute Form-Cardholder Claims Group describing the Cardholder’s complaint in sufficient detail to enable all parties to understand the dispute and a reasonably specific description of the goods/services purchased. This means that the Cardholder email, letter, or message must

في حالة اتفاق التنازل: لا يوجد.
بالنسبة لجميع الحالات الأخرى: الشرط الذي لم تستوفه جهة الإصدار.

رمز السبب: RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة/ غير كاملة.

شرط رفض رد المبالغ المدفوعة: إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة ، أو غير مكتملة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

رمز السبب. RSN05: إذا لم يتم استلام مستندات رد المبالغ المدفوعة.

شرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

رمز السبب. RSN07- إعادة تحميل المبالغ المكررة

شرط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08- رد المبالغ المدفوعة خارج الإطار الزمني.

شرط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار الزمني لرمز سبب رد المبالغ المدفوعة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

7.2.2.2. المعاملة لم تكتمل

الرمز: CBCD12

شرط إنشاء رد المبالغ المدفوعة. أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مطالباً بكل ما يلي:

- مشاركة حامل البطاقة في المعاملة.
- أن يدعي حامل البطاقة أن المعاملة المتنازع عليها لم تكتمل.
- أن حامل البطاقة لم يستخدم السلع أو الخدمات.

بالإضافة إلى ذلك، لم تكن المعاملة المتكررة المتنازع عليها معاملة تمويل فورية (ICT).

الإطار الزمني. في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة.
المستندات المطلوبة. البريد الإلكتروني لحامل البطاقة أو الخطاب أو الرسالة أو مجموعة مطالبات حامل البطاقة بنموذج النزاع المكتمل التي تصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع ووصف محدد بشكل معقول للسلع / الخدمات المشتراة. هذا يعني أن البريد الإلكتروني أو الخطاب أو الرسالة لحامل البطاقة يجب أن يوثق كيفية استيفاء كل نقطة من شروط

document how each point of the Chargeback Creation Conditions was met.

Required Comment. None

Notes. This chargeback is limited to purchase Transactions.

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove the Transaction was successfully completed and the Cardholder received the goods or services.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents.

For contactless Transactions equal to or less than the 300 LYD CVM threshold: The Transaction receipt for the disputed Transaction. For face-to-face Transactions greater than the 300 LYD CVM threshold: The Transaction receipt with valid CVM (Online PIN or Signature) for the disputed Transaction.

For non-face-to-face Transactions: Any relevant documents to support the Acquirer's claim. Examples include, but are not limited to: a signed delivery receipt or any correspondence between the Merchant and the Cardholder confirming receipt of the goods or services.

Required Comment. None

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

إنشاء رد المبالغ المدفوعة.

التعليق المطلوب. لا يوجد.

ملاحظات: يقتصر رد المبالغ المدفوعة هذا على معاملات الشراء.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

RSN01 - المستندات المرفقة وسبل المعالجة

RSN02 - ائتمان تم إصداره مسبقًا

RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.

RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.

RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.

RSN07 - تكرار رد المبالغ المدفوعة.

RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شرط رفض رد المبالغ المدفوعة. يمكن للقابل إثبات اكتمال المعاملة بنجاح وتسلم حامل البطاقة البضائع أو الخدمات.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة.

للمعاملات التي تتم عن بعد والتي تساوي أو تقل عن 300 دينار من عتبة CVM: إيصال المعاملة المتنازع عليها.

بالنسبة للمعاملات التي تتم وجهاً لوجه والتي تزيد عن 300 دينار من عتبة CVM: إيصال المعاملة مع CVM (رقم التعريف الشخصي عبر الإنترنت أو التوقيع) للمعاملة المتنازع عليها

للمعاملات غير المباشرة: أي مستندات ذات صلة لإثبات ادعاء القابل، على سبيل المثال، إيصال تسليم موقع، أو أي مراسلات بين التاجر وحامل البطاقة تؤكد استلام البضائع أو الخدمات. التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد.

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويته والرقم المرجعي الفريد لمقاصة الاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. لم تف جهة الإصدار بشروط رد المبالغ المدفوعة ، أو كانت بيانات رد المبالغ المدفوعة كانت غير صحيحة، أو أن حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم. الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد. التعليق المطلوب. الشرط الذي لم تستوفه جهة الإصدار.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition. The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code: RSN05-Chargeback documents were not received)

Chargeback Rejection Condition. The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.2.8 Credit Posted as a Purchase

Reason Code. CBCD04

Chargeback Creation Condition.

The Cardholder contacted the Issuer claiming that the Cardholder account has been inaccurately posted with a debit instead of a credit.

Time Frame. Within 120 business days of the Transaction processing date.

Required Documents. A Cardholder letter, email, message, or completed Dispute Form-Cardholder Claims Group describing the Cardholder's complaint in sufficient detail to enable all parties to understand the dispute and a refund receipt or other written documentation proving the Cardholder was due a refund.

Required Comment. None

Notes. In order to ensure the Cardholder receives all of the monies due, the Issuer must either:

1. Perform a Credit Posted as a Purchase chargeback for up to twice the original Transaction amount (for the original Transaction that was not refunded and for the credit posted as a purchase).
2. Perform a separate chargeback for Credit Not Processed

رمز السبب. RSN04 - أن تكون مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة/ غير كاملة.

شرط رفض رد المبالغ المدفوعة. إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة أو غير مرتبطة بمطالبة رد المبالغ المدفوعة، أو غير مكتملة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN05 لم يتم استلام مستندات رد المبالغ المدفوعة.

شرط رفض رد المبالغ المدفوعة. لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN07- إعادة تحميل المبالغ المكررة

شرط رفض رد المبالغ المدفوعة: تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08- رد المبالغ المدفوعة خارج الإطار الزمني.

شرط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

8.2.2.2. الائتمان منشور على أنه شراء

رمز السبب. CBCD04

شرط إنشاء رد المبالغ المدفوعة: أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مدعيًا أن حسابه قد تم ترحيله بشكل غير دقيق مع الخصم بدلاً من الائتمان.

الإطار الزمني. في غضون 120 يوم عمل من تاريخ تسوية المعاملة.

المستندات المطلوبة: خطاب حامل البطاقة أو رسالة بريد إلكتروني أو رسالة أو مجموعة مطالبات حامل البطاقة بنموذج نزاع كامل تصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع وإيصال استرداد أو مستندات مكتوبة أخرى تثبت أن حامل البطاقة كان مستحقًا استرداد الأموال.

التعليق المطلوب. لا يوجد.

ملاحظات: لضمان حصول حامل البطاقة على جميع الأموال المستحقة، يجب على جهة الإصدار إما:

1. القيام بتنفيذ ائتمان يتم نشره على أنه استرداد لمبلغ مصاريف الشراء عندما يصل إلى ضعف مبلغ المعاملة الأصلية (للمعاملة الأصلية التي لم يتم ردها وللائتمان الذي تم ترحيله كعملية شراء).
2. القيام بتنفيذ عملية منفصلة لرد المبالغ المدفوعة للائتمان الذي لم تتم معالجته

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove the disputed Transaction was never intended as a credit.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. Any relevant documents to support the Acquirer's claim. For example, the Transaction receipt.

Required Comment. None

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition: The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقًا
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شروط رفض رد المبالغ المدفوعة. إثبات للقابل أن المعاملة المتنازع عليها لم تكن مقصودة على الإطلاق كرسيد.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.

المستندات المطلوبة. أي مستندات ذات صلة لإثبات ادعاء القابل. على سبيل المثال ، إيصال المعاملة. التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شروط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويته والرقم المرجعي الفريد لمقاصة الاسترداد

رمز السبب.-RSN03 رد المبالغ المدفوعة غير صالح:

شروط رفض رد المبالغ المدفوعة. لم تفي جهة الإصدار بشروط رد المبالغ المدفوعة ، أو كانت بيانات رد المبالغ المدفوعة كانت غير صحيحة، أو أن حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد.

التعليق المطلوب. الشرط الذي لم تستوفيه جهة الإصدار.

رمز السبب. RSN04 – إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة

شروط رفض رد المبالغ المدفوعة: إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة، أو غير مكتملة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

Reason Code: RSN05-Chargeback documents were not received)

Chargeback Rejection Condition: The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.3 Fraud Dispute Group

This dispute type may be used by the Issuer when the Cardholder contacted the issuer claiming that a fraudulent Transaction occurred on the Cardholder’s Card for one of the following reasons:

- No Customer Authorization
- Chip Processing Rule
- Multiple Fraudulent Transactions

2.2.3.1 No Cardholder Authorization

Reason Code: CBCD13

Chargeback Creation Condition. The Cardholder contacted the Issuer claiming that the Cardholder did not authorize the non-face-to-face Transaction.

Before processing a No Cardholder Authorization chargeback, the Issuer must block the account on its host or for Transactions involving a token, the Issuer must deactivate the token.

This chargeback is not available for the following Transactions:

- Face-to-face Transactions
- ATM Transactions
- Transactions in which PIN was the CVM
- National Scheme Operator ACS Transactions
- Transactions in which a non-Chip Card was used at a chip-capable vending machine
- Transactions in which a Chip Card without PIN capability was used at a chip and PIN capable vending machine

رمز السبب. RSN05: لم يتم استلام مستندات رد المبالغ المدفوعة.

شُروط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN07- إعادة تحميل المبالغ المكررة

شُروط رفض رد المبالغ المدفوعة: تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08- رد المبالغ المدفوعة خارج الإطار الزمني.

شُروط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

3.2.2. مجموعة منازعات الاحتيال

يمكن استخدام هذا النوع من المنازعات من قبل جهة الإصدار، عندما يقوم حامل البطاقة بالتواصل مع جهة الإصدار مدعيًا حدوث عملية احتيالية على بطاقته وفقاً لأحد الأسباب التالية:

- لا يوجد تفويض بذلك من العميل.
- قاعدة معالجة الشريحة.
- المعاملات الاحتيالية المتعددة.

1.3.2.2. لا يوجد تصريح من حامل البطاقة

رمز السبب: CBCD13

شُروط إنشاء رد المبالغ المدفوعة. أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار، مدعيًا أنه لم يصرح بالمعاملة غير المباشرة.

يجب على جهة الصادر، قبل معالجة رد المبالغ المدفوعة بموجب “عدم تفويض حامل البطاقة”، أن يقوم بحظر الحساب على مضيفه، أما بالنسبة للمعاملات التي تتضمن رمزًا مميزًا، فإنه يجب على جهة الإصدار إلغاء تنشيط الرمز المميز.

رد المبالغ المدفوعة غير متاح للمعاملات التالية:

- المعاملات التي تتم وجها لوجه.
- معاملات أجهزة الصراف الآلي.
- المعاملات التي كان رقم التعريف الشخصي هو CVM
- معاملات ACS لمشغل شبكة الدفع المحلية.
- المعاملات التي تم فيها استخدام بطاقة غير مزودة بشريحة في آلة بيع قادرة على الشريحة.
- المعاملات التي تم فيها استخدام بطاقة شريحة بدون رقم تعريف شخصي في آلة بيع قادرة على الشريحة ورقم التعريف الشخصي.

- Subsequent Transaction dispute (rather a subsequent Transaction dispute must be processed as detailed in the Cardholder Claim Group section)
- Transactions resulting from an account takeover. An account takeover occurs when an existing credit or debit account is used without the actual, implied, or apparent authority of the Cardholder, by a person who gains access to and use of the account through an unauthorized means, such as a change of address or request for re-issuance of credit or debit Cards (or other device for accessing a credit or debit account) but not lost or stolen Cards.

Time Frame. 120 calendar days

Required Documents. One of the following:

- Cardholder email, letter, message, or completed Dispute Form-Fraud stating that the Cardholder did not authorize the Transaction.
- Written complaint from a company or government agency representative on behalf of a corporate Card Cardholder when the company or government agency no longer employs the authorized Cardholder.

Required Comment. None

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove the Cardholder authorized the disputed Transaction.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents.

For airline Transactions: At least one of the following documents and, when necessary, an explanation:

- Flight ticket or boarding pass showing the passenger's name.
- Flight manifest showing the passenger's name.
- Additional Transactions connected with the disputed flight, such as upgrades, excess baggage charges, and in-flight purchases.
- Passenger identification documentation showing a link to the Cardholder.
- Credits of frequent flyer miles for the flight, showing connection to the Cardholder.
- Proof of receipt of the flight ticket at the Cardholder's billing address.

- نزاع المعاملات اللاحقة (بدلاً من ذلك يجب معالجة نزاع المعاملات اللاحقة كما هو مفصل في قسم مجموعة مطالبات حامل البطاقة)
 - المعاملات الناتجة عن الاستيلاء على الحساب. تحدث عملية الاستحواذ على الحساب عندما يتم استخدام حساب ائتمان، أو حساب مدين قائم بدون السلطة الفعلية أو الضمنية أو الواضحة لحامل البطاقة، من قبل شخص يمكنه الوصول إلى الحساب واستخدامه من خلال وسائل غير مصرح بها ، مثل تغيير العنوان أو طلب إعادة إصدار بطاقات الائتمان أو الخصم (أو أي جهاز آخر للوصول إلى حساب ائتمان أو مدين) وليس في حالات فقدان أو سرقة البطاقات.
- الإطار الزمني. في غضون 120 يومًا تقويمياً

المستندات المطلوبة: واحدة من التالية:

- البريد الإلكتروني لحامل البطاقة أو الخطاب أو الرسالة أو نموذج نزاع - احتيال مكتمل يوضح أن حامل البطاقة لم يصرح بالمعاملة.
 - شكوى خطية من شركة أو ممثل وكالة حكومية نيابة عن حامل بطاقة الشركة عندما لا تقوم الشركة أو الوكالة الحكومية بتوظيف حامل البطاقة المفوض.
- التعليق المطلوب. لا يوجد.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقاً
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروعة / غير ذات صلة / غير كاملة.
- RSN05 - لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شرط رفض رد المبالغ المدفوعة. يمكن للقابل إثبات أن حامل البطاقة قد سمح بإجراء بالمعاملة المتنازع عليها.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة:

بالنسبة لمعاملات شركات الطيران: يجب تقديم واحدة من المستندات التالية، وعند الضرورة، شرح:

- تذكرة طيران، أو بطاقة صعود تبين اسم الراكب.
- بيان الرحلة موضح به اسم الراكب.
- المعاملات الإضافية المرتبطة بالرحلة المتنازع عليها، مثل الترقية ورسوم الأمتعة الزائدة والمشتريات على متن الطائرة.
- وثائق هوية المسافرين تظهر ارتباطاً بحامل البطاقة.
- أرصدة أميال المسافرين الدائم للرحلة، تبين الاتصال بحامل البطاقة.
- إثبات استلام تذكرة الطيران على عنوان إرسال الفواتير لحامل البطاقة.

For Recurring Transactions: All of the following:

- A description of the goods or services being provided.
- The start date of the original recurring Transaction.
- State if National Scheme Operator ACS was used in the original Transaction:
- One of the following:
 - The Transaction was properly identified in both authorization and clearing as a recurring Transaction.
 - Documentation proving that the Transaction was recurring. Examples include but are not limited to: The Merchant providing proof that the Cardholder had to click to accept the recurring terms and conditions or the Cardholder signed a contract agreeing to the recurring terms and conditions.

For “No-Show” Transactions: All of the following:

- The primary account number (PAN).
- The Cardholder’s name present on the Card.
- The confirmation number provided at the time the reservation was made.

For Completed Transaction: All of the following:

- All documentation proving the Cardholder’s participation in the original request
- The Unique Reference Number and date
- The pre-authorization was processed as a Chip or magnetic stripe Transaction
- This is a valid remedy to this reason code and Issuer is prohibited from continuing the dispute.

For Account Takeover Transactions: The Acquirer can provide evidence that the Transaction resulted from an account takeover. Documentation proving the Transaction resulted from an account takeover. Examples include, but are not limited to a statement from the Cardholder confirming that the account was in fact taken over and that fraud subsequently occurred.

For all other Transactions: At least one of the following documents and, when necessary, an explanation:

- A receipt, work order, or other document signed by the Cardholder substantiating that the goods or services were received by the Cardholder (commonly referred to as “will call” and “in-store pickup”)
- The Cardholder’s written confirmation of registration to receive electronic delivery of goods or services
- Copies of written correspondence exchanged between the Merchant and the Cardholder (such as letter, email, or fax) showing that the Cardholder participated in the Transaction.
- A Merchant statement documenting all of the following when, after completing an authenticated e-commerce Transaction, the Merchant obtained authorization for a related Transaction involving a partial shipment or the payment of a balance due:
 - The initial Transaction was a National Scheme Operator ACS Transaction
 - Description of the goods or services purchased in the initial Transaction;
 - Date and authorization number for the initial Transaction; and
 - The initial Transaction was not disputed.
- When a Merchant requires a Cardholder to register prior to completing a purchase, the

بالنسبة للمعاملات المتكررة: كل مما يلي:

- القيام بوصف السلع أو الخدمات المقدمة.
- تاريخ بدء المعاملة المتكررة الأصلية.
- تحديد ما إذا تم استخدام ACS لمشغل شبكة الدفع المحلية في المعاملة الأصلية:
- واحدة من التالية:
 - تم تحديد وصف المعاملة بشكل صحيح في كل من التفويض والمقاصة، باعتبارها معاملة متكررة.
 - المستندات التي تثبت أن المعاملة كانت متكررة. على سبيل المثال: تقديم التاجر دليلًا على أن حامل البطاقة اضطر إلى النقر لقبول الشروط والأحكام المتكررة أو أن حامل البطاقة وقع عقدًا بموافقة على الشروط والأحكام المتكررة.

بالنسبة إلى معاملات “عدم الحضور”: كل مما يلي:

- رقم الحساب الأساسي (PAN).
- اسم حامل البطاقة موجود على البطاقة.
- رقم التأكيد المقدم في وقت إجراء الحجز.

بالنسبة للمعاملة المكتملة: كل مما يلي:

- جميع المستندات التي تثبت مشاركة حامل البطاقة في الطلب الأصلي.
- الرقم المرجعي الفريد، والتاريخ.
- ما يفيد أنه قد تمت معالجة التفويض المسبق كمعاملة شريحة، أو معاملة شريط مغناطيسي.
- تعد هذه معالجة صحيحة لرمز السبب، ويحظر على جهة الإصدار مواصلة النزاع.

بالنسبة لمعاملات الاستحواذ على الحساب: يمكن للقابل لتقديم دليل على أن المعاملة كانت نتيجة الاستيلاء على الحساب. المستندات التي تثبت أن المعاملة كانت نتيجة الاستيلاء على الحساب، على سبيل المثال، بيانًا من حامل البطاقة يؤكد أن الحساب قد تم الاستيلاء عليه بالفعل، وأن واقعة الاحتيال قد حدثت لاحقًا.

بالنسبة لجميع المعاملات الأخرى: واحدة على الأقل من المستندات التالية: ، وعند الضرورة ، شرح:

- إيصال المعاملة، أو أمر عمل أو مستند آخر موقع من قبل حامل البطاقة يثبت أن حامل البطاقة قد استلم السلع أو الخدمات (يشار إليها عمومًا باسم “سوف يتصل” و “الاستلام من المتجر”)
- تأكيد كتابي من حامل البطاقة بالتسجيل، لتلقي التسليم الإلكتروني للسلع أو الخدمات.
- نسخ من المراسلات المكتوبة، والمتبادلة بين التاجر وحامل البطاقة (مثل الخطاب أو البريد الإلكتروني أو الفاكس) والتي توضح أن حامل البطاقة قد شارك في المعاملة.
- بيان من التاجر يوثق كل ما يلي عندما يحصل التاجر، بعد إتمام معاملة تجارة الالكترونية المصدق عليها، على تفويض لمعاملة ذات صلة تتضمن شحنة جزئية أو سداد رصيد مستحق:
 - إذا كانت المعاملة الأولية عبارة عن معاملة ACS لمشغل شبكة الدفع المحلية.
 - وصف السلع أو الخدمات المشتراه في المعاملة الأولية.
 - تاريخ ورقم التفويض للمعاملة الأولية.
 - لم يتم التنازع على المعاملة الأولية.
- عندما يطلب التاجر من حامل البطاقة التسجيل قبل إتمام عملية الشراء، يجب على التاجر تقديم

- Merchant must provide documentation confirming the Cardholder or authorized user is registered to purchase goods with a password and must provide one or more of the following documentations:
- The Cardholder or authorized user completed other undisputed purchases prior to, or after, the alleged fraudulent Transaction
 - The Cardholder or authorized user completed the disputed Transaction from a registered device and IP address
 - Details of the purchase
 - Signed proof of delivery
 - Email addresses to support digital download delivery
 - The Cardholder or authorized user registered the disputed goods or services. For example, registration for purposes of warranty or future software updates.
 - The disputed goods or services were used
 - A National Scheme Operator ACS Transaction was used to register a PAN for future Transactions

Required Comment. None

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card Time Frame. Within 20 business days of the processing date of the chargeback. Required Documents. None Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records. Time Frame. Within 20 business days of the processing date of the chargeback. Required Documents. None Required Comment. The condition the Issuer did not meet.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition: The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete. Time Frame. Within 20 business days of the processing date of the chargeback. Required Documents. None Required Comment. None

Reason Code: RSN05-Chargeback documents were not received

Chargeback Rejection Condition: The Required Documents required for this chargeback were not received. Time Frame. Within 20 business days of the processing date of the chargeback. Required Documents. None Required Comment. None

- المستندات التي تؤكد أن حامل البطاقة أو المستخدم المصرح له، مسجل لشراء البضائع بكلمة مرور، ويجب أن يقدم واحدًا أو أكثر من المستندات التالية:
- تنفيذ حامل البطاقة أو المستخدم المرخص له معاملات (مشتريات) أخرى غير متنازع عليها قبل أو بعد المعاملة الاحتيالية المزعومة .
 - تنفيذ حامل البطاقة أو المستخدم المصرح له المعاملة المتنازع عليها من جهاز مسجل وعنوان IP.
 - تفاصيل الشراء.
 - إثبات تسليم موقع.
 - عناوين البريد الإلكتروني لدعم تسليم التنزيل الرقمي.
 - قيام حامل البطاقة أو المستخدم المصرح له بتسجيل السلع أو الخدمات المتنازع عليها. على سبيل المثال ، التسجيل لأغراض الضمان أو تحديثات البرامج المستقبلية.
 - استخدام السلع أو الخدمات المتنازع عليها.
 - تم استخدام معاملة ACS لمشغل شبكة الدفع المحلية لتسجيل رقم الحساب الأساسي للمعاملات المستقبلية.
- التعليق المطلوب. لا يوجد.

رمز السبب. RSN02- ائتمان تم إصداره مسبقًا
شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد.
التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويته والرقم المرجعي الفريد لمقاصة الاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:
شرط رفض رد المبالغ المدفوعة. لم تفي جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد المبالغ المدفوعة غير صحيحة، أو كان حقل رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم. الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد.
التعليق المطلوب. الشرط الذي لم تستوفيه جهة الإصدار.

رمز السبب. RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة/ غير كاملة.
شرط رفض رد المبالغ المدفوعة: إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة ، أو غير مكتملة. الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

رمز السبب. RSN05: لم يتم استلام مستندات رد المبالغ المدفوعة.
شرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة. الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة. المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time. Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.3.2 Chip Processing Rules

Reason Code. CBCD21

Chargeback Creation Condition. One of the following Conditions:

Condition 1: Counterfeit Card. All of the following:

- The Cardholder contacted the Issuer claiming that the Cardholder did not authorize the Transaction.
- The disputed Transaction occurred with a counterfeit card at a Terminal (ATM or POS) that was not chip capable
- The validly issued Card was a Chip Card.

Condition 2: Lost/Stolen Card. All of the following:

- The Cardholder contacted the Issuer claiming that the Cardholder did not authorize the Transaction.
- The disputed Transaction occurred with a lost/stolen Card at a Hybrid Terminal (ATM or POS) that was PIN capable.
- The validly issued Card was a Chip Card with PIN capability.

In addition:

For both Condition 1 and 2: before processing a Chip Processing Rules chargeback, the Issuer must block the account on its host or for Transactions involving a Token, the Issuer must deactivate the Token.

This chargeback is not available for the following Transactions:

- Contactless chip Transactions
- Transactions in which technical fallback occurred. A technical fall Transaction occurs when both the Card or Terminal are chip-capable but for an unknown reason the Transaction was processed using either the magnetic stripe or key-entry.
- Transactions in which the service code indicated the Card is not chip capable
- Transactions resulting from an account takeover. An account takeover occurs when an existing credit or debit account is used without the actual, implied, or apparent authority of the Cardholder, by a person who gains access to and use of the account through an unauthorized means, such as a change of address or request for re-issuance of credit or debit Cards (or other device for accessing a credit or debit account) but not lost or stolen Cards.

رمز السبب. RSN07 إعادة تحميل المبالغ المكررة

شُروط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08 رد المبالغ المدفوعة خارج الإطار الزمني.

شُروط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار الزمني

لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

2.3.2.2 قواعد معالجة الشريحة

رمز السبب. CBCD21

شُروط إنشاء رد المبالغ المدفوعة. أحد الشروط التالية:

الشُروط 1: إذا كانت البطاقة المزورة. كل ما يلي:

- أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مدعيًا أنه لم يصرح بالمعاملة.
- إذا تمت المعاملة المتنازع عليها باستخدام بطاقة مزورة في المحطة (ماكينة الصراف الآلي أو نقاط البيع) لم تكن قادرة على الشريحة.
- إذا كانت البطاقة الصادرة بشكل صحيح بطاقة شريحة.
- الشُروط 2: إذا كانت البطاقة ضائعة أو مسروقة. كل ما يلي:
- أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مدعيًا أنه لم يصرح بالمعاملة.
- إذا تمت المعاملة المتنازع عليها ببطاقة ضائعة أو مسروقة في محطة هجينة (ماكينة الصراف الآلي أو نقاط البيع) كان بإمكانها PIN.
- إذا كانت البطاقة الصادرة بشكل صحيح عبارة عن بطاقة شريحة مزودة بإمكانية رقم التعريف الشخصي. فضلًا عن ذلك:

- بالنسبة لهذين الشرطين: فإنه يجب على جهة الإصدار، قبل معالجة رد المبالغ المدفوعة لقواعد معالجة الشريحة، أن تقوم بحظر الحساب على مضيئه أو للمعاملات التي تتضمن رمزًا، كما يجب عليها إلغاء تنشيط الرمز المميز.
- رد المبالغ المدفوعة غير متاح للمعاملات التالية:
- معاملات الشرائح التي تنفذ عن بعد (غير المتصلة).
- المعاملات التي حدث فيها احتياطي فني. وتحدث معاملة السقوط الفني عندما يكون كل من البطاقة أو الجهاز قادرين على قراءة الشريحة، ولكن لسبب غير معروف تمت معالجة المعاملة باستخدام إما الشريط المغناطيسي أو إدخال المفتاح.
- المعاملات التي يشير فيها رمز الخدمة إلى أن البطاقة غير قادرة على قراءة الشريحة.
- المعاملات الناتجة عن الاستحواذ على الحساب.

وتحدث عملية الاستحواذ على الحساب عندما يتم استخدام حساب ائتمان أو مدين قائم بدون وكالة من حامل البطاقة، من قبل شخص يمكنه الوصول إلى الحساب واستخدامه من خلال وسائل غير مصرح بها، مثل تغيير العنوان أو طلب إعادة إصدار بطاقات الائتمان أو الخصم (أو أي جهاز آخر للوصول إلى حساب ائتمان أو مدين) ولكن لا يتم ضياع أو سرقة البطاقات.

Time Frame. 120 calendar days

Required Documents. One of the following Conditions corresponding to the Chargeback Rejection Condition in this same subsection:

Condition 1: Counterfeit Card

Cardholder email, letter, message, or completed Dispute Form-Fraud stating:

- The Cardholder did not authorize the Transaction.
- The Cardholder is still in possession of the validly issued Card

Condition 2: Lost/Stolen Card

Cardholder email, letter, message, or completed Dispute Form-Fraud stating:

- The Cardholder did not authorize the Transaction.
- The Card was lost/stolen before the date of the disputed Transaction

Required Comments. None

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. One of the following:

- For a contactless Transaction: authorized contactless transaction.
- For all other Transactions: The condition the Issuer did not meet.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition. The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

الإطار الزمني. في غضون 120 يومًا تقويمياً

المستندات المطلوبة: أحد الشروط التالية المقابلة لشروط رفض رد المبالغ المدفوعة في هذا القسم الفرعي نفسه:

الشروط 1: البطاقة المزورة.

البريد الإلكتروني لحامل البطاقة أو الخطاب أو الرسالة أو نموذج نزاع - احتيال مكتمل ينص على ما يلي:

- لم يصرح حامل البطاقة بالمعاملة.
- لا تزال صلاحية البطاقة التي في حيازة الحامل سارية المفعول.

الشروط 2: البطاقة الضائعة أو المسروقة

البريد الإلكتروني لحامل البطاقة أو الخطاب أو الرسالة أو نموذج نزاع - احتيال مكتمل ينص على ما يلي:

- أن حامل البطاقة لم يصرح بإجراء المعاملة.
- أن تكون البطاقة قد ضاعت أو سرقت قبل تاريخ المعاملة المتنازع عليها.

التعليقات المطلوبة: لا توجد.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل الانتصاف
- RSN02 - ائتمان تم إصداره مسبقًا
- RSN03 - رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. RSN02- ائتمان تم إصداره مسبقًا

شروط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويته والرقم المرجعي الفريد لمقاصة الاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شروط رفض رد المبالغ المدفوعة. لم تفي جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد

المبالغ المدفوعة غير صحيحة، أو كان حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في

رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. واحدة من التالية:

- بالنسبة لمعاملة بدون تلامس: معاملة مصرح بها بدون اتصال.
- بالنسبة لجميع المعاملات الأخرى: الشرط الذي لم تستوفيه جهة الإصدار.

رمز السبب. RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.

شروط رفض رد المبالغ المدفوعة: إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة،

أو غير مرتبطة بمطالبة رد المبالغ المدفوعة ، أو غير مكتملة.

Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None
Reason Code: RSN05-Chargeback documents were not received)
Chargeback Rejection Condition. The Required Documents required for this chargeback were not received.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

Reason Code. RSN07-Duplicate Chargeback
Chargeback Rejection Condition. The same Transaction was disputed more than one time.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comments. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame
Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

2.2.3.3 Multiple Fraudulent Transactions

Reason Code: CBCD24
Chargeback Creation Condition. The Cardholder contacted the Issuer claiming all of the following:

- The Cardholder was still in possession and control of all valid Cards at the time of the Transaction(s)
- The Cardholder admits to at least one legitimate face-to-face Transaction
- The Cardholder denies making one or more additional face-to-face Transactions at that same Merchant location

In addition:

- Before processing a Multiple Fraudulent Transactions chargeback, the Issuer must block the Account on its host
- The Transaction(s) being denied by the Cardholder should have occurred either within 15 minutes (before or after) of the legitimate face-to-face Transaction.
- This chargeback is not permitted when PIN was the CVM for the disputed Transaction(s)

Time Frame. 120 calendar days
Required Documents. Cardholder email, letter, message, or completed Dispute Form-Fraud form stating all of the following:

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

رمز السبب. RSN05: إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
شرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا توجد.

رمز السبب. RSN07- إعادة تحميل المبالغ المكررة
شرط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08- رد المبالغ المدفوعة خارج الإطار الزمني.
شرط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار الزمني لرمز سبب رد المبالغ المدفوعة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

3.3.2.2 معاملات احتيالية متعددة:

رمز السبب. CBCD24
شرط إنشاء رد المبالغ المدفوعة: أن يقوم الحامل البطاقة بالتواصل مع جهة الإصدار طالباً بكل ما يلي:

- أن حامل البطاقة مازال يمتلك ويتحكم في جميع البطاقات الصالحة وقت إجراء المعاملة (المعاملات).
- أن يوافق حامل البطاقة على معاملة مشروعة واحدة على الأقل وجهًا لوجه.
- أن يرفض حامل البطاقة إجراء معاملة إضافية أو أكثر وجهًا لوجه في نفس موقع التاجر.

فضلاً عن ذلك:

- قبل معالجة عمليات رد المبالغ المدفوعة على المعاملات الاحتيالية متعددة، يجب على جهة الإصدار حظر الحساب على مضيفه
- يجب أن تتم المعاملة (المعاملات) التي تم رفضها من قبل حامل البطاقة خلال 15 دقيقة (قبل أو بعد) المعاملة الشرعية وجهًا لوجه.
- لا يجوز رد المبالغ المدفوعة إذا كان رقم التعريف الشخصي هو رمز التحقق من البطاقة (CVM) للمعاملة أو المعاملات المتنازع عليها.

الإطار الزمني. في غضون 120 يومًا تقويمياً
المستندات المطلوبة. البريد الإلكتروني لحامل البطاقة، أو الخطاب، أو الرسالة، أو نموذج نزاع-احتيال مكتمل يوضح كل ما يلي:

- The Cardholder was still in possession and control of all valid Cards at the time of the Transaction
- The Cardholder admits to at least one legitimate face-to-face Transaction
- The Cardholder denies making one or more additional face-to-face Transactions at that same Merchant location

Required Comment. The Unique Clearing Reference Number of the valid Transaction.

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01- Attached Documents and Remedy

Chargeback Rejection Condition. Acquirer can prove that both Transactions were valid.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. Valid receipts documenting two separate Transactions.

Required Comment. None

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number (DE 57) of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code: RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition. The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

- أن حامل البطاقة لا يزال يمتلك ويتحكم في جميع البطاقات الصالحة وقت إجراء المعاملة.
 - أن يوافق حامل البطاقة على معاملة شرعية واحدة على الأقل وجهًا لوجه.
 - أن يرفض حامل البطاقة إجراء معاملة إضافية أو أكثر وجهًا لوجه في نفس موقع التاجر.
- التعليق المطلوب. الرقم المرجعي الفريد للمقاصة للمعاملة الصالحة.

شروط رفض رد المبالغ المدفوعة:

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقًا
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. RSN01 المستندات المرفقة وسبل المعالجة

شرط رفض رد المبالغ المدفوعة: أن يقوم القابل بإثبات أن كلا المعاملتين كانتا صالحتين.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. إيصالات صحيحة توثق عمليتين منفصلتين.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN02 ائتمان تم إصداره مسبقًا

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويتها والرقم المرجعي الفريد لمقاصة (DE 57) الاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. لم تف جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد المبالغ المدفوعة غير صحيحة، أو كان حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. الشرط الذي لم تستوفه جهة الإصدار.

رمز السبب. RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.

شرط رفض رد المبالغ المدفوعة: إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة ، أو غير مكتملة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

Reason Code: RSN05-Chargeback documents were not received

Chargeback Rejection Condition. The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.4 Point of Interaction Error

This section provides information for handling a Point-of-Interaction Error chargeback.

A Point-of-Interaction Error chargeback may be submitted when the Cardholder contacted the Issuer alleging one of the following:

- Some or all of the funds debited from the Cardholder’s account as the result of an ATM withdrawal were not dispensed
- The Cardholder’s account has been debited more than once for the same Transaction using the same form of payment.
- The Cardholder paid twice for the same Transaction using two different forms of payment.
- The Cardholder was billed an incorrect amount.
- The Acquirer presented a Transaction past the applicable time frame.
- Funds deposited through an ATM Transaction did not affect the Card balance
- Funds deposited through a POS Transaction did not affect the Card balance
- Funds deposited through an instant credit Transaction (ICT) did not affect the Card balance

2.2.4.1 Cash Not Received

Reason Code. CBCD10 Cash not received

Creation Condition. The Cardholder contacted the Issuer claiming that some or all of the funds debited from the Cardholder’s account as the result of an ATM withdrawal were not dispensed.

Time Frame. 120 calendar days of the Transaction processing date.

Required Documents. None

Required Comment. None

رمز السبب. RSN05: إذا لم يتم استلام مستندات رد المبالغ المدفوعة.

شُروط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN07 إعادة تحميل المبالغ المكررة

شُروط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08 رد المبالغ المدفوعة خارج الإطار الزمني.

شُروط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار

الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

4.2.2 خطأ نقطة التفعيل (التفاعل):

يوفر هذا القسم معلومات للتعامل مع رد المبالغ المدفوعة عند حدوث خطأ نقطة التفاعل.

قد تُجرى عملية رد المبالغ المدفوعة عند نقطة التفعيل، عندما يتصل حامل البطاقة بجهة الإصدار مدعيًا أحد الإجراءات التالية:

- أنه لم يتم الاستغناء عن بعض أو كل الأموال المخصومة من حساب حامل البطاقة نتيجة لسحب أجهزة الصراف الآلي.
- أنه تم الخصم من حساب حامل البطاقة أكثر من مرة، لنفس المعاملة، باستخدام نفس طريقة الدفع.
- أن حامل البطاقة قد قام بالدفع مرتين لنفس المعاملة، وباستخدام طريقتين مختلفتين.
- أنه تم إصدار فاتورة لحامل البطاقة بمبلغ غير صحيح.
- أن القابل قد قام بالمعاملة خارج الإطار الزمني.
- أن الأموال المودعة من خلال معاملة الصراف الآلي لم تؤثر على رصيد البطاقة.
- أن الأموال المودعة من خلال معاملة نقاط البيع لم تؤثر على رصيد البطاقة.
- أن الأموال المودعة من خلال معاملة أئتمانية فورية (ICT) لم تؤثر على رصيد البطاقة.

1.4.2.2 لم يتم قبض النقود:

رمز السبب. CBCD10 النقود لم يتم قبضها.

شُروط الإنشاء. أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مدعيًا أنه لم يتم الاستغناء عن بعض،

أو كل الأموال المخصومة من حسابه نتيجة لعملية السحب من جهاز الصراف الآلي.

الإطار الزمني. في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

Notes:

This chargeback is not available for claims of fraud.

The Issuer may chargeback only the amount which the Cardholder claims was not dispensed by the ATM.

An Issuer must not use this reason code if the Acquirer refunded the disputed amount to the card through the Surplus Option.

If the Acquirer issued a partial surplus to a Card, the Issuer may charge back only the non-credited disputed amount.

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove that the funds were properly dispensed by the ATM.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. The Merchant's explanation and documentation proving the Cardholder was billed the correct amount.

The required documentation must come from the ATM journal and, at minimum, must include:

- Account accessed
- ATM number
- Account PAN read from Track 2 of the magnetic stripe or from the chip
- The ATM financial activity showing that funds were properly dispensed with any error before and after the disputed Transaction.
- Transaction amount
- Transaction date and time
- Transaction trace
- Transaction type

In addition to the required documentation, the Acquirer may provide a Transaction report. When necessary, an explanation describing each element of the journal and/or report.

Required Comment. None.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

ملاحظات:

رد المبالغ المدفوعة غير ممكن لمطالبات الاحتيال.

يجوز لجهة الإصدار استرداد المبلغ الذي يدعي حامل البطاقة أنه لم يتم الاستغناء عنه بواسطة جهاز الصراف الآلي.

يجب ألا تستخدم جهة الإصدار رمز السبب، إذا قام القابل برد المبلغ المتنازع عليه إلى حساب حامل البطاقة من خلال فائض الحساب.

إذا منح القابل فائضًا جزئيًا على البطاقة ، فلا يجوز لمصدر البطاقة سوى استرداد المبالغ غير المدينة.

شروط رفض رد المبالغ المدفوعة:

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقًا
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شروط رفض رد المبالغ المدفوعة: يجوز للجهة القابلة إثبات أن الأموال قد تم صرفها بطريقة صحيحة عن طريق أجهزة الصراف الآلي.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة: أن يقوم التاجر بتقديم أدلة الإثبات التي تثبت أن حامل البطاقة قد تمت فوترته بالمبلغ الصحيح.

يجب أن تكون المستندات صادرة عن مجلة جهاز الصراف الآلي، ويجب أن تتضمن في حدها الأدنى على أحد المستندات التالية:

- الوصول إلى الحساب.
- رقم جهاز الصراف الآلي.
- قراءة رقم الحساب الأساسي للحساب من المسار 2 للشريط المغناطيسي أو من الشريحة.
- أن يظهر التسلسل المالي لأجهزة الصراف الآلي أنه تم الاستغناء عن الأموال بطريقة صحيحة، عن أي خطأ قبل أو بعد المعاملة المتنازع عليها.
- القيمة النقدية للتحويل.
- تاريخ وزمن إجراء المعاملة.
- تتبع المعاملات.
- نوع المعاملة.

بالإضافة إلى هذه المستندات، يجوز للقابل، عند الضرورة، أن يقدم تقريرًا بالمعاملات التي تم إجراؤها، يصف كل عنصر من عناصر المجلة و/ أو التقرير.

التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شروط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code. RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition. The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code: RSN05-Chargeback documents were not received)

Chargeback Rejection Condition. The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.4.2 Paid twice with the same Card

Reason Code. CBCD14 Duplicate amount

Chargeback Creation Condition. The Cardholder contacted the Issuer claiming the Cardholder's account has been debited more than once for the same goods or services.

Time Frame. 120 calendar days of the Transaction processing date.

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويتها والرقم المرجعي الفريد لمقاصة الاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. لم تفي جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد المبالغ المدفوعة غير صحيحة، أو كان حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. الشرط الذي لم تستوفيه جهة الإصدار.

رمز السبب. RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة/ غير كاملة.

شرط رفض رد المبالغ المدفوعة: إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة، أو غير مكتملة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN05: إذا لم يتم استلام مستندات رد المبالغ المدفوعة.

شرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN07- إعادة تحميل المبالغ المكررة

شرط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا شيء.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08- رد المبالغ المدفوعة خارج الإطار الزمني.

شرط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار الزمني

لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

2.4.2.2 تكرار عملية الدفع بنفس البطاقة

رمز السبب. CBCD14 مبلغ مكرر

شرط إنشاء رد المبالغ المدفوعة. أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مدعيًا أن حسابه، قد تم خصمه أكثر من مرة لنفس السلع أو الخدمات.

إطار زمني. 120 يومًا تقويميًا من تاريخ معالجة المعاملة.

Required Documents. A Cardholder letter, email, message, or completed Dispute Form-Point-of-Interaction (POI) Error describing the Cardholder’s complaint in sufficient detail to enable all parties to understand the dispute.

Required Comment. Unique Clearing Reference Number of the valid Transaction

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove that both Transactions were valid. Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. Valid receipts documenting two separate Transactions.

The receipts must clearly establish that the Cardholder was not debited more than once for the same goods or services. A Merchant explanation must be included when the documentation does not clearly establish two separate valid Transactions.

Required Comment. None.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code. RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition. The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comments. None

المستندات المطلوبة. خطاب حامل البطاقة أو بريد إلكتروني أو رسالة أو خطأ مكتمل في نموذج نزاع نقطة تفاعل (POI) يصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع. التعليق المطلوب. الرقم المرجعي الفريد لمقاصة المعاملة الصحيحة.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقًا
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة/ غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شرط رفض رد المبالغ المدفوعة. يجوز للقابل إثبات أن كلا المعاملتين كانتا صحيحتين.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.

المستندات المطلوبة. إيصالات صالحة توثق عمليتين منفصلتين.

إيصالات صحيحة توثق و تثبت بوضوح أن حامل البطاقة لم يتم خصمه أكثر من مرة عن نفس السلع أو الخدمات. ويجب تضمين تفسير التاجر عندما لا تحدد المستندات بوضوح معاملتين صالحتين منفصلتين. التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويتها والرقم المرجعي الفريد لمقاصة الاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. لم تفي جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد المبالغ المدفوعة غير صحيحة، أو كان حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا شيء.

التعليق المطلوب. الشرط الذي لم تستوفيه جهة الإصدار.

رمز السبب. RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة/ غير كاملة.

شرط رفض رد المبالغ المدفوعة: إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة ، أو غير مكتملة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

Reason Code. RSN05-Chargeback documents were not received)

Chargeback Rejection Condition. The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.4.3 Paid by Other Means

Reason Code. CBCD15

Chargeback Creation Condition. The Cardholder contacted the Issuer claiming the Cardholder paid for a Transaction using a National Scheme Operator Card and was subsequently debited for the same Transaction using another form of payment.

Time Frame. 120 calendar days of the Transaction processing date.

Required Documents. A Cardholder letter, email, message, or completed Dispute Form-Point-of-Interaction (POI) Error describing the Cardholder's complaint in sufficient detail to enable all parties to understand the dispute.

The Cardholder letter, email, message, or completed Dispute Form-Point-of-Interaction (POI) Error must specify the alternate means of payment providing sufficient Transaction details to allow the Merchant to locate the alternate payment.

When a non-National Scheme Operator method of payment was used, documentation detailing the specific non-National Scheme Operator method of payment is required. Examples include, but are not limited to:

- A bank statement documenting payment to the Merchant
- A receipt showing cash as the payment method

Required Comment. None

رمز السبب. RSN05: إذا لم يتم استلام مستندات رد المبالغ المدفوعة.

شروط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN07-إعادة تحميل المبالغ المكررة

شروط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08-رد المبالغ المدفوعة خارج الإطار الزمني.

شروط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار

الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

3.4.2.2 الدفع بوسائل أخرى

رمز السبب. CBCD15

شروط إنشاء رد المبالغ المدفوعة: أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مطالباً بأنه قد

دفع مقابل المعاملة باستخدام بطاقة مشغل شبكة الدفع المحلية، وتمت عملية الخصم لاحقاً لنفس

المعاملة، باستخدام طريقة دفع أخرى.

الإطار الزمني. في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة.

المستندات المطلوبة. خطاب حامل البطاقة أو بريد إلكتروني أو رسالة أو خطأ مكتمل في نموذج نزاع

نقطة تفاعل (POI) يصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع.

ويجب أن يحدد خطاب حامل البطاقة أو البريد الإلكتروني أو الرسالة أو خطأ نموذج النزاع المكتمل في

نقطة التفاعل (POI) وسائل الدفع البديلة التي توفر تفاصيل كافية عن المعاملة للسماح للتاجر بتحديد

موقع الدفع البديل.

عند استخدام طريقة الدفع لمشغل شبكة الدفع غير المحلية، يجب أن تحدد المستندات بالتفصيل

طريقة الدفع الخاصة ومشغل شبكة الدفع غير المحلية. تشمل الأمثلة على سبيل المثال لا الحصر:

- كشف حساب مصرفي يوثق عملية الدفع للتاجر.
- إيصال يوضح أن المعاملة ستكون نقدية كطريقة الدفع.

التعليق المطلوب. لا يوجد

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove that both Transactions were valid.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. Valid receipts documenting two separate Transactions.

The receipts must clearly establish that the Cardholder was not debited more than once for the same goods or services. A Merchant explanation must be included when the documentation does not clearly establish two separate valid Transactions.

Required Comment. None.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code. RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition. The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقًا
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل الإنصاف

شروط رفض رد المبالغ المدفوعة. يجوز للقابل إثبات أن كلا المعاملتين كانتا صحيحتين.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. إيصالات صالحة توثق عمليتين منفصلتين.

يجب أن تثبت الإيصالات بوضوح أن حامل البطاقة لم يتم خصمه أكثر من مرة عن نفس السلع أو

الخدمات. ويجب تضمين تفسير التاجر عندما لا تحدد المستندات بوضوح معاملتين صالحتين منفصلتين.

التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شروط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويتها والرقم المرجعي الفريد لمقاصة الاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شروط رفض رد المبالغ المدفوعة. لم تفِ جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد

المبالغ المدفوعة غير صحيحة، أو كان حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد

في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. الشرط الذي لم تستوفه جهة الإصدار.

رمز السبب. RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.

شروط رفض رد المبالغ المدفوعة: إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة،

أو غير مرتبطة بمطالبة رد المبالغ المدفوعة، أو غير مكتملة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

Reason Code. RSN05-Chargeback documents were not received

Chargeback Rejection Condition. The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.4.4 Transaction amount is different

Reason Code. CBCD16

Chargeback Creation Condition. The Cardholder contacted the Issuer claiming the Cardholder was billed an incorrect amount. This includes an increase for loss, theft, or damage.

This chargeback is not available for verbal price agreements.

Time Frame. 120 calendar days of the Transaction processing date.

Required Documents. Both of the following:

- A Cardholder letter, email, message, or completed Dispute Form-Point-of-Interaction (POI) Error describing the Cardholder’s complaint in sufficient detail to enable all parties to understand the dispute, including the Transaction amount that should have been billed.
- Documentation detailing the correct Transaction amount. Examples include, but are not limited to:
 - A receipt or invoice including the correct Transaction amount
 - The final hotel or car rental bill
 - Merchant email confirming price

Required Comment. None

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received

رمز السبب. RSN05: إذا لم يتم استلام مستندات رد المبالغ المدفوعة.

شُروط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN07 إعادة تحميل المبالغ المكررة

شُروط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08- رد المبالغ المدفوعة خارج الإطار الزمني.

شُروط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار

الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

4.4.2.2 الاختلاف في مبلغ المعاملة

رمز السبب. CBCD16

شُروط إنشاء رد المبالغ المدفوعة. ان يقوم حامل البطاقة بالتواصل مع جهة الإصدار مدعيًا أنه تم إصدار

فاتورة له بمبلغ غير صحيح. يتضمن ذلك زيادة الخسائر أو السرقة أو التلف.

لا يمكن رد المبالغ المدفوعة في حالة الاتفاقات الشفوية (اللفظية) للأسعار.

الإطار الزمني. في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة.

المستندات المطلوبة. كلا ما يلي:

- خطاب حامل البطاقة أو رسالة بريد إلكتروني أو رسالة أو خطأ مكتمل في نموذج نزاع نقطة تفاعل (POI) يصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع ، بما في ذلك مبلغ المعاملة التي كان ينبغي تحرير فاتورة بها.
- مستندات تحدد القيمة الصحيحة لمبلغ المعاملة، تشمل الأمثلة على سبيل المثال لا الحصر:
 - إيصال أو فاتورة متضمنة مبلغ المعاملة الصحيح.
 - الفاتورة النهائية للفندق أو تأجير السيارات.
 - البريد الإلكتروني للتاجر الذي يؤكد السعر.

التعليق المطلوب. لا يوجد

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - ائتمان تم إصداره مسبقًا
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة/ غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.

- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can provide evidence that the Cardholder was billed the correct amount.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. The Acquirer’s explanation and any relevant documents to support the Acquirer’s claim. Relevant documents include, but is not limited to, a receipt showing gratuity was added or an itemized receipt equal to the billed amount showing each item purchased and its price to ensure the total was correctly calculated.

Required Comment. None.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code. RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition. The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN05-Chargeback documents were not received)

Chargeback Rejection Condition. The Required Documents required for this chargeback were not received.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 20 business days of the processing date of the chargeback.

- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شرط رفض رد المبالغ المدفوعة. يجوز للقابل إثبات أن حامل البطاقة قد دفع بالمبلغ الصحيح.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. تفسير القابل وأي مستندات ذات صلة لإثبات ادعاءه. تتضمن المستندات ذات الصلة ، على سبيل المثال لا الحصر ، إيصالاً يوضح إضافة المكافأة أو إيصال مفصل يساوي مبلغ الفاتورة الذي يُظهر كل عنصر تم شراؤه وسعره لضمان حساب الإجمالي بشكل صحيح. التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 أئتمان تم إصداره مسبقًا

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويتها والرقم المرجعي الفريد لمقاصة الاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. لم تف جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد المبالغ المدفوعة غير صحيحة، أو كان حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. الشرط الذي لم تستوفه جهة الإصدار.

رمز السبب. RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة/ غير كاملة.

شرط رفض رد المبالغ المدفوعة: إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة ، أو غير مكتملة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN05: إذا لم يتم استلام مستندات رد المبالغ المدفوعة.

شرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. -RSN07 إعادة تحميل المبالغ المكررة

شرط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.4.5 Late Presentment

Reason Code. CBCD17

Chargeback Creation Condition. Issuer may use this reason code when both of the following conditions occurred.

Condition 1: The clearing record was processed beyond:

- 7 days from the authorization date for a Transaction with a POS Entry Mode value of 02, 05, 90, or 81.
- 30 days of the authorization date for a Transaction with a POS Entry Mode value of 01.

When calculating the number of days, consider the Transaction date as day zero.

An Issuer must accept a Transaction submitted beyond the applicable time frame when the account is in good standing or the Transaction can be honored.

Condition 2: The Card is permanently closed.

Time Frame. 120 calendar days of the Transaction processing date.

Required Documents. None

Required Comment. None

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove that the account was open.

Time Frame. Within 20 business days of the processing date of the chargeback.

Required Documents. Documentation that the Issuer authorized a Transaction with the same Card number after the chargeback date.

Required Comment. None.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. -RSN08 رد المبالغ المدفوعة خارج الإطار الزمني.

شرط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

5.4.2.2 التقديم المتأخر

رمز السبب. CBCD17

شرط إنشاء رد المبالغ المدفوعة. يجوز لجهة الإصدار استخدام رمز هذا السبب في الحالتين التاليتين:

الشرط 1: إذا تمت معالجة سجل المقاصة بعد:

- 7 أيام من تاريخ التفويض لمعاملة بقيمة وضع إدخال نقطة البيع 02 أو 05 أو 90 أو 81.
 - 30 يومًا من تاريخ التفويض لمعاملة بقيمة 01 في وضع إدخال نقطة البيع.
- غير أنه يجب الملاحظة، أنه عند حساب عدد الأيام، يجب الاخذ في الاعتبار أن الميعاد يبدأ في السريان من اليوم التالي للمعاملة، بمعنى أن تاريخ الحركة هو اليوم صفر.

يجب أن تقبل جهة الإصدار المعاملة المقدمة بعد الإطار الزمني المعمول به عندما يكون الحساب في وضع جيد أو يمكن الايفاء بالمعاملة.

الشرط 2: البطاقة مغلقة بشكل دائم.

الإطار الزمني. في غضون 120 يومًا تقويمياً من تاريخ تسوية المعاملة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - أئتمان تم إصداره مسبقًا
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شرط رفض رد المبالغ المدفوعة. يجوز للقابل إثبات أن الحساب كان مفتوحًا.

الإطار الزمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. وثيقة تفيد بأن جهة الإصدار قد صرّحت بمعاملة بنفس رقم البطاقة بعد تاريخ رد المبالغ المدفوعة.

التعليق المطلوب. لا يوجد.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. The Merchant posted a refund to Card
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number fields in chargeback did not match any presentment records.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. The condition the Issuer did not meet.

Reason Code. RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition. The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

Reason Code. RSN05-Chargeback documents were not received)

Chargeback Rejection Condition. The Required Documents required for this chargeback were not received.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.
Time Frame. Within 20 business days of the processing date of the chargeback.
Required Documents. None
Required Comment. None

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شروط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة
الإطار الزمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد
التعليق المطلوب. تاريخ الاسترداد الذي تمت معالجته والرقم المرجعي الفريد للمقاصة للاسترداد

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شروط رفض رد المبالغ المدفوعة. لم تفي جهة الإصدار بشروط رد المبالغ المدفوعة ، أو أن أيًا من بيانات رد المبالغ المدفوعة كانت غير صالحة ، أو أن حقلي PAN والرقم المرجعي للمسح الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات العرض التقديمي.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد
التعليق المطلوب. الشرط الذي لم تستوفه جهة الإصدار.

رمز السبب. RSN04 - كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة
شروط رفض رد المبالغ المدفوعة. كانت المستندات المطلوبة التي قدمتها جهة الإصدار إما غير مقروءة أو غير مرتبطة بمطالبة رد المبالغ المدفوعة هذه أو غير مكتملة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

رمز السبب. RSN05 - لم يتم استلام مستندات رد المبالغ المدفوعة

شروط رفض رد المبالغ المدفوعة. لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.
إطار زمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد.
التعليق المطلوب. لا يوجد.

رمز السبب. -RSN07 إعادة تحميل المبالغ المكررة

شروط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.
الإطار الزمني. في غضون 20 يوم عمل من تاريخ معالجة عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد
التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. -RSN08 رد المبالغ المدفوعة خارج الإطار الزمني

شروط رفض رد المبالغ المدفوعة. تمت معالجة عملية رد المبالغ المدفوعة خارج الإطار الزمني لرمز سبب رد المبالغ المدفوعة.
إطار زمني. في غضون 20 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.
المستندات المطلوبة. لا توجد
التعليق المطلوب. لا يوجد

2.2.4.6 ATM deposit was not posted to Card balance

Reason Code. CBCD27 ATM deposit was not posted to the Card balance

Creation Condition. Both of the following:

- The Cardholder contacted the Issuer claiming that some or all of the funds deposited through an ATM Transaction were not applied to the Cardholder's Card account.
- National Scheme Operator did not settle the deposited amount to the Issuer's billing/reconciliation report

Time Frame. 120 calendar days of the Transaction processing date.

Required Documents. A Cardholder letter, email, message, or completed Dispute Form-Point-of-Interaction (POI) Error describing the Cardholder's complaint in sufficient detail to enable all parties to understand the dispute. The Cardholder documentation must include all of the following information:

- ATM location
- Disputed deposit amount
- Total deposit amount
- Transaction date and approximate time

Required Comment. None

Notes: This reason code is prohibited when the disputed Transaction received approved response, or time out response (reason code 91).

The disputed Transaction is the deposit authorization request record.

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. One of the following:

Condition 1: The Acquirer can prove that the deposited funds were returned by the ATM to the Cardholder.

Condition 2: The claimed amount by the Issuer did not match the Acquirer records. The Acquirer must reject the dispute and return back the correct amount based on the Acquirer records via surplus option.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. One of the following Conditions corresponding to the Chargeback Rejection Condition in this same subsection:

Condition 1: The Acquirer's explanation and documentation proving the funds were returned to the Cardholder.

6.4.2.2 6.4.2.2 لم يتم ترحيل إيداع جهاز الصراف الآلي إلى رصيد البطاقة

رمز السبب. CBCD27. لم يتم ترحيل إيداع في جهاز الصراف الآلي إلى رصيد البطاقة.

شروط الإنشاء. كلا ما يلي:

- أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مدعياً أن بعض أو كل الأموال المودعة من خلال معاملة جهاز الصراف الآلي لم يتم تطبيقها على حساب البطاقة الخاص بحامل البطاقة.
- لم يتم مشغل شبكة الدفع المحلية بتسوية المبلغ المودع في تقرير الفواتير/ التسوية الخاصة بجهة الإصدار.

الإطار الزمني. في غضون 120 يومًا تقويمياً من تاريخ تسوية المعاملة.

المستندات المطلوبة. خطاب حامل البطاقة أو بريد إلكتروني أو رسالة أو خطأ مكتمل في نموذج نزاع نقطة تفاعل (POI) يصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع.

يجب أن تتضمن وثائق حامل البطاقة جميع المعلومات التالية:

- مواقع أجهزة الصراف الآلي.
- قيمة مبلغ الإيداع المتنازع عليه.
- إجمالي مبلغ الإيداع.
- تاريخ المعاملة ووقتها التقريبي.

التعليق المطلوب. لا يوجد

ملاحظات: رمز السبب هذا محظور، عندما تتلقى المعاملة المتنازع عليها استجابة معتمدة، أو استجابة مهلة (رمز السبب 91).

المعاملة المتنازع عليها هي سجل طلب تفويض الإيداع.

شروط رفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

- RSN01 - المستندات المرفقة وسبل المعالجة
- RSN02 - أئتمان تم إصداره مسبقاً
- RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.
- RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.
- RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.
- RSN07 - تكرار رد المبالغ المدفوعة.
- RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب.-RSN01 المستندات المرفقة وسبل المعالجة

شروط رفض رد المبالغ المدفوعة. أحد الشروط التالية:

الشرط 1: يجوز للقابل إثبات أن الأموال المودعة قد أعيدت بواسطة جهاز الصراف الآلي إلى حامل البطاقة.

الشرط 2: أن المبلغ المطالب به من قبل جهة الإصدار لا يتطابق مع سجلات القابل. يجب على القابل رفض النزاع وإعادة المبلغ الصحيح بناءً على سجلات القابل عبر خيار الفائض.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. أحد الشروط التالية المقابلة لشرط رفض رد المبالغ المدفوعة في هذا القسم الفرعي نفسه:

الشرط 1: أن يقوم القابل بتقديم تفسيره والمستندات التي تثبت إعادة الأموال إلى حامل البطاقة.

The documentation must come from the ATM journal and, at minimum, must include:

- Account accessed
- ATM number
- Account PAN read from Track 2 of the magnetic stripe or from the chip
- The ATM financial activity showing that funds were properly dispensed without any error before and after the disputed Transaction.
- Transaction amount
- Transaction date and time
- Transaction trace
- Transaction type

Acquirer may provide a Transaction report.

When necessary, an explanation describing each element of the journal and/or report.

Condition 2: Documentation proving the surplus amount.

Required Comment. One of the following Conditions corresponding to the Chargeback Rejection Condition in this same subsection:

Condition 1: None.

Condition 2: Surplus date and amount

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. A refund was posted to the Card

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number) fields in chargeback did not match any presentment records.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code. RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition. The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

يجب أن تتطابق المستندات مع مجلة جهاز الصرافي الآلي ويجب أن تتضمن على الأقل ما يلي:

- الوصول إلى الحساب.
- رقم جهاز الصراف الآلي.
- قراءة رقم الحساب الأساسي الحساب من المسار 2 للشريط المغناطيسي أو من الشريحة.
- أن يظهر النشاط المالي لأجهزة الصراف الآلي، أنه قد تم صرف الأموال بشكل صحيح دون وجود أي خطأ قبل وبعد المعاملة المتنازع عليها.
- القيمة النقدية لمبلغ التحويل.
- تاريخ ووقت المعاملة.
- تتبع تسلسل المعاملات.
- نوع المعاملة.

بإمكان القابل تقديم تقرير النعاملات ، وعند الضرورة تقديم شرح يبين كافة عناصر المجلة و/ أو التقرير.

الشرط 2: توثيق فائض المبلغ.

التعليق المطلوب. أحد الشروط التالية المقابلة لشرط رفض رد المبالغ المدفوعة في هذا القسم الفرعي نفسه:

الشرط 1: لا يوجد.

الشرط 2: تاريخ الفائض والمبلغ

رمز السبب. RSN02- ائتمان تم إصداره مسبقًا

شرط رفض رد المبالغ المدفوعة. تم إرسال رد إلى البطاقة

الإطار زمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. تاريخ الاسترداد الذي تمت معالجته والرقم المرجعي الفريد لمقاصة للاسترداد

رمز السبب. IRS-N03 رد المبالغ المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. لم تفي جهة الإصدار بشروط رد المبالغ المدفوعة ، أو أن أيًا من بيانات رد المبالغ المدفوعة غير صالح ، أو أن حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد لم يتطابقوا مع أي من سجلات العرض التقديمي.

الإطار زمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. الشرط الذي لم تستوفيه جهة الإصدار.

رمز السبب. RSN04 - كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة

شرط رفض رد المبالغ المدفوعة. كانت المستندات المطلوبة التي قدمتها جهة الإصدار إما غير مقروءة أو غير مرتبطة بمطالبة رد المبالغ المدفوعة هذه أو غير مكتملة.

الإطار زمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. لا يوجد

Reason Code: RSN05-Chargeback documents were not received)

Chargeback Rejection Condition. The Required Documents required for this chargeback were not received.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.2.4.7 POS deposit was not posted to Card balance**Reason Code. CBCD28 POS deposit was not posted to the Card balance**

Creation Condition. Both of the following:

- The Cardholder contacted the Issuer claiming that some or all of the funds deposited through a POS Transaction were not applied to the Cardholder's Card account.
- National Scheme Operator did not settle the deposited amount to the Issuer's billing/reconciliation report

Time Frame. 120 calendar days of the Transaction processing date.

Required Documents. A Cardholder letter, email, message, or completed Dispute Form-Point-of-Interaction (POI) Error describing the Cardholder's complaint in sufficient detail to enable all parties to understand the dispute. The Cardholder documentation must include all of the following information:

- Merchant name and address
- Disputed deposit amount
- Total deposit amount
- Transaction date and approximate time

Required Comment. None

Notes: This reason code is prohibited when the disputed Transaction received approved response, or time out response (reason code 91).

The disputed Transaction is the deposit authorization request record.

رمز السبب: RSN05 لم يتم استلام مستندات رد المبالغ المدفوعة

شروط رفض رد المبالغ المدفوعة. لم يتم استلام المستندات المطلوبة المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. لا يوجد

رمز السبب. RSN07 إعادة تحميل المبالغ المكررة

شروط رفض رد المبالغ المدفوعة. تم التنازع على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. RSN08 رد المبالغ المدفوعة خارج الإطار الزمني

شروط رفض رد المبالغ المدفوعة. تمت معالجة عملية رد المبالغ المدفوعة خارج الإطار الزمني لرمز

سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد

التعليق المطلوب. لا يوجد

7.4.2.2 لم يتم ترحيل إيداع نقاط البيع إلى رصيد البطاقة**رمز السبب. D28CBC. لم يتم ترحيل إيداع نقاط البيع إلى رصيد البطاقة**

شروط الإنشاء. كلا مما يلي:

- أن يقوم حامل البطاقة بالتواصل مع جهة الإصدار مدعيًا أن بعض أو كل الأموال المودعة من خلال معاملة نقاط البيع لم يتم تطبيقها على حساب البطاقة الخاص به.
- أن مشغل شبكة الدفع المحلية لم يقم بتسوية المبلغ المودع في تقرير الفواتير/ التسوية الخاصة بجهة الإصدار.

الإطار الزمني. في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة.

المستندات المطلوبة. خطاب حامل البطاقة أو بريد إلكتروني أو رسالة أو خطأ مكتمل في نموذج نزاع- نقطة تفاعل (POI) يصف شكوى حامل البطاقة بتفاصيل كافية لتمكين جميع الأطراف من فهم النزاع.

يجب أن تتضمن وثائق حامل البطاقة جميع المعلومات التالية:

اسم التاجر وعنوانه.

- قيمة مبلغ الإيداع المتنازع عليه.

- إجمالي قيمة مبلغ الإيداع.

- تاريخ المعاملة ووقتها التقريبي.

التعليق المطلوب. لا يوجد

ملاحظات: رمز السبب هذا محظور عندما تتلقى المعاملة المتنازع عليها استجابة معتمدة ، أو استجابة مهلة (رمز السبب 91).

المعاملة المتنازع عليها هي سجل طلب تفويض الإيداع.

Chargeback Rejection Conditions

An Acquirer may reject the chargeback for one of the following reasons:

- RSN01-Attached Documents and Remedy
- RSN02-Credit previously issued
- RSN03-Chargeback is invalid
- RSN04-Chargeback documents were illegible/unrelated/incomplete
- RSN05-Chargeback documents were not received
- RSN07-Duplicate chargeback
- RSN08-Chargeback out of time frame

Reason Code. RSN01-Attached Documents and Remedy

Chargeback Rejection Condition. The Acquirer can prove that the funds were returned by the Merchant to the Cardholder.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. The Acquirer's explanation and documentation proving the funds were returned to the Cardholder.

Required Comment. None.

Reason Code. RSN02-Credit previously issued

Chargeback Rejection Condition. A refund was posted to the Card

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Date of the processed refund and the Unique Clearing Reference Number of the refund

Reason Code. RSN03-Chargeback is invalid:

Chargeback Rejection Condition. The Issuer did not meet the chargeback conditions, any of the chargeback data was invalid, or PAN and Unique Clearing Reference Number) fields in chargeback did not match any presentment records.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. The condition the Issuer did not meet.

Reason Code. RSN04-Chargeback documents were illegible/unrelated/incomplete

Chargeback Rejection Condition. The Required Documents provided by the Issuer were either illegible, not related to this chargeback claim, or incomplete.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

Reason Code: RSN05-Chargeback documents were not received)

Chargeback Rejection Condition. The Required Documents required for this chargeback were not received.

Time Frame. Within 10 business days of the processing date of the chargeback.

شروط إرفض رد المبالغ المدفوعة

يجوز للقابل رفض رد المبالغ المدفوعة لأحد الأسباب التالية:

RSN01 - المستندات المرفقة وسبل المعالجة

RSN02 - ائتمان تم إصداره مسبقًا

RSN03 - إذا كان رد المبالغ المدفوعة غير صالح.

RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.

RSN05 - إذا لم يتم استلام مستندات رد المبالغ المدفوعة.

RSN07 - تكرار رد المبالغ المدفوعة.

RSN08 - رد المبالغ المدفوعة خارج الإطار الزمني.

رمز السبب. -RSN01 المستندات المرفقة وسبل المعالجة

شرط رفض رد المبالغ المدفوعة. يجوز للقابل إثبات أن التاجر قد أعاد الأموال إلى حامل البطاقة.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. أن يقوم القابل بتقديم تفسيره والمستندات التي تثبت رد الأموال إلى حامل البطاقة.

التعليق المطلوب. لا يوجد.

رمز السبب. -RSN02 ائتمان تم إصداره مسبقًا

شرط رفض رد المبالغ المدفوعة. نشر التاجر رد أموال إلى البطاقة

الإطار الزمني. في غضون 10 يوم عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. تاريخ الاسترداد الذي تمت تسويته والرقم المرجعي الفريد لمقاصة الاسترداد.

رمز السبب. RSN03 رد المبالغ المدفوعة غير صالح:

شرط رفض رد المبالغ المدفوعة. تم تفي جهة الإصدار بشروط رد المبالغ المدفوعة، أو كانت بيانات رد المبالغ المدفوعة غير صحيحة، أو كان حقلي رقم الحساب الأساسي والرقم المرجعي للمقاصة الفريد في رد المبالغ المدفوعة لا يتطابقان مع أي من سجلات عرض التقديم.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. الشرط الذي لم تستوفيه جهة الإصدار.

رمز السبب. RSN04 - إذا كانت مستندات رد المبالغ المدفوعة غير مقروءة / غير ذات صلة / غير كاملة.

شرط رفض رد المبالغ المدفوعة: إذا كانت المستندات المطلوبة التي قدمتها جهة الإصدار غير مقروءة، أو غير مرتبطة بمطالبة رد المبالغ المدفوعة، أو غير مكتملة.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. RSN05: إذا لم يتم استلام مستندات رد المبالغ المدفوعة.

شرط رفض رد المبالغ المدفوعة: لم يتم استلام المستندات المطلوبة لرد المبالغ المدفوعة.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

Required Documents. None

Required Comment. None

Reason Code. RSN07-Duplicate Chargeback

Chargeback Rejection Condition. The same Transaction was disputed more than one time.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. Chargeback ID of the previously received chargeback.

Reason Code. RSN08-Chargeback out of time frame

Chargeback Rejection Condition. The chargeback was processed out of the time frame of the chargeback reason code.

Time Frame. Within 10 business days of the processing date of the chargeback.

Required Documents. None

Required Comment. None

2.3 Pre-Arbitration and Arbitration Case Filing

2.3.1 Overview

A dispute may be continued after the chargeback cycles have completed by using the pre-arbitration and arbitration case filing process.

The arbitration process is prohibited when:

- The chargeback creation required documents were not related to the dispute.
- The chargeback creation documents were not provided.
- The chargeback creation was out of time frame.
- The chargeback creation was a duplicate chargeback.

All arbitration cases must be submitted and managed through the National Scheme Operator portal. Daily review of the National Scheme Operator portal to manage cases within applicable timeframes is strongly recommended.

2.3.2 Issuer Submission of a Pre-Arbitration Case

2.3.2.1 Cardholder Dispute-Cardholder Reasserts Claim

An Issuer may submit a pre-arbitration case when both of the following occurred:

- The original chargeback creation was valid
- The chargeback rejection required documents were reviewed by the Cardholder and the Cardholder reasserts their dispute

Required Documents. A new Cardholder letter, email, or message dated after the chargeback rejection and specifically addressing the Merchant's rebuttal provided with the chargeback rejection.

In addition:

- For Disputes Involving Goods or Services were Not as Described or Defective: When not provided with the chargeback creation, documentation from an expert or professional (on their business letterhead, with a business card attached, or validated by other information demonstrating that the opinion expressed is that of an expert) that supports the Cardholder's dispute about the level of quality or misrepresentation may be required when the validity of the dispute is challenged by the Merchant. Other documentation

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

رمز السبب. -RSN07 إعادة تحميل المبالغ المكررة

شرط رفض رد المبالغ المدفوعة. أن تتكرر نفس المنازعة على نفس المعاملة أكثر من مرة.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. معرّف رد المبالغ المدفوعة لعملية رد المبالغ المدفوعة التي تم استلامها مسبقًا.

رمز السبب. -N08 IRS رد المبالغ المدفوعة خارج الإطار الزمني.

شرط رفض رد المبالغ المدفوعة. أن تكون تسوية عملية رد المبالغ المدفوعة قد تمت خارج الإطار

الزمني لرمز سبب رد المبالغ المدفوعة.

الإطار الزمني. في غضون 10 أيام عمل من تاريخ تسوية عملية رد المبالغ المدفوعة.

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

3.2 رفع دعوى ما قبل التحكيم والتحكيم

1.3.2 نظرة عامة

قد يستمر النزاع بعد اكتمال دورات رد المبالغ المدفوعة باستخدام عملية تقديم دعوى ما قبل التحكيم والتحكيم.

تحظر عملية بالتحكيم في الحالات التالية:

- إذا لم تكن المستندات المطلوبة لإنشاء رد المبالغ المدفوعة متعلقة بالنزاع.
- إذا لم يتم توفير مستندات إنشاء رد المبالغ المدفوعة.
- إذا كان إنشاء رد المبالغ المدفوعة خارج الإطار الزمني.
- إذا كان إنشاء رد المبالغ المدفوعة عبارة عن عملية رد مبالغ مدفوعة بطريقة مكررة.

يجب تقديم جميع قضايا التحكيم وإدارتها من خلال بوابة مشغل شبكة الدفع المحلية. يوصى بشدة بإجراء مراجعة يومية لبوابة مشغل شبكة الدفع المحلية لإدارة الحالات ضمن الأطر الزمنية المعمول بها

2.3.2.2 تقديم جهة الإصدار لدعوى ما قبل التحكيم

1.2.3.2 1. نزاع حامل البطاقة - يعيد حامل البطاقة تأكيد المطالبة

يجوز لجهة الإصدار تقديم دعوى ما قبل التحكيم عند حدوث كلا الحالتين التاليتين:

- إذا كان إنشاء رد المبالغ المدفوعة الأصلي صالحًا.
- إذا قام حامل البطاقة بمراجعة المستندات المطلوبة لرفض المبالغ المدفوعة وأعاد حامل البطاقة تأكيد نزاعه.

المستندات المطلوبة: خطاب جديد لحامل البطاقة أو بريد إلكتروني أو رسالة مؤرخة بعد رفض رد المبالغ المدفوعة، وتتناول على وجه التحديد رد التاجر المقدم مع رفض رد المبالغ المدفوعة.

فضلاً عن ذلك:

- بالنسبة للمنازعات التي تتضمن سلعًا أو خدمات لم تكن مطابقة للموصفات أو كانت معيبة: عندما لا يتم تزويدها بإنشاء رد المبالغ المدفوعة ، وتقرير الخبير (على ورق الأعمال الخاص بهم، مع إرفاق

necessary to support the validity of the dispute may include, but is not limited to, the original receipt, invoice, work order, brochure, contract, or appraisal.

- For Disputes Involving Credit Not Processed: When the original Cardholder letter, email, or message included in the chargeback states that the Cardholder returned the merchandise and the Merchant denies receiving the merchandise in the chargeback rejection, the Issuer must then provide proof that the merchandise was returned to and received by the Merchant to accompany the pre-arbitration case.
- For Disputes Involving Goods or Services Were Not Provided: When the chargeback rejection documentation includes a signed delivery receipt, the new Cardholder letter, email, or message must state the signature on the delivery receipt is not the Cardholder's signature or the signature of any person authorized by the Cardholder.
- For Disputes Involving a Lodging or Vehicle Rental "No-Show" Charge: When the original Cardholder letter, email, or message included in the chargeback creation did not include a cancellation number and the Acquirer processed a chargeback rejection that states one the following:
 - The hotel has a reservation program that includes the issuance of confirmation and cancellation numbers.
 - The hotel has no record of the cancellation.

Then the Cardholder must provide proof of Merchant contact within the cancellation time frame required by the reservation program (such as a copy of a phone bill indicating that a call was made to the Merchant before 18:00 [Merchant's local time] on the date of the reservation).

- For Disputes Involving Subsequent Transactions: The new Cardholder letter, email or message form dated after the chargeback rejection must also specifically state:
 - The Cardholder has reviewed the documentation provided by the Merchant in the chargeback rejection
 - The Cardholder engaged in a valid Transaction with the Merchant.
 - A subsequent Transaction occurred with that same Merchant without the Cardholder's consent.
 - The Cardholder contacted the Merchant, or attempted to contact the Merchant, to resolve the dispute.

Required Comment. None

2.3.2.2 Authorization Dispute Group – Invalid Chargeback Rejection

An Issuer may submit a pre-arbitration case when all of the following occurred:

- The chargeback creation was valid
- The chargeback rejection failed to resolve the dispute
- The Issuer continues to claim the Issuer did not approve the Transaction

Required Documents. The Issuer must explain why the Issuer believes the chargeback rejection to be invalid.

Required Comment. None.

بطاقة العمل، أو التحقق من صحتها من خلال معلومات أخرى توضح أن الرأي المعبر عنه هو الخيار) الذي يؤيد وجهة نظر حامل البطاقة حول مستوى الجودة، أو قد يكون التحريف مطلوبًا عندما يتم الطعن في صحة النزاع من قبل التاجر. وقد تتضمن المستندات الأخرى اللازمة لدعم صحة النزاع، على سبيل المثال، الإيصال الأصلي، أو الفاتورة أو أمر العمل أو الكتيب أو العقد أو التقييم.

- بالنسبة للمنازعات المتعلقة بالائتمان الذي لم تتم معالجته: عندما يشير خطاب حامل البطاقة الأصلي أو البريد الإلكتروني أو الرسالة المضمنة في طلب رد المبالغ المدفوعة إلى أن حامل البطاقة أعاد البضائع، وأن التاجر يرفض استلام البضائع في رفض رد المبالغ المدفوعة، يجب على جهة الإصدار بعد ذلك إثبات أن السلعة تم إرجاعها إلى التاجر واستلامها لإرفاقها بدعوى ما قبل التحكيم.

- بالنسبة للمنازعات التي تتضمن سلعًا أو خدمات لم يتم تقديمها: عندما تتضمن مستندات رفض رد المبالغ المدفوعة إيصال تسليم موقعًا، ويجب أن يشير خطاب حامل البطاقة الجديد أو البريد الإلكتروني أو الرسالة الجديدة إلى أن التوقيع على إيصال التسليم، ليس توقيع حامل البطاقة أو توقيع أي شخص ينوب حامل البطاقة.

- بالنسبة للمنازعات التي تنطوي على رسوم "عدم الحضور" الخاصة بالإقامة أو استئجار السيارة: عندما لا يتضمن خطاب حامل البطاقة الأصلي أو البريد الإلكتروني أو الرسالة المضمنة في إنشاء رد المبالغ المدفوعة رقم إلغاء وتعالج الجهة القابلة لرفض رد المبالغ المدفوعة الذي ينص على أحد ما يلي:

- يوجد بالفندق برنامج حجز يتضمن إصدار أرقام التأكيد والإلغاء.

- الفندق ليس لديه سجل للإلغاء.

بعد ذلك، يجب على حامل البطاقة إثبات اتصاله بالتاجر خلال الإطار الزمني للإلغاء الذي يتطلبه برنامج الحجز (مثل نسخة من فاتورة الهاتف تشير إلى أنه تم إجراء مكالمة إلى التاجر قبل الساعة 18:00 [التوقيت المحلي للتاجر] في تاريخ الحجز).

- بالنسبة للمنازعات التي تتضمن معاملات لاحقة: خطاب حامل البطاقة الجديد، البريد الإلكتروني. أو نموذج رسالة مؤرخ بعد رفض رد المبالغ المدفوعة يجب أن يذكر أيضًا على وجه التحديد:
 - أن حامل البطاقة قام بمراجعة الوثائق المقدمة من التاجر في رفض رد المبالغ المدفوعة.
 - أن حامل البطاقة شارك في معاملة صالحة مع التاجر.
 - أن معاملة لاحقة حدثت مع نفس التاجر دون موافقة حامل البطاقة.
 - أن حامل البطاقة تواصل بالتاجر أو حاول الاتصال بالتاجر لحل النزاع.
- التعليق المطلوب. لا يوجد

2.2.3.2 مجموعة منازعات التفويض - رفض غير صالح لرد المبالغ المدفوعة

يجوز لجهة الإصدار تقديم دعوى ما قبل التحكيم عند حدوث كل ما يلي:

- إذا كان إنشاء رد المبالغ المدفوعة صالحًا.
- إذا فشلت عملية رفض رد المبالغ المدفوعة في حل النزاع.
- إذا استمرت جهة الإصدار في المطالبة بأنه لم يوافق على المعاملة.

المستندات المطلوبة. يجب أن تقدم جهة الإصدار تفسيراً لسبب اعتقادها أن رفض رد المبالغ المدفوعة غير صالح.

التعليق المطلوب. لا يوجد.

2.3.2.3 Cardholder Claims Group – Invalid Chargeback Rejection

- An Issuer may submit a pre-arbitration case when both of the following occurred: The original chargeback creation was valid
- One of the following Conditions::

Condition 1: The chargeback rejection required documents failed to remedy the Cardholder Claims Group chargeback.

Condition 2: The chargeback rejection required documents was reviewed by the Cardholder and the Cardholder reasserts their claim.

Required Documents. One of the following Conditions corresponding to the Condition in previous row:

Condition 1: The Issuer must explain why the Issuer believes the chargeback rejection to be invalid.

Condition 2: A new Cardholder letter, email, or message dated after the second presentment specifically stating that the Cardholder has reviewed the documentation provided by the Merchant in the second presentment and the Cardholder continues to maintain that the disputed Transaction was not authorized by the Cardholder.

Required Comment. None.

2.3.2.4 No Cardholder Authorization – Invalid Chargeback Rejection

An Issuer may submit a pre-arbitration case when all of the following occurred:

- The original chargeback creation was valid
- One of the following Conditions:

Condition 1: The chargeback rejection required documents failed to remedy the No Cardholder Authorization chargeback.

Condition 2: The chargeback rejection required documents was reviewed by the Cardholder and the Cardholder reasserts the disputed Transaction is fraudulent

Condition 3: For “No Show” Transaction: One or both of the following:

- The Cardholder account number and/or Cardholder name and/or Cardholder address provided by the Merchant in the chargeback rejection is not accurate.
- The confirmation number provided at the time the reservation was made does not match the confirmation number provided by the Merchant in the chargeback rejection.

Required Documents. One of the following Conditions corresponding to the Condition in the previous row:

Condition 1: The Issuer must explain why the Issuer believes the chargeback rejection to be invalid.

Condition 2: A new Cardholder letter, email, or message dated after the second presentment specifically stating that the Cardholder has reviewed the documentation provided by the Merchant in the second presentment and the Cardholder continues to maintain that the disputed Transaction was not authorized by the Cardholder.

Condition 3: The Issuer must explain which information is not accurate (for example, incorrect Cardholder name or incorrect Cardholder address).

Required Comment. None.

3.2.3.2 مجموعة مطالبات حامل البطاقة - رفض غير صالح لرد المبالغ المدفوعة

يجوز لجهة الإصدار تقديم دعوى ما قبل التحكيم عند حدوث كلتي الحالتين التاليتين:

- إذا كان إنشاء رد المبالغ المدفوعة الأصلي صالحًا.
- أحد الشروط التالية:

الشرط 1: إذا فشلت المستندات المطلوبة لرفض المبالغ المدفوعة في تسوية رد المبالغ المدفوعة لمجموعة مطالبات حامل البطاقة.

الشرط 2: إذا تمت مراجعة المستندات المطلوبة لرفض المبالغ المدفوعة من قبل حامل البطاقة، وأعاد حامل البطاقة تأكيد مطالبته.

المستندات المطلوبة. يجب توافر أحد الشروط التالية المطابقة للشرط في الصف السابق:

الشرط 1: يجب أن تقدم جهة الإصدار تفسيراً لسبب اعتقادها أن رفض رد المبالغ المدفوعة غير صالح.

الشرط 2: خطاب جديد لحامل البطاقة أو بريد إلكتروني أو رسالة مؤرخة بعد عرض التقديم الثاني، تنص على وجه التحديد على أن حامل البطاقة قد راجع المستندات التي قدمها التاجر في العرض الثاني، وأن حامل البطاقة يستمر في التأكيد على أن المعاملة المتنازع عليها لم يتم التصريح بها من قبل حامل البطاقة.

التعليق المطلوب. لا يوجد.

4.2.3.2 لا يوجد تصريح من حامل البطاقة - رفض غير صالح لرد المبالغ المدفوعة

يجوز لجهة الإصدار تقديم دعوى ما قبل التحكيم عند حدوث كل ما يلي:

- إذا كان إنشاء رد المبالغ المدفوعة الأصلي صالحًا.
- أحد الشروط التالية:

الشرط 1: إذا فشلت المستندات المطلوبة الخاصة برفض رد المبالغ المدفوعة في تسوية عملية رد المبالغ المدفوعة بدون ترخيص حامل البطاقة.

الشرط 2: إذا تمت مراجعة المستندات المطلوبة لرفض المبالغ المدفوعة من قبل حامل البطاقة وأكد أن المعاملة المتنازع عليها هي معاملة احتيالية.

الشرط 3: لمعاملة “عدم الحضور”: اتباع أحد الإجراءين التاليين أو كليهما:

- رقم حساب حامل البطاقة و / أو اسم حامل البطاقة و / أو عنوان حامل البطاقة المقدم من التاجر في رفض رد المبالغ المدفوعة غير دقيق.
- رقم التأكيد المقدم في وقت إجراء الحجز لا يتطابق مع رقم التأكيد المقدم من التاجر في رفض رد المبالغ المدفوعة.

المستندات المطلوبة. يجب توافر أحد الشروط التالية المطابقة للشرط في الصف السابق:

الشرط 1: يجب أن تقدم جهة الإصدار تفسيراً لسبب اعتقادها أن رفض رد المبالغ المدفوعة غير صالح.

الشرط 2: خطاب جديد لحامل البطاقة أو بريد إلكتروني أو رسالة مؤرخة بعد عرض التقديم الثاني، تنص على وجه التحديد على أن حامل البطاقة قد راجع المستندات التي قدمها التاجر في العرض الثاني، وأن حامل البطاقة يستمر في التأكيد على أن المعاملة المتنازع عليها لم يتم التصريح بها من قبل حامل البطاقة.

الشرط 3: يجب أن تحدد جهة الإصدار المعلومات غير الدقيقة (على سبيل المثال، اسم حامل البطاقة غير الصحيح، أو عنوانه غير الصحيح).

التعليق المطلوب. لا يوجد.

2.3.2.5 Chip Processing Rules – Invalid Chargeback Rejection

An Issuer may submit an arbitration case when both of the following occurred:

- The original chargeback creation was valid
- The chargeback rejection failed to remedy the dispute

Required Documents. The Issuer must explain why the Issuer believes the chargeback rejection to be invalid.

Required Comment. None

2.3.2.6 Point of Interaction Error – Invalid Chargeback Rejection

An Issuer may submit a pre-arbitration case when both of the following occurred:

- The original chargeback creation was valid
- The chargeback rejection failed to remedy the dispute

Required Documents. The Issuer must explain why the Issuer believes the chargeback rejection to be invalid.

Required Comment. None

2.3.2.7 Required Rejection Documents were illegible/Unrelated/Incomplete

An Issuer may submit a pre-arbitration case when both of the following occurred:

- The chargeback creation was valid
- The required rejection documents were illegible (meaning blank or unreadable pages)

Reason Code: CBCD25

Required Documents. None

Required Comment. None

2.3.2.8 Required Rejection Documents were not received

An Issuer may submit an arbitration case when both of the following occurred:

- The original chargeback was valid
- The required documents were not provided

Reason Code. CBCD26

Required Documents. None

Required Comment. None

2.3.2.9 Change of Chargeback Reason to an Authorization Dispute Group

An Issuer may submit a pre-arbitration case when the Issuer is changing the reason for the dispute from a non-Authorization Dispute Group to an Authorization Dispute Group.

In order to change the reason for a dispute all of the following must occur:

- The original chargeback creation was valid
- The original chargeback creation must have been processed within the applicable time frame
- The chargeback rejection remedied the original chargeback creation and identified that a valid Authorization Dispute Group chargeback is available and meets the corresponding conditions

5.2.3.2. قواعد معالجة الشريحة - رفض غير صالح لرد المبالغ المدفوعة

يجوز لجهة الإصدار تقديم دعوى تحكيم عند حدوث كلتي الحالتين التاليتين:

- إذا كان إنشاء رد المبالغ المدفوعة الأصلي صالحًا
 - إذا فشل رفض رد المبالغ المدفوعة في معالجة النزاع
- المستندات المطلوبة. يجب أن تقدم جهة الإصدار تفسيراً لسبب اعتقادها أن رفض رد المبالغ المدفوعة غير صالح.

التعليق المطلوب. لا يوجد

6.2.3.2. خطأ في نقطة التفاعل - رفض غير صالح لرد المبالغ المدفوعة

يجوز جهة الإصدار تقديم دعوى تحكيم عند حدوث كلتي الحالتين التاليتين:

- إذا كان إنشاء رد المبالغ المدفوعة الأصلي صالحًا.
 - إذا فشل رفض رد المبالغ المدفوعة في معالجة النزاع.
- المستندات المطلوبة. يجب أن تقدم جهة الإصدار تفسيراً لسبب اعتقادها أن رفض رد المبالغ المدفوعة غير صالح.

التعليق المطلوب. لا يوجد.

7.2.3.2. مستندات الرفض المطلوبة غير مقروءة / غير ذات صلة/ غير كاملة

يجوز لجهة الإصدار تقديم دعوى ما قبل التحكيم عند حدوث كلتي الحالتين التاليتين:

- إذا كان إنشاء رد المبالغ المدفوعة صالحًا
- إذا كانت مستندات الرفض المطلوبة غير مقروءة (بمعنى صفحات فارغة أو غير قابلة للقراءة)

رمز السبب. CBCD25

المستندات المطلوبة. لا توجد.

التعليق المطلوب. لا يوجد.

8.2.3.2. لم يتم استلام مستندات الرفض المطلوبة

يجوز لجهة الإصدار تقديم دعوى تحكيم عند حدوث الحالتين التاليتين:

- إذا كانت عملية رد المبالغ المدفوعة الأصلية صالحة.
- إذا لم يتم توفير المستندات المطلوبة للإثبات.

رمز الإسبب. CBCD26

المستندات المطلوبة. لا توجد.

التعليق المطلوب. يوجد.

9.2.3.2. تغيير سبب رد المبالغ المدفوعة إلى مجموعة نزاعات التفويض

يجوز لجهة الإصدار إرسال دعوى ما قبل التحكيم عندما تقوم جهة الإصدار بتغيير سبب النزاع من مجموعة منازعات عدم التفويض إلى مجموعة منازعات التفويض.

ولتغيير سبب النزاع، يجب توافر الشروط التالية:

- أن يكون إنشاء رد المبالغ المدفوعة الأصلي صالحًا.
- يجب أن تتم عملية تسوية إنشاء رد المبالغ المدفوعة الأصلية ضمن الإطار الزمني المعمول به.
- أن يؤدي رفض رد المبالغ المدفوعة إلى إصلاح عملية إنشاء رد المبالغ المدفوعة الأصلية، وتحديد أن رد المبالغ المدفوعة الصالح لمجموعة نزاع التفويض متاح ويفي بالشروط المقابلة.

Required Documents. The Issuer must provide both of the following:

- The Issuer’s explanation as to why the chargeback reason is being changed
- The required documents for the Authorization Dispute Group chargeback

Required Comment. None

2.3.2.10 Change of Chargeback Reason to a Customer Claims Group Chargeback

An Issuer must submit a pre-arbitration case when the Issuer is changing the reason for the dispute from a non-Customer Claims Group chargeback to a Customer Claims Group chargeback.

In order to change the reason for a dispute all of the following must occur:

- The original chargeback creation was valid
- The original chargeback creation must have been processed within the applicable time frame
- The chargeback rejection remedied the original chargeback creation and identified that a valid Customer Claims Group chargeback is available and meets the corresponding conditions

Required Documents. The Issuer must provide both of the following:

- The Issuer’s explanation as to why the chargeback reason is being changed
- The required documents for the Customer Claims Group chargeback

Required Comment. None

2.3.2.11 Change of Chargeback Reason to a No Cardholder Authorization Chargeback

An Issuer must submit a pre-arbitration case when the Issuer is changing the reason for the dispute from a non-No Cardholder Authorization chargeback to a No Cardholder Authorization chargeback.

In order to change the reason for a dispute all of the following must occur:

- The original chargeback creation was valid
- The original chargeback creation must have been processed within the applicable time frame
- The chargeback rejection remedied the original chargeback creation and identified that a valid No Cardholder Authorization chargeback is available and meets the corresponding conditions
- The chargeback rejection required documents were reviewed by the Cardholder and the Cardholder asserts the disputed Transaction is fraudulent

Required Documents. The Issuer must provide all of the following:

- The Issuer’s explanation as to why the chargeback reason is being changed
- The required documents for the No Cardholder Authorization chargeback
- A Cardholder letter, email, or message dated after the chargeback rejection specifically stating that the Cardholder has reviewed the documentation provided by the Merchant in the chargeback rejected and the Cardholder asserts that the disputed Transaction was not authorized by the Cardholder.

Required Comment. None

المستندات المطلوبة. يجب على جهة الإصدار تقديم كلٍ من التاليين:

- أن تقوم جهة الإصدار بتقديم تفسيراً لسبب تغيير سبب رد المبالغ المدفوعة.
- أن تقدم جهة الاصدار المستندات التي تثبت عملية رد المبالغ المدفوعة لمجموعة منازعات التفويض.

التعليق المطلوب. لا يوجد.

10.2.3.2 تغيير سبب رد المبالغ المدفوعة إلى مجموعة مطالبات العملاء المتعلقة برد المبالغ المدفوعة

يجب على جهة الإصدار إرسال دعوى ما قبل التحكيم، عندما تقوم بتغيير سبب النزاع، من مجموعة مطالبات غير العملاء إلى رد المبالغ المدفوعة من مجموعة مطالبات العملاء.

ولتغيير سبب النزاع، يجب توافر الشروط التالية:

- أن يكون إنشاء رد المبالغ المدفوعة الأصلي صالحًا.
- يجب أن تتم عملية تسوية إنشاء رد المبالغ المدفوعة الأصلية ضمن الإطار الزمني المعمول به.
- أن يؤدي رفض رد المبالغ المدفوعة إلى إصلاح عملية إنشاء رد المبالغ المدفوعة الأصلية، وتحديد أن رد المبالغ المدفوعة صالحًا لمجموعة نزاع التفويض متاح وفي بالشروط المقابلة.

المستندات المطلوبة. يجب على جهة الإصدار تقديم كلٍ من التاليين:

- أن تقوم جهة الإصدار بتقديم تفسيراً لسبب تغيير سبب رد المبالغ المدفوعة.
- أن تقدم جهة الاصدار المستندات التي تثبت عملية رد المبالغ المدفوعة لمجموعة العملاء.

التعليق المطلوب. لا يوجد.

11.2.3.2 تغيير سبب رد المبالغ المدفوعة إلى عدم تفويض حامل البطاقة لرد المبالغ المدفوعة

يجب على جهة الإصدار تقديم دعوى ما قبل التحكيم عندما تقوم بتغيير سبب النزاع، من رد المبالغ المدفوعة من عدم تفويض حامل البطاقة، إلى رد المبالغ المدفوعة بدون تصريح حامل البطاقة.

ولتغيير سبب النزاع، يجب توافر الشروط التالية:

- أن يكون إنشاء رد المبالغ المدفوعة الأصلي صالحًا.
- يجب أن تتم معالجة عملية إنشاء رد المبالغ المدفوعة الأصلية ضمن الإطار الزمني المعمول به.
- أن يؤدي رفض رد المبالغ المدفوعة إلى تصحيح عملية إنشاء رد المبالغ المدفوعة الأصلية، وتحديد أن صلاحية رد المبالغ المدفوعة ”لا يوجد تصريح حامل بطاقة“ متاحة وتفي بالشروط المقابلة.
- إذا تمت مراجعة المستندات المثبتة لعملية رفض المبالغ المدفوعة من قبل حامل البطاقة، وأكد أن المعاملة المتنازع عليها معاملة احتيالية.

المستندات المطلوبة. يجب على جهة الإصدار توفير كل ما يلي:

- أن تقوم جهة الإصدار بتقديم تفسيراً لسبب تغيير سبب رد المبالغ المدفوعة.
- أن تقدم جهة الإصدار المستندات المثبتة لعملية استرداد التكاليف بدون تصريح حامل البطاقة.
- خطاب لحامل البطاقة أو بريده الإلكتروني أو رسالة مؤرخة تفيد رفض رد المبالغ المدفوعة، وتشير على وجه التحديد إلى أن حامل البطاقة قد راجع المستندات المقدمة من التاجر في رفض رد المبالغ المدفوعة، ويؤكد حامل البطاقة أن المعاملة المتنازع عليها لم يصرح بها.

التعليق المطلوب. لا يوجد.

2.3.2.12 Change of Chargeback Reason to a Processing Error Group Chargeback

An Issuer must submit a pre-arbitration case when the Issuer is changing the reason for the dispute from a non-Processing Error Group dispute to a Processing Error Group dispute.

In order to change the reason to a Processing Error Group chargeback all of the following must occur:

- The original chargeback creation was valid
- The original chargeback creation must have been processed within the applicable time frame
- The chargeback rejection remedied the original chargeback creation and identified that a valid Processing Error Group chargeback is available and meets the corresponding conditions

Required Documents. The Issuer must provide both of the following:

- The Issuer's explanation as to why the chargeback reason is being changed
- The required documents for the Processing Error Group chargeback

Required Comment. None

2.3.3 Acquirer Response to a Pre-Arbitration Case

An Acquirer may take one of the following actions in response to receiving an arbitration case filing:

- Accept the arbitration case and thereby financial responsibility for the disputed Transaction.
- Reject the arbitration case
- Take no action

The Acquirer may reject the pre-arbitration case for one of the following reasons:

- The original chargeback creation was invalid.
- The pre-arbitration case was invalid. Examples include, but are not limited to, improper required documents, the Issuer submitted the pre-arbitration case beyond the applicable time frame.
- The Merchant has a rebuttal that specifically addresses the documentation provided in the pre-arbitration case. An example includes, but is not limited to, the disputed Transaction was properly authorized.
- When the Issuer has changed the chargeback reason: The chargeback rejection remedied the original chargeback and did not identify a new valid chargeback as being available.

Required Documents. When the Acquirer rejects the arbitration case, the Acquirer must provide an explanation for the rejection, and any relevant documentation that specifically addresses the information contained in the pre-arbitration.

Required Comment. None

2.3.4 Issuer Submission of a Pre-Arbitration Case

The Issuer may reject the Acquirer's claim by escalating the pre-arbitration to arbitration. No new information may be provided. The case will be sent to the arbitration committee for a final decision.

2.3.5 National Scheme Operator Review Process

National Scheme Operator will decline to rule on a case when the Issuer did not follow all filing requirements. Examples of incorrect filing include but are not limited to:

12.2.3.2. تغيير سبب رد المبالغ المدفوعة إلى مجموعة أخطاء في المعالجة

يجب على جهة الإصدار إرسال دعوى ما قبل التحكيم، عندما تقوم بتغيير سبب النزاع، من نزاع لمجموعة أخطاء معالجة غير معالجة، إلى نزاع في مجموعة أخطاء المعالجة.

لتغيير السبب إلى رد المبالغ المدفوعة من مجموعة أخطاء المعالجة ، يجب أن توافر الشروط التالية:

- أن يكون إنشاء رد المبالغ المدفوعة الأصلي صالحًا.
- يجب أن تتم معالجة عملية إنشاء رد المبالغ المدفوعة الأصلية ضمن الإطار الزمني المعمول به.
- أن يؤدي رفض رد المبالغ المدفوعة إلى إصلاح عملية إنشاء رد المبالغ المدفوعة الأصلية وتحديد أن عملية رد المبالغ المدفوعة لمجموعة أخطاء المعالجة الصالحة متاحة وتفي بالشروط المقابلة المستندات المطلوبة. يجب على جهة الإصدار تقديم كلٍ من التاليين:
- شرح جهة الإصدار لسبب تغيير سبب رد المبالغ المدفوعة
- المستندات المطلوبة لرد المبالغ المدفوعة من مجموعة أخطاء المعالجة التعليق المطلوب. لا يوجد

3.3.2 رد القابل على دعوى ما قبل التحكيم

يجوز للجهة القابلة اتخاذ أحد الإجراءات التالية ردًا على استلام دعوى تحكيم:

- الموافقة على التحكيم، وبالتالي المسؤولية المالية للمعاملة المتنازع عليها.
- رفض دعوى التحكيم.
- عدم اتخاذ أي إجراء.

يجوز للجهة القابلة رفض دعوى ما قبل التحكيم لأحد الأسباب التالية:

- إذا كان إنشاء رد المبالغ المدفوعة الأصلي غير صالح.
- إذا كانت دعوى ما قبل التحكيم باطلة. على سبيل المثال، المستندات المطلوبة غير الملائمة، أو قدمت جهة الإصدار دعوى ما قبل التحكيم بعد الإطار الزمني المعمول به.
- إذا كان التاجر يمتلك دليل نفي، يتناول على وجه التحديد المستندات المقدمة في مرحلة ما قبل التحكيم. يتضمن على سبيل المثال، المعاملة المتنازع عليها المصرح بها بشكل صحيح.
- إذا غيّرت جهة الإصدار سبب رد المبالغ المدفوعة: عالج رفض رد المبالغ المدفوعة عملية رد المبالغ المدفوعة الأصلية ولم يحدد إمكانية رد المبالغ المدفوعة الجديدة الصالحة على أنها متوفرة.

المستندات المطلوبة. عندما يرفض القابل دعوى التحكيم ، فإنه يجب عليه تقديم تفسيراً للرفض وأي مستندات ذات صلة تتناول على وجه التحديد المعلومات الواردة في ما قبل التحكيم. التعليق المطلوب. لا يوجد.

4.3.2 تقديم جهة الإصدار لدعوى ما قبل التحكيم

يجوز لجهة الإصدار رفض طلب القابل عن طريق تصعيد ما قبل التحكيم إلى التحكيم. فقد لا يتم تقديم مستندات جديدة. تحال الدعوى إلى هيئة التحكيم للبت فيها نهائياً.

5.3.2 عملية مراجعة مشغل شبكة الدفع المحلية

سيرفض مشغل شبكة الدفع المحلية الحكم في حالة لم تتبع جهة الإصدار جميع متطلبات التسجيل. تتضمن أمثلة الملفات غير الصحيحة على سبيل المثال الحالات التالية:

- The case has insufficient documentation to enable National Scheme Operator to rule on the case and assign responsibility for the disputed amount.
- The case was filed beyond the appropriate filing period.

The Issuer may resubmit a case that has been declined for ruling when the Issuer can correct the deficiency that caused the case to be declined within the applicable filing time frames.

National Scheme Operator will review the case, the applicable rules, and render a decision. The National Scheme Operator decision in final.

2.4 Compliance / Non Compliance

A Member may ask National Scheme Operator to resolve a rules violation causing financial loss through a compliance case.

A Member may file a compliance case when all of the following conditions have been met.

- Another Member, whether directly or indirectly, has violated any of the rules directly causing another Member to experience a financial loss.

The Filing Member must document a financial loss because of the violation and not simply assert a violation as a basis for filing the case. In other words, the loss could have been avoided had the Filed-Against Member followed the rules.

- The Filing Member submitted a pre-compliance case.
- The Filed-Against Member did not accept responsibility for the pre-compliance case.

A compliance case must not be filed:

- When a chargeback creation or rejection is available
- When a chargeback creation or rejection is prohibited
- For a claim that a Cardholder was credited twice (once by the Issuer as a result of a chargeback and again through a refund processed by the Merchant); the matter must be resolved during the chargeback and arbitration process.

2.4.1 Missing, Invalid or Inaccurate Authorization Data

Pre-compliance Condition. An Issuer may file a pre-compliance case against an Acquirer when both of the following:

- Any of the mandatory or optional data elements supplied in the authorization request message are missing, invalid or inaccurate.
- The Issuer suffered a financial loss directly due to the violation.

Pre-compliance Time Frame. At least 30 calendar days prior to escalating the pre-compliance case to a compliance case.

Pre-compliance Required Documents. All the following:

- Unique Reference Number (DE 57)
- Merchant name
- Transaction date
- Transaction amount
- Name of rule violation
- Violation date
- The specific authorization data asserted to be missing, invalid, or inaccurate.

- في الحالة التي لا تحتوي على مستندات كافية لتمكين مشغل شبكة الدفع المحلية من الحكم في المنازعة، وتحديد المسؤولية عن المبلغ المتنازع عليه.
 - إذا تم رفع المنازعة بعد انقضاء الميعاد المقرر لها.
- يجوز لجهة الإصدار إعادة إرسال حالة تم رفضها للحكم عندما يمكنها تصحيح النقص الذي تسبب في رفض الحالة خلال المواعيد المحددة للإيداع المعمول بها.
- ويجب على مشغل شبكة الدفع المحلية القيام بمراجعة الحالة والقواعد المعمول بها وإصدار قرار بذلك، ويكون قراره نهائياً.

4.2الامتثال / عدم الامتثال

يجوز للعضو أن يطلب من مشغل شبكة الدفع المحلية حل مشكلة انتهاك القواعد الذي يتسبب في خسارة مالية من خلال حالة الامتثال.

يجوز للعضو رفع منازعة امتثال عند استيفاء جميع الشروط التالية.

- أن يقوم عضو آخر بانتهاك هذه القواعد، بشكل مباشر أو غير مباشر، مما تسبب بشكل مباشر في تعرض عضو آخر لخسارة مالية.
- يجب على العضو المتقدم إثبات الخسارة المالية، بسبب هذا الانتهاك وليس مجرد تأكيد الانتهاك كأساس لرفع الدعوى. وبعبارة أخرى ، كان من الممكن تجنب الخسارة لو أن العضو المدعى عليه قد اتبع القواعد.
- أن يكون العضو صاحب الشكوى قد قدم حالة ما قبل الامتثال.
- أن يكون العضو المقدم ضده هذا الادعاء، لم يعلن مسؤوليته عن حالة الامتثال المسبق.

يجب عدم رفع دعوى الامتثال:

- عندما يتوفر إنشاء رد المبالغ المدفوعة أو الرفض.
- عندما يتم حظر إنشاء أو رفض المبالغ المدفوعة.
- للمطالبة بأن حامل البطاقة قد تم قيده مرتين (مرة واحدة من قبل جهة الإصدار كنتيجة لرد المبالغ المدفوعة ومرة أخرى من خلال إعادة الأموال التي قام التاجر بمعالجتها) ؛ يجب حل المسألة أثناء عملية رد المبالغ المدفوعة عن طريق التحكيم.

1.4.2 بيانات التفويض مفقودة أو غير صحيحة أو غير دقيقة

شرط الامتثال المسبق. يجوز لجهة الإصدار رفع دعوى امتثال مسبق، ضد جهة قابلة عند وقوع الحالتين التاليين:

- إذا كانت عناصر البيانات الإلزامية أو الاختيارية المتوفرة في رسالة طلب التفويض مفقودة أو غير صالحة أو غير دقيقة.
 - إذا لحقت بجهة الإصدار خسارة مالية مباشرة بسبب الانتهاك.
- الإطار الزمني. ما لا يقل عن 30 يومًا تقويميًا قبل التمسك بحالة الامتثال المسبق إلى حالة الامتثال. المستندات المطلوبة للامتثال المسبق. كل ما يلي:

- رقم مرجعي مميز (DE 57)
- اسم التاجر.
- تاريخ المعاملة.
- قيمة مبلغ التحويل.
- تحديد القاعدة التي لم يتم الامتثال لها.
- تاريخ المخالفة.
- بيانات التفويض المحددة التي تم التأكيد على أنها مفقودة أو غير صالحة أو غير دقيقة.

- Documentation confirming that the authorization data, as received, misrepresented the nature of the Transaction
- Documentation explaining why the missing, invalid, or inaccurate authorization data resulted in the Transaction being authorized.
- Documentation explaining why the Transaction would not have been authorized if complete, valid, and accurate data had been received
- Documentation proving, to the satisfaction of National Scheme Operator, that the Issuer would not have suffered the financial loss had the mandatory authorization data been present, valid, and accurate and that the filing was not based solely on the data being missing, invalid, or inaccurate.

Compliance Condition. An Issuer may escalate the pre-compliance case to a compliance case when the pre-compliance case is rejected. No new information may be provided.

Compliance Time Frame. Within 120 calendar days of the Transaction processing date or rule violation date.

2.4.2 Inaccurate Clearing Data that Restricts Chargeback Cycles

Pre-compliance Condition. Both of the following:

- An Issuer or Acquirer may file a pre-compliance case when the clearing data in the presentment message or any subsequent chargeback cycle was inaccurate, causing a valid chargeback cycle (chargeback creation, chargeback rejection, or arbitration) to be rejected by the network or unable to be processed by the Member. This includes when a Merchant was improperly identified in the clearing records as ACS capable.

As used herein, “inaccurate” means data that does not accurately reflect the conditions that were present at the point of interaction at the time a Transaction occurred or that does not match data provided in the original presentment.

- The Filing Member suffered a financial loss directly due to the violation.

Pre-compliance Time Frame. At least 30 calendar days prior to escalating the pre-compliance case to a compliance case.

Pre-compliance Required Documentation.

When the Filing Member is the Issuer:

- Unique Clearing Reference Number
- Merchant name
- Transaction date
- Transaction amount
- Name of rule violation
- Violation date
- Document the data elements causing, or that will cause, the chargeback to be rejected.
- Identifying the values the Issuer believes should have been provided in the authorization or clearing messages.
- Specify the chargeback reason and provide the required documentation as set forth in the applicable message reason code.

When the Filing Member is the Acquirer:

- Unique Clearing Reference Number
- Merchant name
- Transaction date
- Transaction amount

- المستندات التي تؤكد أن بيانات التفويض، كما وردت، غير من طبيعة المعاملة.
- المستندات التي تثبت سبب فقدان بيانات التفويض أو عدم صلاحيتها أو عدم دقتها مما أدى إلى الموافقة على المعاملة.
- المستندات التي تثبت سبب عدم الموافقة على المعاملة إذا تم استلام بيانات كاملة وصحيحة ودقيقة.
- مستند يثبت، لمشغل شبكة الدفع المحلية، أن جهة الإصدار لن تلحقها خسارة مالية لو كانت بيانات التفويض الإلزامية موجودة وصالحة ودقيقة، وأن التسجيل لم يكن مبنياً فقط على البيانات المفقودة وغير الصالحة، أو غير الدقيقة .

شرط الامتثال: يجوز لجهة الإصدار التمسك بحالة الامتثال المسبق إلى حالة الامتثال إذا تم رفض حالة الامتثال المسبق. لا يُشترط توفير معلومات جديدة.

الإطار الزمني. في غضون 120 يومًا تقويمياً من تاريخ تسوية المعاملة أو تاريخ انتهاك القاعدة.

2.4.2. بيانات المقاصة غير الدقيقة التي تقيد دورات رد المبالغ المدفوعة.

شرط الامتثال المسبق. كلا ما يلي:

يجوز لجهة الإصدار أو القابل رفع دعوى امتثال مسبق

- إذا كانت بيانات المقاصة في رسالة عرض التقديم أو أي دورة لاحقة لرد المبالغ المدفوعة غير دقيقة، مما يتسبب في رفض عملية دورة صحيحة لرد المبالغ المدفوعة (إنشاء رد المبالغ المدفوعة أو رفض رد المبالغ المدفوعة أو التحكيم) من قبل الشبكة أو أن العضو غير قادر على معالجتها. ويكون ذلك، عندما يتم تحديد التاجر بشكل غير صحيح في سجلات المقاصة على أنه قادر على إدارة خدمات التأمين.

وتشير عبارة “غير دقيقة” إلى أن البيانات لا تعكس بدقة الظروف التي كانت موجودة في نقطة التفاعل في وقت حدوث المعاملة، أو كانت لا تتطابق مع البيانات المقدمة في العرض الأصلي.

- أن يكون العضو المشتكي قد لحقته، خسارة مالية مباشرة بسبب الانتهاك.

الإطار الزمني. ما لا يقل عن 30 يومًا تقويمياً قبل تصعيد حالة الامتثال المسبق إلى حالة الامتثال.

المستندات المطلوبة للامتثال المسبق

عندما يكون العضو القائم بالإيداع هو جهة الإصدار:

- الرقم المرجعي الفريد للمقاصة.
- اسم التاجر.
- تاريخ المعاملة.
- قيمة مبلغ التحويل.
- تحديد القاعدة التي لم يتم الامتثال لها.
- تاريخ المخالفة.
- إثبات عناصر البيانات التي تتسبب في رفض رد المبالغ المدفوعة أو التي ستؤدي إليه.
- تحديد القيم النقدية التي تعتقد جهة الإصدار أنه كان يجب توفيرها في التفويض أو مسح الرسائل.
- تم تحديد سبب رد المبالغ المدفوعة، وتقديم المستندات المثبتة على النحو المبين في رمز سبب الرسالة المعمول به.

عندما يكون العضو القائم بالإيداع هو القابل:

- الرقم المرجعي الفريد للمقاصة.
- اسم التاجر.
- تاريخ المعاملة.
- قيمة مبلغ التحويل.

- Name of rule violation
- Violation date
- Document the data elements causing the reject and provide the valid values as submitted in the authorization or clearing message.
- Provide a valid remedy to the chargeback as set forth in the applicable message reason code.

Compliance Condition. The Filing Member may escalate the pre-compliance case to a compliance case when the pre-compliance case is rejected. No new information may be provided.

Compliance Time Frame. Within 120 calendar days of the Transaction processing date or rule violation date.

2.4.3 Interchange Reimbursement Fee

Pre-compliance Condition. Both of the following:

- The Issuer can document that an Acquirer improperly applied an interchange rate to one or more Transactions
- The Filing Member suffered a financial loss directly due to the violation

Pre-compliance Time Frame. At least 30 calendar days prior to escalating the pre-compliance case to a compliance case

Pre-compliance Required Documents. All of the following:

- Processing date
- Unique Clearing Reference Number
- Documentation detailing the incorrect interchange rate that was applied to the Transaction(s)
- Documentation detailing the correct interchange rate that should have been applied to the Transaction(s)
- Documentation explaining the Issuer’s claim that interchange was applied incorrectly

Compliance Condition. The Issuer may escalate the pre-compliance case to a compliance case when the pre-compliance case was rejected. No new information may be provided.

Compliance Time Frame. Within 120 calendar days of the Transaction processing date or rule violation date.

2.4.4 All Other Rules Violations

Pre-compliance Condition. Both of the following:

- A rule was violated
- The Filing Member suffered a financial loss directly due to the violation

Pre-compliance Time Frame. At least 30 calendar days prior to escalating the pre-compliance case to a compliance case

Pre-compliance Required Documents. All of the following:

- Unique Clearing Reference Number
- Merchant name
- Transaction date
- Transaction amount
- Name of rule violation
- Violation date
- Documentation explaining how the rule violation caused the financial loss.

- تحديد القاعدة التي لم يتم الامتثال لها.

- تاريخ المخالفة.

- إثبات عناصر البيانات التي تتسبب في رفض رد المبالغ المدفوعة أو التي ستؤدي إليه.

- استخدام طريقة صالحة لرد المبالغ المدفوعة على النحو المنصوص عليه في رمز سبب الرسالة المعمول به.

شرط الامتثال. يجوز للعضو المطالب بالامتثال، التمسك بحالة الامتثال المسبق إلى حالة الامتثال عندما يتم رفض حالة الامتثال المسبق. لا يُشترط توفير معلومات جديدة.

الإطار الزمني للامتثال. في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة أو تاريخ انتهاك القاعدة.

3.4.2 رسوم السداد المتبادل

شرط الامتثال المسبق. كل مما يلي:

- يجوز لجهة الإصدار أن تثبت قيام القابل بتطبيق سعر تبادل بشكل غير صحيح على معاملة واحدة أو أكثر

- أن يكون العضو المدعي قد لحقته خسارة مالية بسبب عدم امتثال عضو آخر لقواعد الامتثال.

الإطار الزمني للامتثال المسبق. ما لا يقل عن 30 يومًا تقويميًا قبل تصعيد حالة الامتثال المسبق إلى حالة الامتثال

المستندات المطلوبة للامتثال المسبق. كل ما يلي:

- تاريخ المعاملة.
- رقم مرجعي مميز للمقاصة.
- مستندات توضح بالتفصيل معدل التبادل غير الصحيح الذي تم تطبيقه على المعاملة (المعاملات).
- مستندات توضح بالتفصيل معدل التبادل الصحيح الذي كان ينبغي تطبيقه على المعاملة (المعاملات).
- مستندات توضح ادعاء جهة الإصدار بأن التبادل قد تم تطبيقه بشكل غير صحيح.

شرط الامتثال. يجوز لجهة الإصدار تصعيد حالة الامتثال المسبق إلى حالة الامتثال عندما يتم رفض حالة الامتثال المسبق. قد لا يتم توفير معلومات جديدة.

الإطار الزمني للامتثال. في غضون 120 يومًا تقويميًا من تاريخ تسوية المعاملة أو تاريخ انتهاك القاعدة.

4.4.2 جميع انتهاكات القواعد الأخرى

شرط الامتثال المسبق. كلا ما يلي:

- أن يكون هناك عدم الالتزام بإحدى قواعد الامتثال.

- أن يكو العضو المدعي قد لحقته خسارة مالية بسبب عدم امتثال عضو آخر لقواعد الامتثال.

الإطار الزمني للامتثال المسبق. ما لا يقل عن 30 يومًا تقويميًا قبل تصعيد حالة الامتثال المسبق إلى حالة الامتثال.

المستندات المطلوبة للامتثال المسبق. كل ما يلي:

- رقم مرجعي فريد للمقاصة
- اسم التاجر
- تاريخ المعاملة
- قيمة التحويل
- اسم انتهاك القاعدة
- تاريخ المخالفة
- مستندات تثبت أن مخالفة القواعد قد تسببت في الخسارة المالية.

Compliance Condition. An Issuer or Acquirer may escalate the pre-compliance case to a compliance case when the pre-compliance case was rejected. No new information may be provided.

Compliance Time Frame. Within 120 calendar days of the Transaction processing date or rule violation date.

2.4.5 National Scheme Operator Review Process

Following same procedures forementioned in point 2.3.5 as a standard process that would be followed by the National Scheme Operator for any Non Compliance or being not abided to the rules.

Regulatory Rules of The Libyan National Payment Scheme

Chapter 3 – Interchange and Pricing

This chapter contains the rules on fees that pass from Member to Member, such as interchange and service fees, and on fees paid by Members to the National Scheme Operator.

3.1 Fee Types

An interchange fee is the fee that passes between the Acquirer and the Issuer with respect to a Transaction conducted at a Merchant, the “purchase” part of a “purchase with cash back” Transaction or a Merchandise Transaction conducted at an ATM, including a chargeback, second presentment and reversal of such a Transaction.

A service fee is the fee that passes between the Acquirer and the Issuer with respect to any other type of Transaction, including a Manual Cash Disbursement Transaction, ATM Transaction, the “cash-back” part of a “purchase with cash back” Transaction, or refund, including a chargeback, second presentment and reversal of such a Transaction.

A scheme fee is a fee that a Member pays to the National Scheme Operator with respect to its participation in and use of the payment scheme.

3.2 Interchange and Service Fees

3.2.1 Interchange Reimbursement Fees – Overview

A Transaction settled between Members gives rise to the payment of the appropriate interchange fee or service fee, as applicable.

Refer to section 3.3 for more detailed information.

3.2.2 Scheme Determines Interchange Reimbursement Fees Rates

The National Scheme Operator has the right to establish interchange fees and service fees (hereafter referred to as “interchange fees,” “service fees,” or collectively, “fees”).

The National Scheme Operator shall inform Members of all fees that it establishes and shall periodically publish fee tables.

No members should be eligible to make any bilateral agreements

شرط الامتثال. يجوز لجهة الإصدار أو القابل تصعيد حالة الامتثال المسبق إلى حالة امتثال عندما يتم رفض حالة الامتثال المسبق. لا يُشترط توفير معلومات جديدة.

الإطار الزمني للامتثال. في غضون 120 يومًا تقويمياً من تاريخ تسوية المعاملة أو تاريخ انتهاك القاعدة.

5.4.2 عملية مراجعة مشغل شبكة الدفع المحلية

اتباع نفس الإجراءات المذكورة في النقطة 5.3.2 كعملية قياسية يتبعها مشغل شبكة الدفع المحلية لحالات عدم امتثال أو عدم الالتزام بالقواعد.

القواعد التنظيمية شبكة الدفع المحلية الليبية

الفصل 3 – التبادل والتسعير

يحتوي هذا الفصل على قواعد انتقال الرسوم من عضو إلى عضو ، مثل رسوم التبادل والخدمة، والرسوم التي يدفعها الأعضاء لمشغل شبكة الدفع المحلية.

1.3 أنواع الرسوم

رسوم التبادل هي الرسوم التي يتم تمريرها بين القابل وجهة الإصدار فيما يتعلق بالمعاملة التي يتم إجراؤها لدى التاجر، أو جزء “الشراء” من معاملة “الشراء باسترداد نقدي” أو معاملة البضائع التي يتم إجراؤها في جهاز الصراف الآلي، بما في ذلك استرداد المبالغ المدفوعة، التقديم الثاني وعكس هذه المعاملة.

رسوم الخدمة هي الرسوم التي يتم تمريرها بين القابل وجهة الإصدار فيما يتعلق بأي نوع آخر من المعاملات، بما في ذلك معاملة الدفع النقدي اليدوي، ومعاملة الصراف الآلي، وجزء “استرداد النقود” من معاملة “الشراء باسترداد نقدي”، أو استرداد، بما في ذلك رد المبالغ المدفوعة، التقديم الثاني وعكس هذه المعاملة.

رسم الشبكة هو الرسم الذي يدفعه العضو لمشغل شبكة الدفع المحلية فيما يتعلق بمشاركته في نظام الدفع واستخدامه.

2.3 رسوم التبادل والخدمة

1.2.3 رسوم سداد التبادل - نظرة عامة

تؤدي المعاملة التي تتم تسويتها بين الأعضاء إلى دفع رسوم التبادل أو رسوم الخدمة المناسبة، عند الاقتضاء.

راجع القسم 3.3 للحصول على معلومات أكثر تفصيلاً.

2.2.3 يحدد النظام معدلات رسوم السداد التبادلية.

يحق لمشغل شبكة الدفع المحلية تحديد رسوم التبادل ورسوم الخدمة (يشار إليها فيما يلي باسم “رسوم التبادل” أو “رسوم الخدمة” أو “الرسوم” بشكل جماعي).

يجب على مشغل شبكة الدفع المحلية إبلاغ الأعضاء بجميع الرسوم التي يحددها ونشر جداول الرسوم بشكل دوري.

يجب ألا يُسمح لأي من الأعضاء بعقد أي اتفاقيات ثنائية

3.2.3 Cost Studies

(Category A)

The National Scheme Operator has the right to conduct one or more cost studies for the purpose of establishing interchange and service fees.

In order to ensure a sufficient quantity and level of data quality and representativeness, the National Scheme Operator has the right to designate any number of Members to participate in cost studies. Each Member so designated is required to participate and must provide and be able to certify that it has provided the National Scheme Operator or its agent with complete and accurate information in the form and manner requested and for such period of time and by the specified date.

3.2.4 Allocation of Expenses

The National Scheme Operator has the right to allocate expenses related to any cost study among Members conducting the Activity that is the subject of the cost study. The expenses may be allocated as the National Scheme Operator deems appropriate and the decision of the National Scheme Operator is binding on all Members.

3.2.5 Compliance with a Cost Study

(Category A)

A Member designated to participate in a cost study that fails to fully and timely participate is subject to noncompliance assessments and other disciplinary action as determined by the National Scheme Operator.

For the Non-Compliance fees , please refer to the early stated fees within Chapter-2 Compliance.

3.3 Interchange Reimbursement Fees Overview

Interchange and service fees may have varying rates and structures.

The amount of the fee may depend on a number of factors, including but not limited to the following:

- The type of Card product used (debit, prepaid, commercial)
- The mode of acquisition (such as chip, e-commerce, contactless)
- How rapidly the Transaction is cleared
- The category of Merchant accepting the transaction (such as supermarket, hotel, restaurant)
- The type of Terminal (such as chip-capable, magnetic stripe-only, contactless-enabled)
- The type of Merchant Category Code.

The combination of Card product and Transaction type gives an interchange or service fee “program.” For example, for a debit card accepted at a retail location, the debit POS interchange program would be applied.

3.3.1 Fee Tiers

Within each interchange program there may be a number of fee “tiers,” each of which corresponds to the level of security of the transaction, the type of terminal used, and so on.

For example, if the card is accepted at a chip-capable terminal with PIN pad, the chip fee tier is applied.

Each fee tier within a program may have a different fee rate.

3.2.3 دراسات التكلفة

(الفئة أ)

يجوز لمشغل شبكة الدفع المحلية إجراء دراسة أو أكثر للتكلفة من أجل تحديد رسوم التبادل والخدمة.

إضافة إلى ذلك فإنه يجوز مشغل شبكة الدفع المحلية من أجل ضمان كمية ومستوى كافيين من جودة البيانات والتمثيل، اختيار عدد من الأعضاء للمشاركة في دراسات التكلفة. يُطلب من كل عضو تم اختياره أن يقوم بهذه الدراسات بشكل دقيق ، وأن يشهد انه قد قدم المطلوب لمشغل الشبكة أو عميل المشغل خلال المدة الزمنية المطلوب منه إجراء الدراسة خلالها.

4.2.3 تخصيص المصروفات

يجوز لمشغل شبكة الدفع المحلية تخصيص النفقات المتعلقة بدراسة التكلفة بين الأعضاء الذين يقومون بالنشاط الذي هو موضوع دراسة التكلفة. ويتم تخصيص النفقات وفقًا لما يراه مشغل شبكة الدفع المحلية مناسبًا ويكون قراره ملزمًا لجميع الأعضاء.

5.2.3 الامتثال لدراسة التكلفة

(الفئة أ)

يخضع العضو المختار للمشاركة في دراسة التكلفة التي لم تنجح في المشاركة الكاملة، وفي الوقت المناسب لتقييم عدم الامتثال والإجراءات التأديبية الأخرى على النحو الذي يحدده مشغل شبكة الدفع المحلية.

بالنسبة لرسوم عدم الامتثال، يجب الرجوع إلى الرسوم المشار إليها سابقاً ضمن الامتثال للفصل الثاني.

3.3 نظرة عامة على رسوم سداد التبادل

قد يتم تحديد قيمة رسوم التبادل والخدمة بأسعار وطرق مختلفة.

قد يعتمد مبلغ الرسوم على عدد من العوامل، بما في ذلك على سبيل المثال لا الحصر ما يلي:

- نوع بطاقة المنتج المستخدمة (الخصم، مسبق الدفع ، تجارية).
- طريقة الاستحواذ (مثل الشريحة، التجارة الإلكترونية، عن بعد).
- مدى سرعة تصفية المعاملة.
- فئة التاجر الذي يقبل المعاملة (مثل سوبر ماركت، فندق، مطعم)
- نوع الجهاز (مثل قادر على الشريحة، الشريط المغناطيسي فقط ، ممكن عن بعد)
- نوع رمز فئة التاجر.

يعطي الجمع بين منتج البطاقة ونوع المعاملة “برنامج” رسوم خدمة أو تبادل. على سبيل المثال ، بالنسبة لبطاقة الخصم المقبولة في أحد مواقع البيع بالتجزئة، سيتم تطبيق برنامج تبادل نقاط البيع المدين.

1.3.3 مستويات الرسوم

قد يكون هناك عدد من “مستويات” الرسوم داخل كل برنامج تبادل، يتوافق كل منها مع مستوى أمان المعاملة، ونوع المحطة المستخدمة وما إلى ذلك.

على سبيل المثال، إذا تم قبول البطاقة في محطة بها شريحة مزودة بلوحة رقم اتلعراف الشخصي، فسيتم تطبيق فئة رسوم الشريحة.

قد يكون لكل فئة رسوم داخل البرنامج معدل رسوم مختلف

3.3.2 Fee Structure

The structure of the fee may include:

- A percentage of the transaction
- A flat fee amount
- A minimum fee
- A maximum fee
- A combination of the above

3.4 General Interchange Reimbursement Fees Requirements

(Category A)

Acquirers must apply the correct interchange and service fees to Transactions, in accordance with the Interchange Reimbursement Fees programs established by the National Scheme Operator.

Acquirers must submit Transactions completed at Merchants with the Exact interchange fee tier applicable to them.

3.5 Interchange Reimbursement Fees Rates

The interchange and service fees are stated as follows based on the Merchant Discount Rate (MDR) applied:

- National Scheme Operator is XX% of the applied MDR
- Acquirer Bank XX% of the applied MDR
- Issuer Bank XX% of the Applied MDR

3.6 Interchange Reimbursement Fees Programs

The Interchange Reimbursement Fees built with accordance to MDR applied according to each line of business.

3.7 Interchange Reimbursement Fee Adjustments

(Category A)

It is the responsibility of each Member to reconcile the totals and Transactions provided by the National Scheme Operator to its own internal records on a daily basis.

A Member, in the course of its reconciliation, or the National Scheme Operator, may identify an error in the application of interchange or service fees.

When an error is identified, the party that has suffered a corresponding financial loss has the right to recover its loss by filing a compliance case as set out in chapter 11.

If the error is identified by the National Scheme Operator, it has the right to correct the error by appropriately debiting and crediting the settlement accounts of the Acquirers and Issuers involved.

The National Scheme Operator shall Inform the Members involved in writing before making the adjustment. The period covered by an adjustment shall in no case exceed one calendar year. Adjustments are processed in clearing as Fee Collection messages.

3.8 Interchange Reimbursement Fee-related Fines

The National Scheme Operator has the right to assess fines in case a Member is found to have intentionally or negligently applied incorrect interchange or service fees to Transactions. The fines may be up to three times the benefit which the Member derived from applying the incorrect fees.

2.3.3 هيكل الرسوم

قد يشمل هيكل الرسوم ما يلي:

- نسبة من المعاملة.
- مبلغ رسم مقطوع.
- حد أدنى للرسوم.
- الحد الأقصى للرسوم.
- مزيج مما ذكر أعلاه.

4.3 المتطلبات العامة لسداد رسوم التبادل

(الفئة أ)

يجب على القابلين تطبيق رسوم التبادل والخدمات الصحيحة على المعاملات، وفقاً لبرامج رسوم سداد التبادل التي وضعها مشغل شبكة الدفع المحلية.

يجب على القابلين إرسال المعاملات المكتملة لدى التجار مع فئة رسوم التبادل المطبقة عليهم.

5.3 معدلات رسوم سداد التبادل

يتم تحديد رسوم التبادل والخدمة على النحو التالي بناءً على معدل خصم التاجر (MDR) المطبق:

- مشغل شبكة الدفع المحلية هو XX% من معدل خصم التاجر MDR المطبق.
- مصرف القابل XX% من معدل خصم التاجر MDR المطبق.
- مصرف جهة الإصدار XX% من معدل خصم التاجر MDR المطبق.

6.3 برامج رسوم السداد التبادلية

رسوم السداد التبادلية المبنية وفقاً لمعايير معدلات خصم التاجر MDR المطبقة وفقاً لكل خط عمل.

7.3 تعديلات رسوم السداد التبادلية

(الفئة أ)

يتحمل كل عضو مسؤولية التوفيق بين المجاميع والمعاملات التي يوفرها مشغل شبكة الدفع المحلية مع السجلات الداخلية الخاصة به على أساس يومي.

يجوز للعضو، في سياق التسوية الخاصة به، أو لمشغل شبكة الدفع المحلية، تحديد الخطأ في تطبيق رسوم التبادل أو الخدمة.

عند تحديد هذا الخطأ، يجوز للطرف الذي لحقته خسارة مالية مقابلة، المطالبة باسترداد ما يعادل خسارته عن طريق رفع طلب امتثال على النحو المبين في الفصل 11.

إذا تم تحديد الخطأ بواسطة مشغل شبكة الدفع المحلية، فيجوز له تصحيح الخطأ عن طريق الخصم والاعتماد بشكل مناسب من حسابات التسوية الخاصة بالقابلين وجهات الإصدار المعنيين.

يجب على مشغل شبكة الدفع المحلية إبلاغ الأعضاء المشاركين كتابةً قبل إجراء التعديل. ويجب ألا تتجاوز الفترة التي يغطيها التعديل بأي حال من الأحوال سنة تقويمية واحدة تتم تسوية التعديلات في المقاصة كرسائل تحصيل الرسوم.

8.3 الغرامات المتعلقة بدفع رسوم التبادل

يجوز لمشغل شبكة الدفع المحلية تقييم الغرامات في حالة اكتشاف أن العضو قد قام عن قصد أو عن طريق الخطأ بتطبيق رسوم تبادل أو خدمة غير صحيحة على المعاملات. وقد تصل قيمة الغرامات إلى ثلاثة أضعاف الفائدة التي يجنيها العضو من تطبيق الرسوم غير الصحيحة.

3.9 Member Fee Collection and Funds Disbursement

(Category C)

The National Scheme Operator has the right to establish Member-to-Member fees other than interchange and service fees, for example, “good-faith” acceptance fees, card capture fees and merchant rewards. The Member to which such a fee is owed collects the fee from the other Member by submitting a Fee Collection message.

A Member-to-Member fee must be collected within [XX] months of the event that is the basis for the fee.

3.10 Fee Collection

(Category C)

A fee collection is a clearing-only message. The reason for the fee collection must be indicated with by appropriate code in the message. Refer to book 1 for more information on fee collection messages.

If the fee collection message requires supporting documentation, the message originator must send the documentation in the manner specified by the National Scheme Operator. The message originator should label the documentation in order to allow the receiving Member to readily match the documentation to the applicable message and/or Transaction.

3.11 SCHEME FEES

3.11.1 Scheme Fees – General

(Category A)

Each Member is responsible to timely pay to the National Scheme Operator all fees, charges, assessments and the like applicable to Activity that are in effect from time to time, including those set forth in the applicable National Scheme Operator billing manual.

If a Member does not timely pay the National Scheme Operator or any other person any amount due under the Standards, then the National Scheme Operator has the right, immediately and without providing prior notice to the Member, to assess and collect from that Member, on a current basis as the National Scheme Operator deems necessary or appropriate, such amount, as well as the actual attorneys’ fees and other costs incurred by the National Scheme Operator in connection with any effort to collect such amount from that Member.

The National Scheme Operator has the right to assess and collect such amount at any time after the applicable amount becomes due, by any means available to the National Scheme Operator, which shall specifically include, by way of example and not limitation:

- The taking or setoff of funds or other assets of the Member held by the National Scheme Operator;
- The taking or setoff of funds from any account of the Member upon which the National Scheme Operator is authorized to draw;
- The taking of funds being paid by the Member to any other Member; and
- The taking of funds due to the Member from any other Member.

Each Member expressly authorizes the National Scheme Operator to take the Member’s funds and other assets as authorized by this Rule, and to apply such funds and other assets

9.3 تحصيل رسوم الأعضاء وصرف الأموال

(الفئة ج)

يجوز لمشغل شبكة الدفع المحلية تحصيل رسوم من عضو إلى عضو بخلاف رسوم التبادل والخدمة، على سبيل المثال، رسوم قبول “حسن النية” ورسوم الحصول على البطاقة ومكافآت التاجر. ويقوم العضو الدائن بهذه الرسوم بتحصيل الرسوم من العضو الآخر عن طريق إرسال رسالة تحصيل الرسوم. يجب تحصيل الرسوم من عضو إلى عضو في غضون [XX] شهرًا من تاريخ الواقعة التي تمثل أساس الرسوم.

10.3 تحصيل الرسوم

(الفئة ج)

تحصيل الرسوم هو رسالة مقاصة فقط، وتجب الإشارة إلى سبب تحصيل الرسوم بالرمز المناسب في الرسالة. الرجوع إلى الكتاب 1 لمزيد من المعلومات حول رسائل تحصيل الرسوم. إذا كانت رسالة تحصيل الرسوم تتطلب مستندات مؤيدة، فيجب على مُنشئ الرسالة إرسال المستندات بالطريقة المحددة بواسطة مشغل شبكة الدفع المحلية. ويجب عليه كذلك، أن يقوم بتصنيف المستندات من أجل السماح للعضو المستلم بمطابقة هذه المستندات بسهولة مع الرسالة و/ أو المعاملة السارية.

11.3 رسوم الشبكة

1.11.3 رسوم الشبكة – عام

(الفئة أ)

كل عضو مسؤول عن دفع جميع الرسوم والتكاليف والتقييمات وما شابه ذلك المطبقة على النشاط الساري من وقت لآخر، بما في ذلك تلك المنصوص عليها في دليل فوترة مشغل شبكة الدفع المحلية المعمول به.

إذا لم يدفع العضو لمشغل شبكة الدفع المحلية أو أي شخص آخر أي مبلغ مستحق بموجب المعايير في الوقت المناسب، فيجوز لمشغل شبكة الدفع المحلية، فورًا ودون تقديم إخطار مسبق إلى العضو، اتخاذ إجراءات تقييم وتحصيل مثل هذا المبلغ من ذلك العضو ، بتاريخ أساس حالي كما يقدره مشغل شبكة الدفع المحلية ضروريًا أو مناسبًا ، بالإضافة إلى أتعاب المحاماة الفعلية والتكاليف الأخرى التي يتكبدها مشغل شبكة الدفع المحلية فيما يتعلق بجهود تحصيل هذا المبلغ من ذلك العضو.

يجوز لمشغل شبكة الدفع المحلية تقدير وتحصيل هذا المبلغ في أي وقت، عندما يكون هذا المبلغ مستحق الأداء، وبأي وسيلة متاحة لمشغل شبكة الدفع المحلية ، والتي يجب أن تشمل على وجه التحديد، على سبيل المثال وليس الحصر:

- حجز أو مقاصة الأموال أو الأصول الأخرى للعضو التي يحتفظ بها مشغل شبكة الدفع المحلية.
- حجز الأموال أو مقاصتها من أي حساب للعضو يرخّص لمشغل شبكة الدفع المحلية بالسحب منه.
- حجز الأموال التي يدفعها العضو إلى أي عضو آخر.
- حجز الأموال المستحقة للعضو من أي عضو آخر

ويجب على كل عضو أن يرخّص لمشغل شبكة الدفع المحلية بحجز أموال العضو والأصول الأخرى كما هو مصرح به بموجب هذه القاعدة، وإخضاع هذه الأموال والأصول الأخرى لأي التزام عليه تجاه مشغل شبكة الدفع المحلية أو أي شخص آخر بموجب المعايير، و لا يجوز لأي عضو أن يكون لديه أي

to any obligation of the Member to the National Scheme Operator or any other person under the Standards, and no Member shall have any claim against the National Scheme Operator or any other person in respect of such conduct by the National Scheme Operator.

Each Member agrees upon demand to promptly execute, acknowledge and deliver to the National Scheme Operator such instruments, agreements, lien waivers, releases, and other documents as the National Scheme Operator shall, from time to time, request in order to exercise its rights under this Rule.

For Fees Applied by the Scheme , please refer to Annex (A).

3.11.2 Taxes and Other Charges

(Category A)

Each Member must pay when due all taxes charged by any jurisdiction with respect to its Activity. In the event the National Scheme Operator is charged taxes or other charges by a country or other jurisdiction as a result of or otherwise directly or indirectly attributable to Activity, the Member is obligated to reimburse the National Scheme Operator the amount of such taxes or other charges. The National Scheme Operator has the right to collect such taxes or other charges from the settlement account of the Principal responsible in accordance with the Standards for the Activity that gave rise to the charge.

3.11.3 Scheme Fees – Rates

The scheme fees are indicated as fixed percentage of the collected MDR which is set to be 52% of the applied MDR.

The National Scheme Operator has the right to modify the scheme fees, including deleting and adding fees.

3.11.4 Scheme Fee Collection and Funds Disbursement

The National Scheme Operator collects scheme fees by debiting the Member’s settlement account. The scheme fees are detailed in the corresponding invoice provided by the National Scheme Operator.

3.11.5 Fee Assessment and Responsibility

The National Scheme Operator has the right to suspend, delay, or adjust a Member’s settlement position at any time in order to resolve any errors in scheme fees assessment or payment.

دعوى ضد مشغل شبكة الدفع المحلية أو أي شخص آخر فيما يتعلق بهذا السلوك من قبل مشغل شبكة الدفع المحلية.

يوافق كل عضو عند الطلب على التنفيذ الفوري والإقرار وتسليم مشغل شبكة الدفع المحلية مثل هذه الأدوات والاتفاقيات وإعفاءات الامتياز والإصدارات والمستندات الأخرى التي يطلبها مشغل شبكة الدفع المحلية، من وقت لآخر، من أجل ممارسة حقوقه بموجب هذه القاعدة. لمعرفة الرسوم المطبقة من قبل الشبكة، يرجى الرجوع إلى الملحق (أ).

2.11.3 الضرائب والرسوم الأخرى

(الفئة أ)

يلتزم كل عضو بأن يدفع في تاريخ الاستحقاق جميع الضرائب التي تفرضها القوانين. وفي حال تم فرض ضريبة على المشغل بموجب القانون أو أية رسوم أخرى من قبل بلد أو ولاية قضائية أخرى نتيجة للنشاط أو منسوب إليه بشكل مباشر أو غير مباشر، يكون العضو ملزمًا بسداد مبلغ هذه الضرائب أو الرسوم الأخرى لمشغل شبكة الدفع المحلية. يجوز لمشغل شبكة الدفع المحلية تحصيل هذه الضرائب أو الرسوم الأخرى من حساب التسوية للموكل المسؤول وفقًا لمعايير النشاط الذي أدى إلى فرض الرسوم.

3.11.3 رسوم الشبكة – الأسعار

يشار إلى رسوم الشبكة كنسبة مئوية ثابتة من معدل خصم التاجر MDR المحصل والذي تم تعيينه ليكون 52 ٪ من معدل خصم التاجر MDR المطبق. يجوز لمشغل شبكة الدفع المحلية تعديل رسوم الشبكة، بما في ذلك إلغاء أو إضافة الرسوم.

4.11.3. تحصيل رسوم الشبكة وصرف الأموال

يقوم مشغل شبكة الدفع المحلية بتحصيل رسوم الشبكة عن طريق الخصم من حساب تسوية العضو. ويتم تفصيل رسوم الشبكة في الفاتورة المقابلة المقدمة من قبل مشغل شبكة الدفع المحلية.

5.11.3. تقييم الرسوم والمسؤولية

يجوز لمشغل شبكة الدفع المحلية تعليق أو تأخير أو تعديل موقف تسوية العضو في أي وقت من أجل حل أي أخطاء في تقييم رسوم الشبكة أو دفعها.

Regulatory Rules of The Libyan National Payment Scheme

Chapter 4 – eCommerce and Digital Services

PART I – eCommerce & related service

4.1 Introduction

eCommerce is a term meant by electronic commerce that runs through internet service, eCommerce operates in different types of market segments and can be conducted over computers, tablets, smartphones, and other smart devices. Nearly every imaginable product and service is available through ecommerce transactions, including books, music, plane tickets, and financial services such as stock investing and online banking.

- It is conducted over computers, tablets, smartphones, and other smart devices.
- eCommerce operates in several market segments including business-to-business, business-to-consumer, consumer-to-consumer, and consumer-to-business.

The National Scheme Operator within its' role and assigned tasks by the CBL, have enabled the eCommerce services by establishing the NUMO payment gateway to open new services and expand and to enrich the payment industry in Libya.

The National Scheme Operator has the right to process and to drive the electronic payment services through the National Payment Gateway including ePayment Gateway, electronic commerce, QR code payments & acceptance, and mobile payment services.

4.2 eCommerce Considerations & Eco System Components

Following preset standards released by EMVCo applying the latest supported secured protocols and standards of eCommerce services, the National Scheme Operator in-line with following such rules took the right steps to obtain and to operate the 3D-Secured environment version 2.0 and later versions.

An e-commerce Transaction must not be affected using contactless payment functionality or as a purchase with cash back Transaction.

4.2.1 eCommerce Considerations

Electronic payment services for all NUMO brand can only be processed through the defined Payment Gateway operated and processed by the National Scheme operator, and routed through the National Switchto associated issuing bank.

All working member banks are requested to join and to use the hosted and operated services to accept NUMO brand.

Acquirers Considerations

The following measurements are required and must be considered by the Acquiring banks on-boarding merchants to the ePayment Gateway services, which is hosted and operated by the National Scheme Operator.

القواعد التنظيمية لشبكة الدفع المحلية الليبية

الفصل 4 – التجارة الإلكترونية والخدمات الرقمية

الجزء الأول - التجارة الإلكترونية والخدمات ذات الصلة

1.4. مقدمة

التجارة الإلكترونية هي مصطلح يقصد به التجارة التي تعمل من خلال خدمة الإنترنت، وتعمل التجارة الإلكترونية في أنواع مختلفة من قطاعات السوق ويمكن إجراؤها عبر أجهزة الكمبيوتر والأجهزة اللوحية والهواتف الذكية والأجهزة الذكية الأخرى. ويتوفر كل منتج وخدمة يمكن تخيلها تقريبًا من خلال معاملات التجارة الإلكترونية، بما في ذلك الكتب والموسيقى وتذاكر الطائرة والخدمات المالية مثل الاستثمار في الأسهم والخدمات المصرفية عبر الإنترنت.

- يتم إجراؤه عبر أجهزة الكمبيوتر والأجهزة اللوحية والهواتف الذكية والأجهزة الذكية الأخرى.
- تعمل التجارة الإلكترونية في العديد من قطاعات السوق بما في ذلك قطاع الأعمال، ومن الأعمال إلى المستهلك، ومن المستهلك إلى المستهلك، ومن المستهلك إلى الأعمال.

وقد قام مشغل شبكة الدفع المحلية ضمن دوره والمهام الموكلة إليه من قبل مصرف ليبيا المركزي، بتمكين خدمات التجارة الإلكترونية من خلال إنشاء بوابة الدفع نمو من فتح خدمات جديدة وتوسيع تنمية صناعة الدفع في ليبيا.

يجوز لمشغل شبكة الدفع المحلية معالجة وإدارة خدمات الدفع الإلكتروني من خلال بوابة الدفع المحلية، بما في ذلك بوابة الدفع الإلكتروني والتجارة الإلكترونية ومدفوعات وقبول رمز الاستجابة السريعة وخدمات الدفع عبر الهاتف المحمول.

2.4. اعتبارات التجارة الإلكترونية ومكونات النظام البيئي

وفقًا للمعايير المحددة مسبقًا التي أصدرتها EMVCo والتي تطبق أحدث البروتوكولات والمعايير المؤمنة المدعومة لخدمات التجارة الإلكترونية، اتخذ مشغل شبكة الدفع المحلية ، وبما يتماشى مع هذه القواعد التالية، الخطوات الصحيحة للحصول على الإصدار 2.0 وتشغيله من البيئة الآمنة ثلاثية الأبعاد والإصدارات الأحدث.

يجب ألا تتأثر معاملة التجارة الإلكترونية باستخدام وظيفة الدفع عن بعد أو عملية شراء بمعاملة استرداد نقدي.

1.2.4 اعتبارات التجارة الإلكترونية

لا يمكن معالجة خدمات الدفع الإلكتروني لجميع علامات نمو التجارية إلا من خلال بوابة الدفع المحددة التي يتم تشغيلها ومعالجتها بواسطة مشغل شبكة الدفع المحلية، وتوجيهها من خلال مصرف الإصدار المرتبط بـ Switchto المحلي.

يُطلب من جميع المصارف العضوة العاملة الانضمام واستخدام الخدمات المستضافة والمُدارة لقبول علامة نمو التجارية.

اعتبارات القابليين

القياسات التالية مطلوبة ويجب مراعاتها من قبل المصارف (القابلة) على التجار الذين يعملون على خدمات بوابة الدفع الإلكتروني، والتي يستضيفها مشغل شبكة الدفع المحلية ويديرها.

1. Acquirers must do the proper follow up on their relevant merchants that merchant must not refuse to complete an e-commerce Transaction solely because the Cardholder does not have a digital certificate or other secured protocol.
2. Card verification method for this type of Transaction would be Card number, Expiry date of card and CVV2 in addition to second level of authentication (One Time Password) are the minimum acceptance level to comply with 3D Secure payment standards associated with EMVco. Known rules.
3. Acquirers must ensure that all their merchants are on-boarded on the designated 3DS server.
4. If there is any surcharge or fees is added to the final price, the Cardholder must be informed prior to processing the payment and consent to the additional charge (for example: delivery charges, additional taxes, insurance fees.....etc.)
5. Refund/Cancelation policy must be clearly displayed before processing the Transaction and the Cardholder's acknowledgement of it must be obtained.
6. The PAN must be masked upon entry, last 4 digits only may be displayed.
7. An e-commerce Transaction requires authorization by the Issuer means that it can be processed online based.

Merchant Considerations

The Merchant must display the NUMO Logo on its website where payment methods are listed, the acquirer bank is responsible to avail and to secure the proper setup and branding process needed for such inline with the merchant onboarding process.

Merchant must provide a mailing address and a contact telephone number and/or email address as a channel for customer queries. This information shall be displayed on any page within the Merchant's website, but must be readily accessible to a Cardholder, and remain displayed for at least 90 calendar days after the last day on which a Transaction was performed.

Displaying the price information or fees due to payment, including currency, and the details of the timing of billing and fulfillment of Transactions, and provide a function for Cardholders to confirm a purchase before the completion of the sale.

The Transaction amount used in the authorization message must match the value of the products and services in an individual shipment, including any additional charges for packing and shipment and to be properly communicated to the customer performing the transaction.

If the purchase will be delivered in multiple shipments, the Merchant must notify the Cardholder and ensure that the combined amount of all shipments does not exceed the total purchase amount agreed with the Cardholder. The Merchant must obtain the Cardholder's agreement to any increase in the purchase amount as a result of multiple or partial deliveries. Each shipment, and any increase to the original agreed purchase amount, must be processed by the Merchant as a separate authorized Transaction.

1. يجب أن يقوم القابلون بمتابعة للتجار المعنيين متابعة مناسبة، حيث يجب ألا يرفض التاجر إتمام معاملة التجارة الإلكترونية لمجرد أن حامل البطاقة ليس لديه شهادة رقمية أو بروتوكول آمن آخر.
2. ستكون طريقة التحقق من البطاقة لهذا النوع من المعاملات هي رقم البطاقة وتاريخ انتهاء صلاحية البطاقة و CVV2 بالإضافة إلى المستوى الثاني من المصادقة (كلمة المرور لمرة واحدة) هي الحد الأدنى لمستوى القبول للامتثال لمعايير الدفع الآمنة ثلاثية الأبعاد المرتبطة بقواعد EMVco. المعروفة.
3. يجب أن يتأكد القابلون من أن جميع التجار لديهم موجودون على خادم 3DS المخصص.
4. في حالة إضافة أي رسوم إضافية أو رسوم إلى السعر النهائي، يجب إبلاغ حامل البطاقة قبل معالجة الدفع والموافقة على الرسوم الإضافية (على سبيل المثال: رسوم التوصيل والضرائب الإضافية ورسوم التأمين ... إلخ).
5. يجب عرض سياسة الاسترداد/ الإلغاء، بوضوح قبل معالجة المعاملة، ويجب الحصول على إقرار حامل البطاقة بها.
6. يجب إخفاء رقم الحساب الشخصي (PAN) عند الإدخال، ويمكن عرض آخر 4 أرقام فقط.
7. تتطلب معاملة التجارة الإلكترونية الحصول على تصريح من جهة الإصدار مما يعني أنه يمكن معالجتها عبر الإنترنت.

اعتبارات التاجر

يجب أن يقوم التاجر بعرض شعار نمو على موقعه على الويب، حيث يتم سرد طرق الدفع، ويكون المصرف القابل مسؤولاً عن الاستفادة وتأمين عملية الإعداد المناسبة والعلامة التجارية اللازمة لذلك بما يتماشى مع عملية إعداد التاجر.

يجب أن يقدم التاجر عنوانًا بريديًا ورقم هاتف للاتصال و/ أو عنوان بريد إلكتروني كقناة لاستفسارات العملاء. ويجب عرض هذه المعلومات على أي صفحة داخل موقع التاجر على الويب، و يجب أن تكون متاحة بسهولة لحامل البطاقة، وتظل معروضة لمدة 90 يومًا تقويميًا على الأقل بعد آخر يوم تم فيه إجراء المعاملة.

عرض معلومات السعر أو الرسوم المستحقة الدفع، بما في ذلك العملة ، وتفاصيل توقيت الفواتير وتنفيذ المعاملات ، وتوفير وظيفة لحاملي البطاقات لتأكيد الشراء قبل إتمام البيع.

يجب أن يتطابق مبلغ المعاملة المستخدمة في رسالة التفويض مع قيمة المنتجات والخدمات في الشحنة الفردية، بما في ذلك أي رسوم إضافية للتعبئة والشحن وأن يتم إبلاغ العميل الذي يقوم بالمعاملة بشكل صحيح.

إذا تم تسليم المشتريات في عدة شحنات، يجب على التاجر إخطار حامل البطاقة والتحقق من أن المبلغ الإجمالي لجميع الشحنات لا يتجاوز إجمالي مبلغ الشراء المتفق عليه مع حامل البطاقة. ويجب أن يحصل التاجر على موافقة حامل البطاقة على أي زيادة في مبلغ الشراء نتيجة عمليات التسليم المتعددة أو الجزئية. كما يجب أن تتم معالجة كل شحنة وأي زيادة على مبلغ الشراء الأصلي المتفق عليه بواسطة التاجر كمعاملة منفصلة معتمدة.

If the products or services purchased are not available at time of the Transaction, the Merchant must inform the Cardholder and obtain the Cardholder's agreement to a delayed delivery (specifying the anticipated delivery date) before proceeding with the Transaction.

The Merchant must advise the Cardholder if the products or services ordered will not be delivered within the time frame originally disclosed to and agreed with the Cardholder.

The Cardholder must be notified of the new anticipated delivery timeframe and given an opportunity to cancel the Transaction.

The information provided on any email acknowledgment of the Cardholder's order must comply with the Transaction receipt requirements described in this chapter.

Issuer Considerations

1. All Issuer banks of NUMO brand must ensure that their issued cards are registered at the National Scheme Operator and their details are accurate and updated.
2. Issuers will be responsible for fraudulent trials that did not follow the 3D secure rules by verifying the additional information submitted through the ACS stating that cardholder did not succeed to verify authentication.

4.2.2 Eco System Components

(See appendix number 28)

3DS Server & Payment Gateway

The National Scheme Operator should availed the 3DS server which is the part used by the acquirers and manage through it the on-boarding of their related merchants, availing the 3DS Client which is the consumer-facing component allowing consumer interaction with the 3DS Requestor for initiation of the EMV 3-D Secure protocol.

The National Scheme operator can license a 3DS integrator which acts as 3-D Secure participant that facilitates and integrates the 3DS Requestor Environment, and optionally facilitates integration between the Merchant and the Acquirer.

The national payment gateway serves as the front channel for the electronic payments conducted by customers and can be configured to be associated with Merchant web page through adjustable branding features.

All the Acquirers licensed for electronic payment acceptance are requested to be part of the 3D secured services for NUMO and they need to apply for this through the National Scheme Operator to conduct the required certification and registration process for such service prior launching their services.

ACS

Access Control Server (ACS) is the availed component by the National Scheme Operator which its' main task is to operate in the Issuer Domain, and its' role verifies whether authentication is available for a card number and device type, and authenticates specific

إذا كانت المنتجات أو الخدمات المشتراة غير متوفرة في وقت إجراء المعاملة، يجب على التاجر إبلاغ حامل البطاقة والحصول على موافقة حامل البطاقة على التسليم المتأخر (تحديد تاريخ التسليم المتوقع) قبل متابعة المعاملة.

يجب على التاجر إبلاغ حامل البطاقة إذا كانت المنتجات أو الخدمات المطلوبة لن يتم تسليمها خلال المواعيد الزمنية التي تم الإفصاح عنها في الأصل والموافقة عليها مع حامل البطاقة. يجب إخطار حامل البطاقة بالمواعيد الجديدة المتوقعة للتسليم، وإعطائه فرصة لإلغاء المعاملة. يجب أن تتوافق المعلومات المقدمة في أي إقرار بالبريد الإلكتروني لطلب حامل البطاقة مع متطلبات استلام المعاملة الموضحة في هذا الفصل.

اعتبارات جهة الإصدار

1. يجب على جميع المصارف المصدرة لعلامة نمو التجارية التأكد من أن بطاقتها الصادرة مسجلة لدى مشغل شبكة الدفع المحلية وأن تفاصيلها دقيقة ومحدثة.
2. تتحمل جهات الإصدار مسؤولية التجارب الاحتمالية التي لم تتبع قواعد الحماية ثلاثية الأبعاد من خلال التحقق من المعلومات الإضافية المقدمة من خلال ACS والتي تفيد بأن حامل البطاقة لم ينجح في التحقق من المصادقة.

2.2.4 مكونات النظام البيئي

(انظر الملحق رقم 28)

خادم 3DS وبوابة الدفع

يجب أن يستفيد مشغل شبكة الدفع المحلية من خادم 3DS وهو الجزء الذي يستخدمه القابلون ويدير من خلاله استيعاب التجار المرتبطين بهم، والاستفادة من عميل 3DS وهو المكون المواجه للمستهلك الذي يتيح تفاعل المستهلك مع طالب 3DS للبدء بروتوكول EMV D Secure3D.

يمكن لمشغل شبكة الدفع المحلية ترخيص برنامج تكامل ثلاثي الأبعاد يعمل كمشارك آمن ثلاثي الأبعاد يعمل على تسهيل ودمج بيئة الطالب لـ 3DS ، ويسهل اختياريًا التكامل بين التاجر والقابل.

تعمل بوابة الدفع المحلية كقناة أمامية للمدفوعات الإلكترونية التي يقوم بها العملاء ويمكن تهيئتها لربطها بصفحة الويب الخاصة بالتاجر من خلال ميزات العلامة التجارية القابلة للتعديل.

يُطلب من جميع القابلين المرخصين لقبول الدفع الإلكتروني أن يكونوا جزءًا من الخدمات المضمونة ثلاثية الأبعاد لنمو ويجب عليهم التقدم بطلب لذلك من خلال مشغل شبكة الدفع المحلية لإجراء عملية التصديق والتسجيل المطلوبة لهذه الخدمة قبل إطلاق خدماتهم.

ACS

خادم التحكم في الوصول (ACS) وهو المكون الذي يتم الاستفادة منه بواسطة مشغل شبكة الدفع المحلية وتتمثل مهمته الرئيسية في العمل في مجال جهة الإصدار، ويتحقق دوره مما إذا كانت المصادقة متاحة لرقم البطاقة ونوع الجهاز، ويصادق على حاملي البطاقات المحددين.

Cardholders.

As forementioned all NUMO issuers must be on-boarded on the services of the ACS and the National Scheme operator availed the needed UI (User Interface) for maintaining the life cycle of cards issued by NUMO issuers in addition to API interface for bulk uploads and system to system integration.

Through the ACS the additional verification to challenge the card holder is been maintained and verified by the ACS and submits the confirmation as part of the ISO message during authorisation verification by the Issuer.

Results of verification shall be included in the ISO 8583 message associated as per the National Scheme Operator message specifications, defining the results and status for card holder authentication performed as well as merchant status on 3DS server.

DS

The Directory Server (DS) availed by the National Scheme Operator is to be the server component that performs number of functions that include: authenticating the 3DS Server, routing messages between the 3DS Server and the ACS, and validating the 3DS Server, the 3DS SDK, and the 3DS Requestor.

It integrates securely with the ACS as well as the 3DS servers and has the capability of integration based on the requirements and the standards set with accordance to EMVCo 3D Secure payment 2.0 and following versions.

National Payment Gateway

National Scheme Operator avails the Gateway web channel that to be promoted by Acquiring banks to their merchants and hooked up with their web pages and mobile applications to process the payment transactions, it is been maintained and administrated through privileges granted to acquiring banks to on-board their merchants through it and to define the Merchants identifiers and the associated discount rates as well as merchants details , it also can avail the required reports to the merchants to control and to know the transactions processed through them – with consideration to PCI rules of masking the cards and sensitive card data.

National Switch

The National Switch operated by the National Scheme Operator is the main pillar for conducting all NUMO products payment transactions being the only link between NUMO issuers and acquirers, it also takes additional role to ensure that the 3DS Secured messages are processed in the right format and contains the right credentials to confirm that both Issuer and acquirer are secured.

4.2.3 Acquirers and Merchants Obligations

A receipt must be provided for each Card-not-present Transaction. For each completed e-commerce Transaction, a printable receipt page must be displayed after the Cardholder confirms a purchase. With respect to an e-commerce Transaction, non-face-to-face recurring payment Transaction, or any other Card-not-present Transaction upon Cardholder request, a receipt is permitted to be sent to the Cardholder by email or other electronic means.

كما ذكرنا سابقًا، يجب إشراك جميع جهات إصدار نمو على خدمات ACS واستفادة مشغل شبكة الدفع المحلية من واجهة المستخدم المطلوبة للحفاظ على دورة حياة البطاقات الصادرة عن جهات إصدار نمو بالإضافة إلى واجهة API للتحميلات المجمعة وتكامل الأنظمة .

من خلال ACS، يتم الحفاظ على التحقق الإضافي للطعن في حامل البطاقة والتحقق منه بواسطة ACS وإرسال التأكيد كجزء من رسالة ISO أثناء التحقق من التفويض من قبل جهة الإصدار.

يجب تضمين نتائج التحقق في رسالة ISO 8583 المرتبطة وفقًا لمواصفات رسالة مشغل شبكة الدفع المحلية، مع تحديد نتائج وحالة مصادقة حامل البطاقة التي تم إجراؤها بالإضافة إلى حالة التاجر على خادم 3DS .

DS

خادم الدليل (DS) الذي يوفره مشغل شبكة الدفع المحلية هو مكون الخادم الذي يؤدي عددًا من الوظائف التي تشمل مصادقة خادم 3DS ، وتوجيه الرسائل بين خادم 3DS و ACS ، والتحقق من صحة خادم 3DS ، و 3DS SDK ، وطالب 3DS .

يتكامل بشكل آمن مع ACS بالإضافة إلى خوادم 3DS ولديه القدرة على التكامل بناءً على المتطلبات والمعايير الموضوعة وفقًا لـ EMVCo 3D Secure payment 2.0 والإصدارات التالية.

بوابة الدفع المحلية

يستفيد مشغل شبكة الدفع المحلية من قناة البوابة الإلكترونية التي سيتم الترويج لها من قبل المصارف القابلة على التجار وربطها بصفحات الويب وتطبيقات الهاتف المحمول الخاصة بهم لمعالجة معاملات الدفع، ويتم صيانتها وإدارتها من خلال الامتيازات الممنوحة للمصارف لتمكين المصارف من احتواء التجار من خلاله وتحديد معرفات التجار ومعدلات الخصم المرتبطة بها وكذلك تفاصيل التجار، كما يمكنه الاستفادة من التقارير المطلوبة للتجار للتحكم ومعرفة المعاملات التي تتم معالجتها من خلالهم - مع مراعاة قواعد PCI لإخفاء البطاقات وبيانات البطاقة الحساسة.

المحول المحلي

إن المحول المحلي الذي يديره مشغل شبكة الدفع المحلية هي جهة الإصدار الأساسية لإجراء جميع معاملات دفع منتجات نمو كونه الرابط الوحيد بين جهات إصدار نمو والقابلين، كما أنه يأخذ دورًا إضافيًا لضمان معالجة رسائل 3DS Secured بالتنسيق الصحيح وتحتوي على أوراق الاعتماد الصحيحة لتأكيد تأمين كل من جهة الإصدار والقابل.

3.2.4 التزامات القابلين والتجار

يجب تقديم إيصال لكل معاملة غير موجودة بالبطاقة. لكل معاملة تجارة إلكترونية مكتملة، ويجب عرض صفحة إيصال قابلة للطباعة بعد تأكيد حامل البطاقة على الشراء. فيما يتعلق بمعاملة التجارة الإلكترونية، أو معاملة الدفع المتكررة غير المباشرة، أو أي معاملة أخرى غير موجودة بالبطاقة بناءً على طلب حامل البطاقة، يُسمح بإرسال إيصال إلى حامل البطاقة عن طريق البريد الإلكتروني أو أي وسيلة إلكترونية أخرى.

At the final stage of the Transaction, detailed data of the order must be displayed for the Cardholder and must include all of following:

- Order Number/ID.
- Total amount to be charged to the Account, including delivery charges.
- Order date and Estimated date of delivery/service fulfillment.
- Summary of ordered merchandise/service.

The Merchant should maintain all related correspondences, order screens and any related document to support the Transaction.

PART II – Cards Digitization and Mobile Wallets

4.3 Mobile Payment Devices

There is no limitation on the type of account that has the right to co-reside on the same Mobile Payment Device user interface, so long as such accounts are not linked, but rather exist independently and are accessed by a separate and distinct Payment Application hosted on the same or different user interfaces.

Mobile Payment Devices are permitted to support National Scheme Operator contactless payment and/or Digital Secure Remote Payment functionality. If an Issuer chooses to add this functionality to a Secure Element (SE)-based Mobile Payment Device, the application software, personalization data, and all other aspects of the functionality must comply with the requirements set forth in the Standards, including but not limited to other applicable technical specifications published by National Scheme Operator from time to time. The SE must meet all applicable security requirements.

4.3.1 Wallet Definition

The wallet is a secure money management app and can be an online platform that allows its users to make purchases with retailers on-site, transfer or send money and track rewards programs. Also, the users can manage their bill payments through services associated with some of the authorities.

The Wallets can be linked to a bank account and must be associated to a mobile number.

4.3.2 Wallet enabled services

National Payment Gateway enabled number of services via the wallets used in the country whereby a user can inquire and conduct transfers to another user wallet, bills payment including telecom, internet, utility and traffic fees in addition to wide range of other services availed through the National Payment Gateway.

Wallet transfer services are set to an identified cap per day/Month as stated by the CBL.

Users are capable to withdraw money from their Wallet by visiting any retailers that are scattered across the governates or through any ATM that displays NUMO logo with such capability.

Additional capability of the existing wallet is the feature of generating Virtual Card Number (VCN) that can be used for electronic payments, whether through the payment gateway or via Mail and Telephone Order services under same forementioned rules of acceptance, the VCN will be generated based on NUMO owned BIN ranges associated with the designated cardholder issuing banks.

في المرحلة الأخيرة من المعاملة، يجب عرض بيانات الطلب التفصيلية لحامل البطاقة ويجب أن تتضمن كل ما يلي:

- رقم الطلب / معرف.
- المبلغ الإجمالي الذي سيتم تحميله على الحساب، بما في ذلك رسوم التسليم.
- تاريخ الطلب والتاريخ التقديري للتسليم / الوفاء بالخدمة.
- ملخص للبضائع والخدمات المطلوبة .

ويجب أن يحتفظ التاجر بجميع المراسلات المتعلقة بالمعاملة وشاشات الطلبات وأي مستندات ذات صلة لدعم المعاملة.

الجزء الثاني - رقمنة البطاقات والمحافظ المحمولة

3.4 أجهزة الدفع عبر الهاتف المحمول

لا توجد قيود على نوع الحساب الذي له الحق في الإقامة المشتركة على نفس واجهة مستخدم جهاز الدفع عبر الهاتف المحمول ، طالما أن هذه الحسابات ليست مرتبطة، بل موجودة بشكل مستقل ويمكن الوصول إليها بواسطة تطبيق دفع منفصل ومميز مستضاف على نفس واجهات المستخدم أو واجهات مختلفة.

يسمح لأجهزة الدفع عبر الهاتف المحمول بدعم الدفع عن بعد لمشغل شبكة الدفع المحلية و/ أو وظيفة الدفع الرقمي الآمن عن بُعد. إذا اختارت جهة الإصدار إضافة هذه الوظيفة إلى جهاز الدفع بواسطة الهاتف المحمول المستند إلى عنصر آمن (SE)، فيجب أن يتوافق برنامج التطبيق وبيانات التخصيص وجميع الجوانب الأخرى للوظيفة مع المتطلبات المنصوص عليها في المعايير، بما في ذلك على سبيل المثال لا الحصر إلى المواصفات الفنية المطبقة الأخرى المنشورة بواسطة مشغل شبكة الدفع المحلية من وقت لآخر. يجب أن يفي (SE) جميع متطلبات الأمان المعمول بها.

1.3.4 تعريف المحفظة

المحفظة هي تطبيق آمن لإدارة الأموال ويمكن أن تكون منصة عبر الإنترنت تتيح لمستخدميها إجراء عمليات شراء مع تجار التجزئة في الموقع، وتحويل الأموال أو إرسالها وتتبع برامج المكافآت. أيضًا ، يمكن للمستخدمين إدارة مدفوعات فواتيرهم من خلال الخدمات المرتبطة ببعض السلطات. يمكن ربط المحافظ بحساب مصرفي ويجب أن تكون مرتبطة برقم هاتف محمول.

2.3.4 الخدمات الممكنة للمحفظة

أتاحت بوابة الدفع المحلية عددًا من الخدمات عبر المحافظ المستخدمة في الدولة حيث يمكن للمستخدم الاستعلام وإجراء التحويلات إلى محفظة مستخدم أخرى، ودفع الفواتير بما في ذلك رسوم الاتصالات والإنترنت والمرافق والمرور بالإضافة إلى مجموعة واسعة من الخدمات الأخرى المتاحة من خلال بوابة الدفع المحلية.

يتم تعيين خدمات تحويل المحفظة إلى حد أقصى محدد يوميًا / شهرًا كما هو مذكور من قبل مصرف ليبيا المركزي.

يمكن للمستخدمين سحب الأموال من محفظتهم من خلال زيارة مواقع أي تجار تجزئة منتشرين في جميع أنحاء البلاد أو من خلال أي ماكينة صراف آلي تعرض شعار نمو بهذه الإمكانيّة.

القدرة الإضافية للمحفظة الحالية هي ميزة إنشاء رقم البطاقة الافتراضية (VCN) التي يمكن استخدامها للمدفوعات الإلكترونية، سواء من خلال بوابة الدفع أو عبر البريد وخدمات الطلب الهاتفي بموجب نفس قواعد القبول المذكورة أعلاه، سيتم إنشاء VCN على أساس نطاقات أرقام تعريف مصرفية مملوكة لنمو والمرتبطة بالمصارف المصدرة لحامل البطاقة المعين.

4.3.3 Wallet management server

Wallet Management server is an essential component responsible of managing all wallets associated with it and must avail the security certificates to handshake with each device operated through it, in addition to conducting the registration processes and avails the SDK that can be used by wallet developers to design and prepare the wallets and its' functions. This part would be integrated with Utility payments service providers and some other entities which are interested in fast and secured payments.

Its; usually operated either by Issuer banks or through a Wallet service Provider.

The National Scheme Operator avails and supervise such services within its' delegated tasks from the CBL.

4.3.4 Wallet service provider

The National Scheme Operator enables the services introduced via accredited wallet service providers, The wallet service providers are solution providers that provides a digital or virtual wallet for holding, receiving, and transferring virtual or digitized money.

The accredited wallet service providers that are interested to work in Libya must be compliant with relevant PCI rules and following the security measurements known for such services.

In Addition to their product portfolio for scalability and multiple payment methods, with variety of links with utility bills aggregator and customer debit bank accounts integration ...etc.

They should not be indifferentiable or with a distinguished services with limitation to a specific brand or network and must support the integration for NUMO products.

4.3.5 Consumer Device Cardholder Verification Method (CDCVM)

Consumer authentication technologies used on consumer devices, such as personal computers, tablets, mobile phones, and watches, are designed to verify a person as an authorized device user based on one or more of the following:

- “Something I know”—Information selected by and intended to be known only to that person, such as a passcode or pattern
- “Something I am”—A physical feature that can be translated into biometric information for the purpose of uniquely identifying a person, such as a face, fingerprint, or heartbeat
- “Something I have”—Information intended to uniquely identify a particular consumer device

Any such consumer authentication technology must be approved by National Scheme Operator as a “National Scheme Operator-qualified CVM” before it may be used as a Consumer Device Cardholder Verification Method (CDCVM) to process a Transaction. If the issuer banks see additional control to be applied with the CDCVM for large amounts performed through wallets , specifically for Hosted card Emulator (Tokenization based wallets) – they may require as such to provide a PIN entry over the POI.

3.3.4 خادم إدارة المحفظة

يعد خادم إدارة المحفظة مكونًا أساسيًا مسؤولًا عن إدارة جميع المحافظ المرتبطة به ويجب أن يستفيد من شهادات الأمان للمصافحة مع كل جهاز يتم تشغيله من خلاله، بالإضافة إلى إجراء عمليات التسجيل والاستفادة من SDK التي يمكن استخدامها من قبل مطوري المحفظة لتصميم وإعداد المحافظ ووظائفها.

سيتم دمج هذا الجزء مع مقدمي خدمة مدفوعات المرافق وبعض الكيانات الأخرى المهمة بالمدفوعات السريعة والأمانة.

إنه؛ يدار عادة إما من قبل المصارف المصدرة أو من خلال مقدم خدمة المحفظة.

يستفيد مشغل شبكة الدفع المحلية من هذه الخدمات ويشرف عليها ضمن المهام المفوضة له من مصرف ليبيا المركزي

4.3.4 مقدم خدمة المحفظة

يمكن مشغل شبكة الدفع المحلية الخدمات المقدمة من خلال مقدمي خدمة المحفظة المعتمدين، ومقدمو خدمة المحفظة هم مقدمو حلول يوفرهم محفظة رقمية أو افتراضية لحفظ واستلام وتحويل الأموال الافتراضية أو الرقمية.

يجب أن يمثل مقدمو خدمة المحفظة المعتمدين المهتمين بالعمل في ليبيا لقواعد PCI ذات الصلة واتباع القياسات الأمنية المعروفة لمثل هذه الخدمات.

بالإضافة إلى مجموعة منتجاتهم من أجل قابلية التوسع وطرق الدفع المتعددة ، مع مجموعة متنوعة من الروابط مع مجمع فواتير الخدمات وتكامل حسابات العملاء المصرفية المدين ... إلخ.

لا ينبغي أن يكونوا محايدين / متحيزين أو مع خدمات مميزة مع تقييد لعلامة تجارية معينة أو شبكة ويجب أن تدعم تكامل منتجات نمو.

5.3.4 طريقة التحقق من حامل بطاقة جهاز المستهلك (CDCVM)

لقد تم تصميم تقنيات مصادقة المستهلك المستخدمة على أجهزة المستهلك، مثل أجهزة الكمبيوتر الشخصية والأجهزة اللوحية والهواتف المحمولة والساعات، للتحقق من شخص ما كمستخدم جهاز معتمد بناءً على واحد أو أكثر مما يلي:

- “شيء ما أعرفه” - معلومات يختارها، ويقصد أن تكون معروفة لهذا الشخص فقط، مثل رمز المرور أو النمط.
- “شيء ما أنا عليه” - ميزة مادية يمكن ترجمتها إلى معلومات بيومترية بغرض التعرف بشكل فريد على الشخص ، مثل الوجه أو بصمة الإصبع أو ضربات القلب.
- “شيء لدي” - معلومات تهدف إلى التعرف بشكل فريد على جهاز مستهلك معين.

يجب أن تتم الموافقة على أي تقنية مصادقة للمستهلك من قبل مشغل شبكة الدفع المحلية باعتبارها “CVM المؤهل لمشغل شبكة الدفع المحلية ” قبل أن يتم استخدامها كطريقة للتحقق من حامل بطاقة جهاز المستهلك (CDCVM) لمعالجة المعاملة.

إذا قدرت المصارف المصدرة أن تحكّم إضافيًا يتم تطبيقه مع CDCVM للمبالغ الكبيرة التي يتم إجراؤها من خلال المحافظ، وتحديدًا لمحاكي البطاقات المستضافة (المحافظ المستندة إلى الرمز الفريد) - فقد يطلبون على هذا النحو توفير إدخال رقم التعريف الشخصي على نقطة التفاعل.

4.3.6 Implementation Guidelines & Security Requirements

- The Wallet must apply through the app all the security requirements for the code to avoid any potential penetrations preferred to rely on latest technology such as white box cryptography or similar wallet app security measurements.
- The wallet must be secured through a password or other alternative associated with CDCVM to enable the access to the wallet.
- Successful pen test must be conducted with evidence that can be referred to by the auditors.
- Updated and regular PCI-DSS certificate should exist and renewed frequently.
- Each bank interested in such implementation should acknowledge the National Scheme operator defining the wallet service provider they deal with or state if its self-managed services.

4.3.7 Issuer Banks Responsibilities

- Perform the right due diligence for selecting the right model that fits with their digital transformation plan.
- To ensure that security measurements are applied and meets the requirements of PCI-DSS as well as Pen test needed to protect their customers.
- Issuers cannot selectively apply the digital wallet services for certain brand against other brands operated by the banks, such discrimination is prohibited.
- Apply RBA system (Risk Based Assessment) to help detecting any potential fraudulent trials or misbehavior that can be considered against AML/CFT.

4.3.8 Acceptance of Digitized Payments

- Wallet transactions based on mobile wallet balance can be accepted through transfers managed by the mobile application after providing the required CDCVM verification, this is applied on transfers from a customer wallet to another customer wallet or managing bill payments.
- Some of provided functions can be associated with cash dispense through designated ATMs or through specified and authorized agents against certain fees its' borderlines are defined by the National Scheme Operator,
- For HCE tokenized cards, the acquirer is requested to route the recognized BIN to its' associated network and to provide the additional required information containing the Token Requester ID and the device type as well as the issuer identifiers.

4.3.9 Acquirers Responsibilities

- No distinctive selection for supporting specific wallet services of a certain brand than the other.
- The NUMO brand and its' related digitized services must be presented and accepted in a way not less than any other ICS brand acceptance.
- Acquirers introducing cash dispense services for wallets can be only linked and operated for such services through the National Scheme Operator switching services.

4.3.10 Recurring Payments & Card On File

- The National Payment Gateway introduces to the market the recurring payment services through merchants – such service enables multiple deductions at a certain date for a registered cardholder card through merchant as a subscription in service or as payment of installments agreed by the cardholder.

6.3.4 إرشادات التنفيذ ومتطلبات الأمان

- اختراقات محتملة، ويفضل الاعتماد على أحدث التقنيات مثل تشفير الصندوق الأبيض أو قياسات أمان تطبيقات المحفظة المماثلة.
- يجب تأمين المحفظة من خلال كلمة مرور أو بديل آخر مرتبط بـ CDCVM لتمكين الوصول إلى المحفظة.
- يجب إجراء اختبار القلم الناجح مع الأدلة التي يمكن الرجوع إليها من قبل المدققين.
- يجب أن توجد شهادة PCI-DSS محدثة ومنظمة وتجدد بشكل متكرر.
- يجب على كل مصرف مهتم بهذا التنفيذ أن يقر بمشغل شبكة الدفع المحلية الذي يحدد مقدم خدمة المحفظة الذي يتعامل معه أو يحدد ما إذا كانت خدماته ذاتية الإدارة.

7.3.4 مسؤوليات المصارف المصدرة

- بذل العناية الواجبة لاختيار النموذج الذي يتناسب مع خطة التحول الرقمي الخاصة بهم.
- ضمان تطبيق القياسات الأمنية وتلبية متطلبات PCI-DSS وكذلك اختبار القلم اللازم لحماية عملائهم.
- لا يمكن لجهات الإصدار تطبيق خدمات المحفظة الرقمية بشكل انتقائي لعلامة تجارية معينة ضد العلامات التجارية الأخرى التي تديرها المصارف، وهذا التمييز محظور.
- تطبيق نظام RBA (التقييم القائم على المخاطر) للمساعدة في الكشف عن أية معاملات احتيالية محتملة أو سوء سلوك يمكن اعتباره ضد مكافحة غسيل الأموال ومكافحة تمويل الإرهاب.

8.3.4 قبول المدفوعات الرقمية

- يمكن قبول معاملات المحفظة بناءً على رصيد محفظة الهاتف المحمول من خلال التحويلات التي يديرها تطبيق الهاتف المحمول بعد توفير التحقق المطلوب من CDCVM، ويتم تطبيق ذلك على التحويلات من محفظة عميل إلى محفظة عميل أخرى أو إدارة مدفوعات الفواتير.
- يمكن ربط بعض الوظائف المقدمة بالتوزيع النقدي من خلال أجهزة الصراف الآلي المعينة أو من خلال وكلاء محددين ومعتمدين مقابل رسوم معينة يحدد مشغل شبكة الدفع المحلية حدودها.
- بالنسبة لبطاقات ترميز HCE، يُطلب من القابل توجيه رقم التعريف المصرفي المعترف به إلى الشبكة المرتبطة بها وتقديم المعلومات الإضافية المطلوبة التي تحتوي على معرف مقدم الطلب ونوع الجهاز بالإضافة إلى معرفات جهة الإصدار.

9.3.4 مسؤوليات القابلين

- لا يوجد اختيار مميز لدعم خدمات محفظة معينة لعلامة تجارية معينة عن الأخرى.
- يجب تقديم علامة نمو التجارية والخدمات الرقمية المرتبطة بها وقبولها بطريقة لا تقل عن قبول أي علامة تجارية أخرى لـ ICS.
- لا يمكن ربط القابلين الذين يقدمون خدمات التوزيع النقدي للمحافظ وتشغيلهم لهذه الخدمات إلا من خلال خدمات تبديل مشغل شبكة الدفع المحلية.

10.3.4 المدفوعات المتكررة والبطاقة في الملف

- تقدم بوابة الدفع المحلية للسوق خدمات الدفع المتكررة من خلال التجار، وتتيح هذه الخدمة إجراء خصومات متعددة في تاريخ معين لبطاقة حامل البطاقة المسجلة من خلال التاجر كاشتراك في الخدمة أو كدفع أقساط يتفق عليها حامل البطاقة.

- The merchant may apply a transaction processing through associated API availed by the National Payment Gateway or via a file submitted for collection either through submitting to the network or via availed specific API.
- The National Payment Gateway can avail tokenization services for Cards on File by generating the associated token for each card per specific merchant and merchants may only use that token within request for payment process.
- Merchants requests to have the real card number to request for recurring payment must rely on certified tokenization vault or to be PCI DSS certified and must share desired proof of such certification and to maintain the renewal of such certification.

PART III – QR Code

QR Code consolidated specs and definitions

QR Codes are two-dimensional machine-readable barcodes, which are increasingly used to facilitate mobile payments at the point-of-sale. The National Scheme Operator is following the EMV QR Code Specification for Payment Systems supports two differing QR Code payment use cases:

- Consumer-presented – the customer displays the QR Code on their mobile device and the merchant uses an optical scanner to read the code.
- Merchant-presented – the merchant displays the QR Code and the customer uses their mobile device to scan the code.

The clarity provided by the specifications will enable merchants to accept QR Code payment solutions from various providers in a standardized manner. Consumers will also benefit from a more uniform experience that offers greater convenience and familiarity.

The followed National Scheme Operator QR Code Specification for Payment Systems can coexist with existing proprietary QR Code solutions.

“With the increasing deployment of QR Code payment methods, it is important that the payments ecosystem provides a consistent experience for merchants and consumers.

Given the early stage of deployment of this emerging payment technology and growing adoption, now is the time to ensure the technology’s potential is not constrained in the future due to interoperability issues with the established payment infrastructure.”

QR Code Merchant presented

The use of a basic merchant QR Code. A basic merchant QR Code can be used in simple purchases with no additional service, such as convenience fees or tips, in a merchant supporting one payment network. This example includes only the mandatory data objects required in the merchant QR Code.

The merchant QR code is commonly displayed on a sticker or poster, and the Transaction Amount is likely absent from the merchant QR code.

The data in this QR Code is most suitable for a merchant location or segment where interactions between the consumer and the merchant are basic, and the merchant location does not use a digital display, such as a coffee cart with relatively low traffic.

- يجوز للتاجر تطبيق معالجة معاملة من خلال واجهة برمجة التطبيقات المرتبطة التي توفرها بوابة الدفع المحلية أو عبر ملف مقدم للتحويل إما من خلال الإرسال إلى الشبكة أو عبر واجهة برمجة التطبيقات المحددة المتاحة.
- يمكن لبوابة الدفع المحلية الاستفادة من خدمات الترميز للبطاقات الموجودة في الملف عن طريق إنشاء رمز مرتبط لكل بطاقة لكل تاجر محدد، ولا يجوز للتاجر استخدام هذا الرمز الفريد إلا في طلب عملية الدفع.
- يجب أن يعتمد طلب التاجر للحصول على رقم البطاقة الحقيقي لطلب الدفع المتكرر على قبول رمزي معتمد أو أن يكون معتمدًا من PCI DSS ويجب عليهم مشاركة الدليل المطلوب لهذه الشهادة والحفاظ على تجديد هذه الشهادة.

الجزء الثالث - رمز الاستجابة السريعة

المواصفات والتعاريف الموحدة لرمز الاستجابة السريعة

رموز QR هي رموز شريطية ثنائية الأبعاد يمكن قراءتها آليًا، والتي تُستخدم بشكل متزايد لتسهيل المدفوعات عبر الهاتف المحمول في نقطة البيع. ويتبع مشغل شبكة الدفع المحلية مواصفات رمز الاستجابة السريعة EMV لأنظمة الدفع التي تدعم حالتين مختلفتين لاستخدام دفع رمز الاستجابة السريعة:

- مقدم من المستهلك - يعرض العميل رمز الاستجابة السريعة (QR Code) على أجهزته المحمولة ويستخدم التاجر ماسحًا ضوئيًا لقراءة الرمز.
- مقدم من التاجر - يعرض التاجر رمز الاستجابة السريعة (QR Code) ويستخدم العميل جهازه المحمول لمسح الرمز ضوئيًا.

سيسمح الوضع الذي توفره المواصفات للتجار بقبول حلول الدفع باستخدام رمز الاستجابة السريعة من مختلف المقدمين بطريقة موحدة. سيستفيد المستهلكون أيضًا من تجربة أكثر اتساقًا توفر قدرًا أكبر من الراحة .

يمكن أن تتعايش مواصفات رمز QR مشغل شبكة الدفع المحلية المتبع لأنظمة الدفع مع حلول رمز الاستجابة السريعة الحالية.

”مع الانتشار المتزايد لطرق الدفع باستخدام رمز الاستجابة السريعة، فإنه من المهم أن يوفر النظام البيئي للمدفوعات تجربة متسقة للتجار والمستهلكين.

نظرًا للمرحلة المبكرة من نشر تقنية الدفع الناشئة هذه والاعتماد المتزايد، فقد حان الوقت الآن لضمان عدم تقييد إمكانيات التكنولوجيا في المستقبل بسبب مشكلات التشغيل البيئي مع البنية التحتية للدفع المنشأة ”.

رمز الاستجابة السريعة للتاجر

استخدام رمز QR الأساسي للتاجر. يمكن استخدام رمز الاستجابة السريعة والأساسي للتاجر في عمليات شراء بسيطة بدون خدمة إضافية، مثل رسوم الراحة أو النصائح، في تاجر يدعم شبكة دفع واحدة. يتضمن هذا المثال فقط البيانات الإلزامية المطلوبة في رمز الاستجابة السريعة الخاص بالتاجر.

عادةً ما يتم عرض رمز الاستجابة السريعة الخاص بالتاجر على ملصق ومن المحتمل أن يكون مبلغ المعاملة غائبًا عن رمز الاستجابة السريعة الخاص بالتاجر.

البيانات الموجودة في رمز الاستجابة السريعة هذا هي الأنسب لموقع أو مقطع التاجر حيث تكون التفاعلات بين المستهلك والتاجر أساسية، ولا يستخدم موقع التاجر شاشة رقمية، مثل عربة القهوة

The following data objects are intended to be used and processed:

- Payload Format Indicator presented as value (01)
- Merchant Account Information
- Merchant Category Code
- Transaction Currency To be set to value (434)
- Country Code to be set to value (LY)
- Merchant Name
- Merchant City
- Cyclic Redundancy Check (CRC) Calculated using the algorithm defined as per standards of EMV MERCHANT QR

The following describes key points in the transaction.

1. The consumer uses their mobile phone to scan the merchant QR Code poster.
2. The consumer QR application supports the payload format indicated by the Payload Format Indicator and proceeds with recovering the data objects from the QR Code.

The consumer QR application uses the Merchant Account Information to select the payment card to be used to complete the transaction.

3. The consumer QR application displays the Merchant Name, Merchant City, and Transaction Currency to the consumer, and prompts the consumer to enter a Transaction Amount.

Important: The consumer QR application should use the currency code read from the merchant QR Code for the transaction, and should not use any other currency code that may be present in the QR application other than 434.

4. Once the consumer inputs the Transaction Amount and confirms payment, the consumer QR application sends the Merchant Account Information, Transaction Currency, Transaction Amount, and other data (for example, consumer payment information) to the network.
5. Once the transaction is successfully completed by the network, payment confirmations are sent to the merchant POI and the consumer mobile phone.

Important: Network processing is a sole discretion to the National Scheme Operator.

QR Code Consumer presented

Following the fore set standards of EMV Consumer-Presented Mode QR Code transaction, consumers can make purchases—using credentials associated with their EMV card and previously provisioned to their device—by selecting the QR option for payment within their mobile application, which will result in the display of the QR Code, and having that QR Code scanned at the time of payment to complete the transaction.

Transactions are always authorized online and given that the scanning of the QR Code is a one-way transfer of data from the consumer's device to the POI, the payload of the QR Code does not contain any data from the POI.

In the event that any cardholder verification is required, it is envisaged that it would be performed through CDCVM. Thus, unlike typical payment transactions, the requirement for CVM is never communicated, or delegated to the POI.

ذات حركة المرور المنخفضة نسبيًا.

الغرض من البيانات التالية هو استخدامها ومعالجتها:

- تم تقديم مؤشر تنسيق الحمولة كقيمة (01)
- معلومات حساب التاجر.
- رمز فئة التاجر.
- عملة المعاملة التي سيتم تعيينها على القيمة (434)
- تعيين رمز البلد على القيمة (دينار ليبي).
- اسم التاجر.
- مدينة التاجر.
- فحص التكرار الدوري (CRC) محسوب باستخدام الخوارزمية المحددة وفقًا لمعايير EMV QR التاجر.

فيما يلي وصف للنقاط الرئيسية في المعاملة.

1. يستخدم المستهلك هاتفه المحمول لمسح ملصق رمز الاستجابة السريعة الخاص بالتاجر.
2. يدعم تطبيق QR للمستهلك تنسيق الحمولة المشار إليه بواسطة مؤشر تنسيق الحمولة ويواصل استعادة البيانات من رمز الاستجابة السريعة.

يستخدم تطبيق QR الخاص بالمستهلك معلومات حساب التاجر لتحديد بطاقة الدفع المراد استخدامها لإكمال المعاملة.

3. يعرض تطبيق QR الخاص بالمستهلك اسم التاجر، مدينة التاجر، عملة المعاملة للمستهلك، ويطلب من المستهلك إدخال مبلغ المعاملة.

تنويه هام: يجب أن يستخدم تطبيق QR الخاص بالمستهلك رمز العملة الذي تمت قراءته من رمز QR الخاص بالتاجر للمعاملة، ويجب ألا يستخدم أي رمز عملة آخر قد يكون موجودًا في تطبيق QR بخلاف 434.

4. بمجرد قيام المستهلك بإدخال مبلغ المعاملة وتأكيد الدفع، يرسل تطبيق QR للمستهلك معلومات حساب التاجر وعملة المعاملة ومبلغ المعاملة والبيانات الأخرى (على سبيل المثال، معلومات دفع المستهلك) إلى الشبكة.

5. بمجرد إتمام الشبكة للمعاملة بنجاح، يتم إرسال تأكيدات الدفع إلى مركز معلومات التاجر، والهاتف المحمول للمستهلك.

تنويه هام: معالجة الشبكة تخضع للسلطة التقديرية لمشغل شبكة الدفع المحلية.

رمز الاستجابة السريعة للمستهلك

وفقًا للمعايير المحددة مسبقًا لمعاملة رمز الاستجابة السريعة للوضع الذي يقدمه المستهلك من EMV، يمكن للمستهلكين إجراء عمليات شراء - باستخدام بيانات الاعتماد المرتبطة ببطاقة EMV الخاصة بهم والتي تم توفيرها مسبقًا إلى أجهزتهم - عن طريق تحديد خيار QR للدفع داخل تطبيق الهاتف المحمول الخاص بهم ، مما سيؤدي إلى عرض رمز الاستجابة السريعة وإجراء مسح ضوئي لرمز الاستجابة السريعة في وقت الدفع لإتمام المعاملة.

يجوز دائمًا إجراء المعاملات عبر الإنترنت، ونظرًا لأن مسح رمز الاستجابة السريعة ضوئيًا هو نقل أحادي الاتجاه للبيانات من جهاز المستهلك إلى نقطة التفاعل ، فإن حمولة رمز الاستجابة السريعة لا تحتوي على أي بيانات من نقطة التفاعل.

إذا كانت هناك ضرورة للتحقق من حامل البطاقة، فمن المتوقع أن يتم إجراؤه من خلال CDCVM. وبالتالي، على عكس معاملات الدفع النموذجية، لا يتم أبدًا إبلاغ متطلبات CVM أو تفويضها إلى نقطة التفاعل.

QR Code various components

The following describes the high-level functionality of various components of the QR Code processing architecture on the consumer device:

- Mobile application/wallet—A consumer-facing user interface (UI) application provided by the issuer, merchant, or a third-party and provisioned to the consumer's mobile device. It includes the functionality to encode the payment credentials based on this specification, and then displays the resulting QR Code.

The mobile application is responsible for providing a UI that will facilitate card application selection, perform any required CDCVM processing and rendering of the corresponding QR Code.

- QR Code Reader—Scans the QR Code, decodes the QR Code and sends the data recovered to the POI System. This data constitutes the base64 encoded QR Code Payload.
- POI Application—The application developed by the POI vendor to process the base64 encoded QR Code payload defined in this specification. Its functions include base64 decoding, parsing the data, checking content and format and transaction processing.

On the network the following are the roles as per the existing EMV infrastructure:

- Acquirer—The acquirer/processor processing the authorisation transaction received from the merchant.
- National Scheme Network—Responsible for transaction routing to the issuer and any corresponding tokenisation services and functions.
- Issuer—The issuer of the original payment card, that is used in the QR Code transaction.

PART IV – Rules and Operation considerations

4.4 NSO Role for eCommerce & Digitized Payment Services

- The National Scheme Operator is the Payment Gateway provider for the NUMO brand acceptance via eComemrce payments.
- National scheme operator furnished the required platform to host and operate a 3D-Secured payments in-line with EMVco. Mandates and requirements.
- All NUMO eCommerce related services must be driven and controlled via the provided payment gateway services and the National Scheme Switching services.
- The National scheme operator under the CBL delegated rights may set the rules that govern the eCommerce-based transactions and to take the right auditing steps to ensure and to review the compliance with such rules.
- The National Scheme Operator under the same CBL given delegated rights can set the fees of accessing the above mentioned platforms and the cost of processing wallet based transactions via the National Switch after doing the proper alignment with the CBL.

مكونات مختلفة لرمز الاستجابة السريعة

فيما يلي وصف للوظائف عالية المستوى لمختلف مكونات بنية معالجة رمز الاستجابة السريعة على جهاز المستهلك:

- تطبيق الهاتف المحمول / المحفظة - تطبيق واجهة مستخدم المستهلك (UI) المقدم من جهة الإصدار أو التاجر أو جهة خارجية ويتم توفيره لجهاز الهاتف المحمول الخاص بالمستهلك. ويتضمن وظيفة ترميز بيانات اعتماد الدفع بناءً على هذه المواصفات، ثم يعرض رمز الاستجابة السريعة الذي يتم التوصل إليه.

تطبيق الهاتف المحمول مسؤول عن توفير واجهة مستخدم تسهل اختيار تطبيق البطاقة، وتنفيذ أي معالجة CDCVM مطلوبة وتقديم رمز الاستجابة السريعة المقابل.

- قارئ رمز الاستجابة السريعة — يسمح رمز الاستجابة السريعة ويفك تشفير رمز الاستجابة السريعة ويرسل البيانات المستردة إلى نظام نقطة التفاعل. تشكل هذه البيانات حمولة رمز الاستجابة السريعة المشفرة لـ base64.
- تطبيق نقطة التفاعل - التطبيق الذي طوره بائع نقطة التفاعل لمعالجة حمولة رمز QR المشفرة لـ base64 المحددة في هذه المواصفات. تشمل وظائفه فك تشفير base64، وتحليل البيانات، وفحص المحتوى والتنسيق ومعالجة المعاملات.

على الشبكة، فيما يلي المهام وفقاً للبنية التحتية EMV الحالية:

- القابل - القابل/المعالج يعالج معاملة التفويض المستلمة من التاجر.
- شبكة النظام المحلية - مسؤولة عن توجيه المعاملات إلى جهة الإصدار وأي خدمات ووظائف رمزية مقابلة.
- جهة الإصدار - جهة إصدار بطاقة الدفع الأصلية، المُستخدمة في معاملة رمز الاستجابة السريعة.

الجزء الرابع - القواعد واعتبارات التشغيل

4.4 دور مشغل شبكة الدفع المحلية في التجارة الإلكترونية وخدمات الدفع الرقمية

- مشغل شبكة الدفع المحلية هو مقدم بوابة الدفع لقبول علامة نمو التجارية عبر مدفوعات التجارة الإلكترونية.
- يقوم مشغل شبكة الدفع المحلية بتزويد المنصة المطلوبة لاستضافة وتشغيل مدفوعات 3D Secured- بما يتماشى مع مهام و متطلبات EMVco.
- يجب تشغيل جميع الخدمات المتعلقة بالتجارة الإلكترونية التابعة لنمو والتحكم فيها عبر خدمات بوابة الدفع المقدمة وخدمات تبديل الشبكة المحلية.
- يجوز لمشغل شبكة الدفع المحلية بموجب الحقوق المفوضة من مصرف ليبيا المركزي وضع القواعد التي تحكم المعاملات القائمة على التجارة الإلكترونية واتخاذ خطوات التدقيق الصحيحة لضمان ومراجعة الامتثال لهذه القواعد.
- يمكن لمشغل شبكة الدفع المحلية بموجب نفس الحقوق المفوضة من مصرف ليبيا المركزي تحديد رسوم الوصول إلى المنصات المذكورة أعلاه وتكلفة معالجة المعاملات القائمة على المحفظة عبر المحول الوطني بعد إجراء التوافق الصحيح مع مصرف ليبيا المركزي.

4.5 Compliance & Risk Factors

eCommerce companies have been collecting, analyzing, and storing data about customers for a long time. Privacy and security concerns in e-commerce.

The member banks on-boarding merchants must perform the sufficient due diligence and investigate merchant legal paper to assure that the sites introducing the services are legal and illegitimate.

- Acquirers must assure that their merchants have established and enforced a strong data privacy and online security policy, train their staff, and incentivize them to become data security champions. Implement protocols like two-factor authentication (2FA) to add an extra layer of accountability.
- The operational risk that can be resulted through eCommerce-based services is considered much higher than face to face transactions, the acquiring banks must buffer and provision for any potential risk that cannot be avoided due to certain types of transactions.
- All parties in this eco system must Keep software, SaaS, and plugins up to date. And to remove and uninstall incompatible plugins and themes immediately. Enablement of firewalls and virus protection—but should not rely 100% on their device settings. And better be looking into more comprehensive solutions based on your data protection needs.
- Prevention and limitation of unauthorized access to payment related platforms shall limit and reduce the level of vulnerability and possibility to penetrate customers data.
- The CBL through its,' tools and the National Scheme Operator as being its' delegate shall guarantee- that all proper steps are taken correctly to secure card holders data and check against the fore set payment compliance and rules announced and regulated by the CBL.

4.6 Generic Rules for Cards Tokenization

- Tokenization of cards meant to be replacing sensitive card data as card number, expiry date , card specific identifiers with a token to manage the payment securely without the need of obtaining all PCI restrictions for payment transactions
- The Tokenization service must be managed through a secured vault applying the needed encryption to sensitive stored information and supported with a solution component as a portal to manage token and card life cycle, also to have the set of APIs to integrate with Issuers and token requestor API to link with wallet management servers, all of those components mentioned must be fully PCI-DSS compliant.
- Any Issuer bank desire to join tokenization services introduced by International card schemes or NUMO DES platform once established must comply with the integration APIS needed for associating its' Issuer TSP component with schemes needs and must perform the needed certification process prior being permitted to start sch service.
- For OEM Tokenization services (Apple Pay, Google Pay, Samsung pay ...etc.), the National Scheme operator must be part of the agreement .
- OEM Tokenized services shall not be start in Libya without pertaining the right approvals from the Central Bank of Libya.

5.4 الامتثال وعوامل الخطر

تقوم شركات التجارة الإلكترونية بجمع وتحليل وتخزين البيانات حول العملاء لفترة طويلة، إذ أن هناك مخاوف تتعلق بالخصوصية والأمان في التجارة الإلكترونية.

- يجب على التجار الأعضاء في المصارف اتخاذ إجراءات العناية المطلوبة والتحقيق في الأوراق القانونية الخاصة بالتاجر للتأكد من أن المواقع التي تقدم الخدمات قانونية ومشروعة.
- يجب أن يضمن القابلون أن التجار لديهم قد وضعوا وفرضوا سياسة قوية لخصوصية البيانات وأمن الإنترنت، وتدريب موظفيهم، وتحفيزهم ليصبحوا رواداً لأمن البيانات. ثم يقوموا بتنفيذ بروتوكولات مثل المصادقة الثنائية (2FA) لزيادة مستوى إضافي من المساءلة .
- تعتبر المخاطر التشغيلية التي يمكن أن تنتج من خلال الخدمات المستندة إلى التجارة الإلكترونية أعلى بكثير من المعاملات التقليدية وجهاً لوجه، ولذلك يجب على المصارف القابلة أن تحمي وتؤمن أي مخاطر محتملة لا يمكن تجنبها بسبب أنواع معينة من المعاملات.
- يجب على جميع الأطراف في هذا النظام البيئي تحديث البرامج و SaaS والمكونات الإضافية. وإزالة وإلغاء تثبيت المكونات الإضافية والسمات غير المتوافقة على الفور. تمكين جدران الحماية والحماية من الفيروسات ولكن يجب ألا تعتمد بنسبة 100% على إعدادات أجهزتهم
- ومن الأفضل البحث عن حلول أكثر شمولاً بناءً على احتياجات حماية البيانات الخاصة بك.
- يجب أن يحد منع الوصول غير المصرح به إلى المنصات المتعلقة بالدفع ويقلل من مستوى الضعف وإمكانية اختراق بيانات العملاء.
- مصرف ليبيا المركزي من خلال أدواته ومشغل شبكة الدفع المحلية بصفته مندوبه يضمن - أن يتم اتخاذ جميع الخطوات المناسبة بشكل صحيح لتأمين بيانات حاملي البطاقات والتحقق من امتثال الدفع المحدد مسبقاً والقواعد المعلنة والمنظمة من قبل مصرف ليبيا المركزي.

6.4 قواعد عامة لترميز البطاقات

- ترميز البطاقات يهدف إلى استبدال بيانات البطاقة الحساسة كرقم البطاقة وتاريخ انتهاء الصلاحية، ومعرفات البطاقة الخاصة برمز لإدارة الدفع بشكل آمن دون الحاجة إلى الحصول على جميع قيود PCI لمعاملات الدفع.
- يجب إدارة خدمة الترميز من خلال قبول مؤمن يطبق التشفير المطلوب على المعلومات المخزنة الحساسة، ويدعمه مكون حل كبوابة لإدارة دورة حياة الترميز والبطاقة، وكذلك للحصول على مجموعة من واجهات برمجة التطبيقات للتكامل مع جهات الإصدار وطالب الرمز الفريد API للارتباط بخوادم إدارة المحفظة، يجب أن تكون جميع المكونات المذكورة متوافقة تمامًا مع PCI-DSS.
- يجب أن يتوافق مصرف جهة الإصدار التي ترغب في الانضمام إلى خدمات الترميز التي تقدمها مخططات البطاقات الدولية أو منصة نمو DES بمجرد إنشائها مع APIS للتكامل المطلوب لربط مكون TSP الخاص بجهة الإصدار باحتياجات الشبكة ويجب أن يؤدي عملية الاعتماد المطلوبة قبل السماح له ببدء خدمة sch.
- بالنسبة لخدمات ترميز (Pay Apple ، Google Pay ، Samsung pay ، OEM ... إلخ) ، يجب أن يكون مشغل شبكة الدفع المحلية طرفاً في الاتفاقية.
- لن تبدأ خدمات ترميز OEM في دولة ليبيا دون الحصول على الموافقات الصحيحة من مصرف ليبيا المركزي

4.7 Clearing & Settlement for eCommerce & Digital Payment services

4.7.1 eCommerce clearing & Settlement

- Through the Payment Gateway a daily extraction file with all transactions processed Payment Gateway platform, segregated by Acquirer bank – (File for each acquirer) and contains all the transactions performed in last 24 hours prior the time of generating the file.
- The file shall be processed and converted to affect bank records and to be transformed into the recognized format of the clearing process.
- The acquirer banks may use the file during the time of processing to perform the proper settlement with their relevant merchants and deducted the standard agreed merchant discount rate and settling with the switch for the processing fees.

4.7.2 Mobile Digital payments clearing and settlement

Three types of transactions are subject to clearing and settlement for mobile digitized transactions.

1. Transactions made through a mobile wallet balance , this is been cleared using the same daily file of extraction, similar to what is used for the payment gateway and to be used for settling the balances of mobile line owners with their banks as well as performing the RTGS settlement needed between banks for reconciliation.
2. Transactions made through mobile wallet services such as bill payments or donations and any other type of issuer related and managed functions are to be handled by the Issuer bank and the operator of the wallet through internal accounting and reconciliation services.
3. Transactions made through HCE wallet either visa OEM or through a tokenization wallet managed by the Issuers , this goes through the normal flow of card based transactions, however if there is a part related to OEM the final clearance process got to extract certain reporting mechanism and approved process from CBL to settle and clear such transactions to credit the OEM share of processing fees.

4.8 Linked Value-added services

Additional Value-added services can be introduced through existing solutions which lies under the services of acceptance such as.

- Relying on the existing payment gateway to support Soft-POS acceptance.
- EFT POS is another alternative that can be implemented relying on back end and switch services behaving as an adaptor to translate standard commercial cashier transactions into a structured payment transaction.
- Other services can be introduced such as Aggregation services for multiple merchants which is a role that can be taken through Web based solution providers by hosting multiple merchants web pages and associate through one deal with an acquirer to perform the payment through its' payment gateway.

7.4. المقاصة والتسوية للتجارة الإلكترونية وخدمات الدفع الرقمي

1.7.4. مقاصة وتسوية التجارة الإلكترونية

- من خلال بوابة الدفع، ملف استخراج يومي مع جميع المعاملات التي تمت معالجتها، ومنصة بوابة الدفع، مفصولة عن طريق مصرف التاجر - (ملف لكل قابل) ويحتوي على جميع المعاملات المنجزة في آخر 24 ساعة قبل وقت إنشاء الملف.
- يجب معالجة الملف وتحويله للتأثير على السجلات المصرفية وتحويله إلى التنسيق المعترف به لعملية المقاصة.
- يجوز للمصارف المقتنية استخدام الملف أثناء وقت المعالجة لإجراء التسوية المناسبة مع التجار المعنيين وخصم معدل خصم التاجر القياسي المتفق عليه والتسوية مع التبديل لرسوم المعالجة.

2.7.4. مقاصة وتسوية المدفوعات الرقمية المتنقلة

هناك ثلاثة أنواع من المعاملات تخضع للمقاصة والتسوية للمعاملات الرقمية المتنقلة.

1. المعاملات التي تتم من خلال رصيد محفظة الهاتف المحمول، ويتم تصفيتا باستخدام نفس ملف الاستخراج اليومي، على غرار ما يتم استخدامه لبوابة الدفع ويستخدم لتسوية أرصدة أصحاب خطوط الهاتف المحمول مع مصارفهم وكذلك أداء تسوية RTGS اللازمة بين المصارف للتسوية فيما بينها.
2. المعاملات التي تتم من خلال خدمات المحفظة المتنقلة مثل مدفوعات الفواتير أو التبرعات، وأي نوع آخر من الوظائف ذات الصلة والمدارة بجهة الإصدار يتم التعامل معها من قبل المصرف المصدر ومشغل المحفظة من خلال خدمات المحاسبة والتسوية الداخلية.
3. المعاملات التي تتم من خلال محفظة HCE إما من خلال فيزا OEM أو من خلال محفظة الرموز الفريدة التي تديرها جهات الإصدار، وهذا يمر عبر التدفق الطبيعي للمعاملات القائمة على البطاقة، ولكن إذا كان هناك جزء متعلق بـ OEM ، فإن عملية التخليص النهائي يجب أن تستخرج آلية إبلاغ معينة وعملية معتمدة من مصرف ليبيا المركزي لتسوية وتصفية هذه المعاملات لاعتماد حصة OEM من رسوم المعالجة.

8.4. خدمات القيمة المضافة المرتبطة

يمكن تقديم خدمات القيمة المضافة الإضافية من خلال الحلول الحالية التي تقع ضمن خدمات القبول مثل.

- الاعتماد على بوابة الدفع الحالية لدعم قبول Soft-POS.
- EFT POS هو بديل آخر يمكن تنفيذه بالاعتماد على النهاية الخلفية وخدمات التبديل التي تتصرف كمحول لترجمة معاملات أمين الصندوق التجارية القياسية إلى معاملة دفع منظمة.
- يمكن تقديم خدمات أخرى مثل خدمات التجميع للعديد من التجار وهو الدور الذي يمكن القيام به من خلال موفري الحلول المستندة إلى الويب من خلال استضافة صفحات ويب متعددة للتجار والمشاركة من خلال صفقة واحدة مع القابل لإجراء الدفع من خلال بوابة الدفع الخاصة به.

Additional Value-added services can be introduced through existing solutions which lies under the services of acceptance such as.

- Relying on the existing payment gateway to support Soft-POS acceptance.
- EFT POS is another alternative that can be implemented relying on back end and switch services behaving as an adaptor to translate standard commercial cashier transactions into a structured payment transaction.
- Other services can be introduced such as Aggregation services for multiple merchants which is a role that can be taken through Web based solution providers by hosting multiple merchants web pages and associate through one deal with an acquirer to perform the payment through its' payment gateway.

يمكن تقديم خدمات القيمة المضافة الإضافية من خلال الحلول الحالية التي تقع ضمن خدمات القبول مثل.

- الاعتماد على بوابة الدفع الحالية لدعم قبول Soft-POS.
- EFT POS هو بديل آخر يمكن تنفيذه بالاعتماد على النهاية الخلفية وخدمات التبديل التي تتصرف كمحول لترجمة معاملات أمين الصندوق التجارية القياسية إلى معاملة دفع منظمة.
- يمكن تقديم خدمات أخرى مثل خدمات التجميع للعديد من التجار وهو الدور الذي يمكن أن يحدث من خلال موفري الحلول المستندة إلى الويب من خلال استضافة العديد من صفحات الويب الخاصة بالتجار والمشاركة من خلال صفقة واحدة مع القابل لإجراء الدفع من خلال بوابة الدفع الخاصة به.

Appendix Number 6



(الملحق رقم 6)

Appendix Number 7



(الملحق رقم 7)

Appendix Number 8



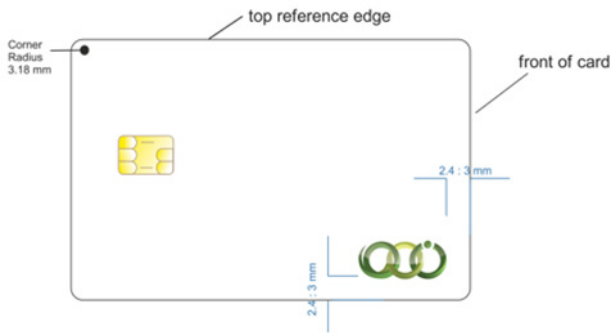
(الملحق رقم 8)

Appendix Number 9



(الملحق رقم 9)

Appendix Number 10



(الملحق رقم 10)

(الملحق رقم 1)

العنصر	الوصف	تغيير المسار	تغيير التاريخ

Appendix Number 1

Change Date	Track change	Description	ITEM

Appendix Number 2



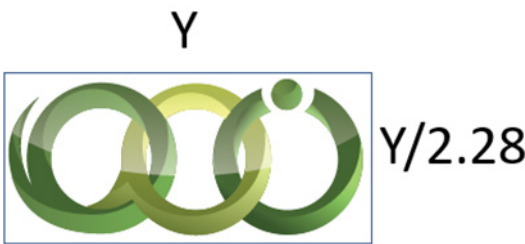
(الملحق رقم 2)

Appendix Number 3



(الملحق رقم 3)

Appendix Number 4



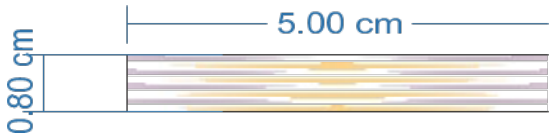
(الملحق رقم 4)

Appendix Number 5



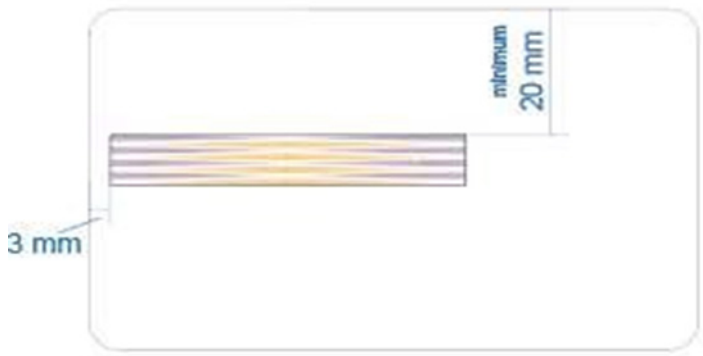
(الملحق رقم 5)

Appendix Number 14



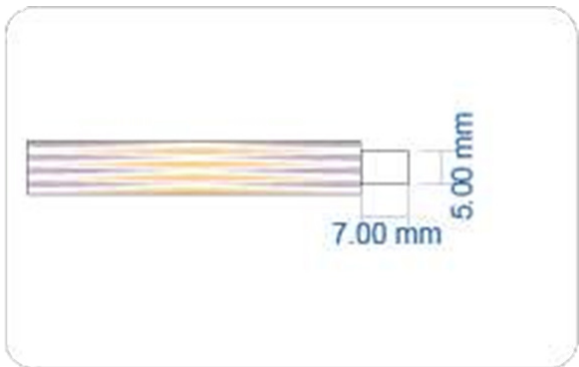
(الملحق رقم 15)

Appendix Number 15



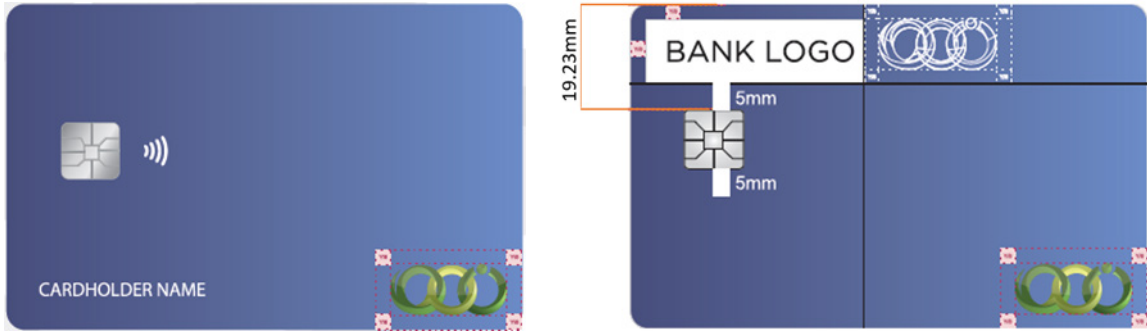
(الملحق رقم 16)

Appendix Number 17



(الملحق رقم 17)

Appendix Number 11



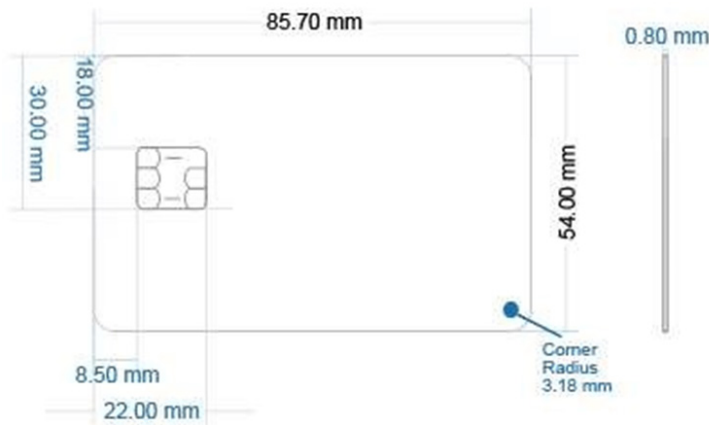
(الملحق رقم 11)

Appendix Number 12



(الملحق رقم 12)

Appendix Number 12



(الملحق رقم 13)

العرض	الارتفاع	السمك	الهدف	الحد الأدنى	الحد الأقصى	المستوى القبول
85.6 ملم	53.98 ملم	800 ميكرومتر	85.47 ملم	53.92 ملم	840 ميكرومتر	cpk 1
85.90 ملم	54.18 ملم	840 ميكرومتر	85.90 ملم	54.18 ملم	840 ميكرومتر	cpk 1
85.47 ملم	53.92 ملم	760 ميكرومتر	85.47 ملم	53.92 ملم	760 ميكرومتر	cpk 1

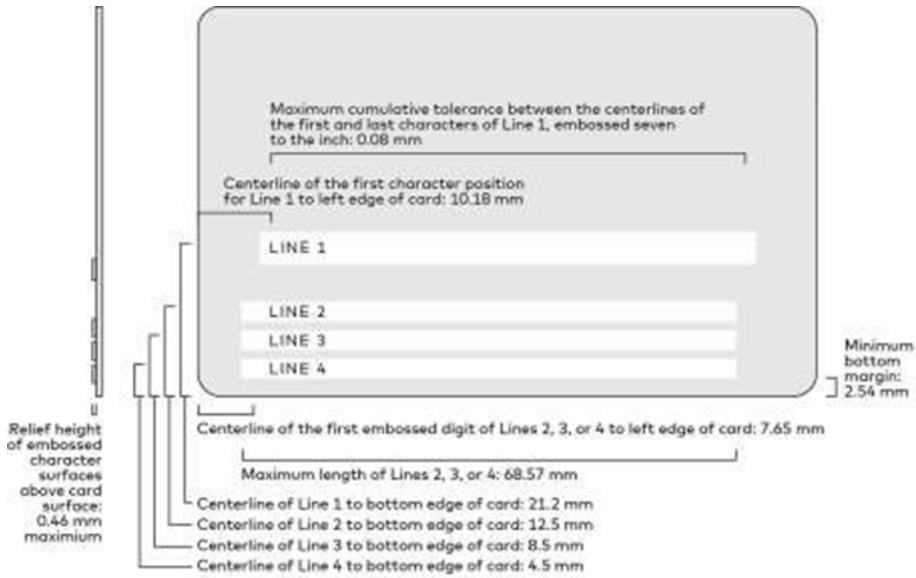
(الملحق رقم 14)

Appendix Number 14

Width	Height	Thickness	Target	Minimum	Maximum	Accept Level
85.6 mm	53.98 mm	800 Qm	85.47 mm	53.92 mm	840 Qm	1 cpk
85.90 mm	54.18 mm	840 Qm	85.90 mm	54.18 mm	840 Qm	1 cpk
85.47 mm	53.92 mm	760 Qm	85.47 mm	53.92 mm	760 Qm	1 cpk

Appendix Number 21

(الملحق رقم 21)



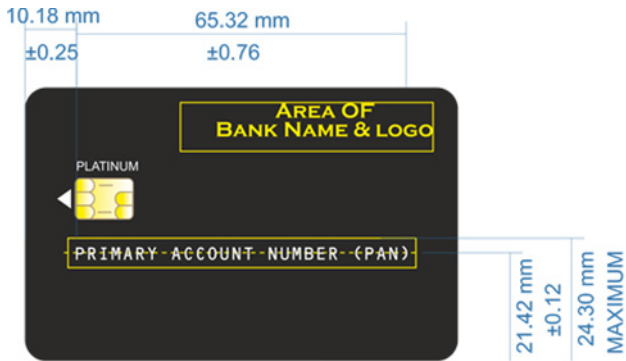
Appendix Number 22

(الملحق رقم 22)



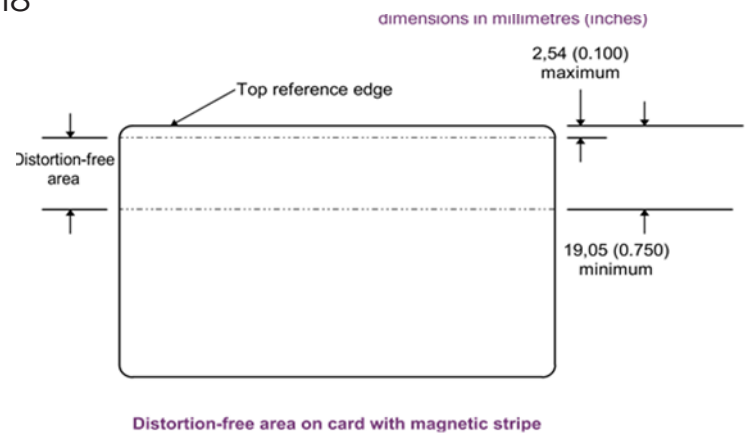
Appendix Number 23

(الملحق رقم 23)



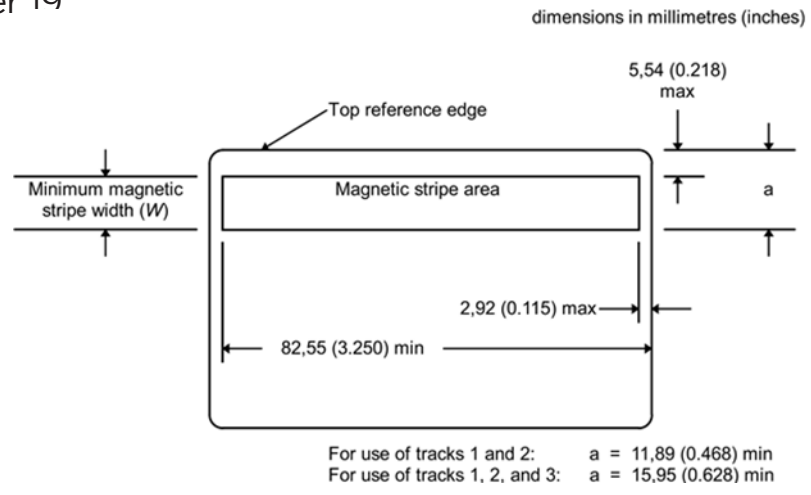
Appendix Number 18

(الملحق رقم 18)



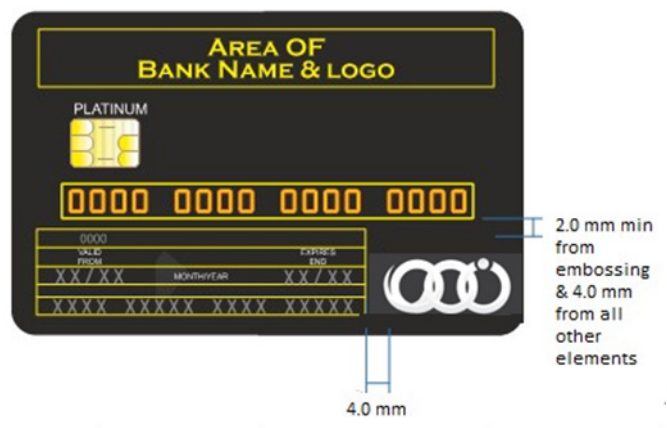
Appendix Number 19

(الملحق رقم 19)



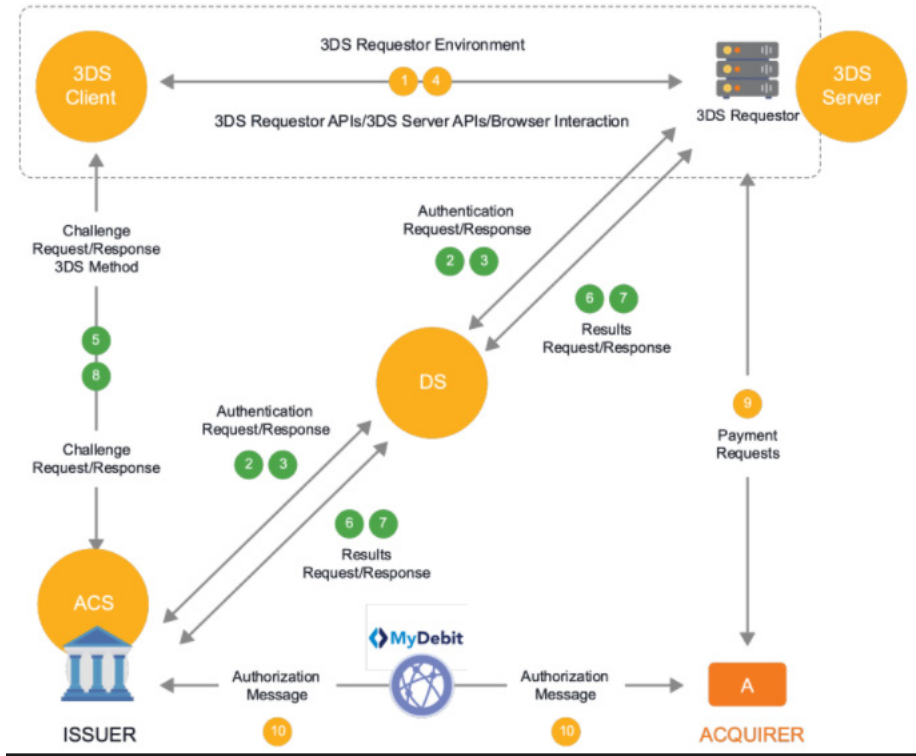
Appendix Number 20

(الملحق رقم 20)



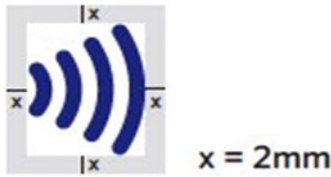
Appendix Number 28

(الملحق رقم 28)



Appendix Number 24

(الملحق رقم 24)



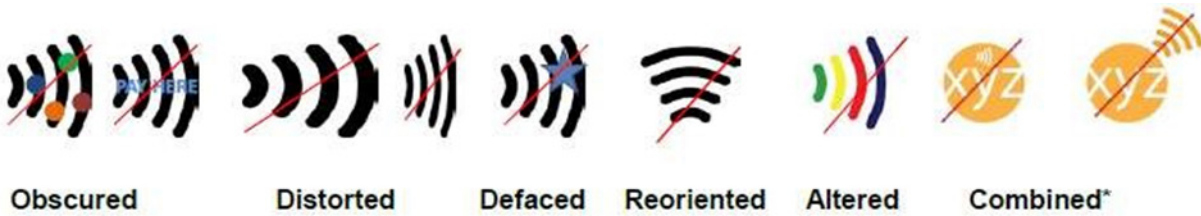
Appendix Number 25

(الملحق رقم 25)



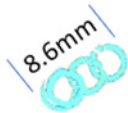
Appendix Number 26

(الملحق رقم 26)



Appendix Number 27

(الملحق رقم 27)





القواعد التنظيمية لشبكة الدفع المحلية الليبية

Regulatory Rules of The Libyan National Payment Scheme