



# Transaction Processing Rules

19 December 2019

## Summary of Changes, 19 December 2019

The following are changes with the most recent publication of this document.

Chapter Number	Rule Name	Source or Explanation of Revisions
Applicability of Rules in this Manual	Removed all occurrences of Mastercard Electronic.	See "AN 1343—Decommissioning of Mastercard Electronic," 1 December 2017.
Applicability of Rules in this Manual	Applicability of Rules in this Manual	See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.
Chapter 1—Connecting to the Interchange System and Authorization Routing	1.1 Connecting to the Interchange System	See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.
Chapter 1—Connecting to the Interchange System and Authorization Routing	1.2 Authorization Routing—Mastercard POS Transactions	See "AN 2208—Revised Standards—Use of Mastercard-Sourced BIN Tables," 19 June 2019.
	1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions	
Chapter 1—Connecting to the Interchange System and Authorization Routing	Europe Region 1.1 Connecting to the Interchange System	See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.
Chapter 1—Connecting to the Interchange System and Authorization Routing	Europe Region 1.2 Authorization Routing—Mastercard POS Transactions	See "AN 2208—Revised Standards—Use of Mastercard-Sourced BIN Tables," 19 June 2019.
Chapter 2—Authorization and Clearing Requirements	2.1 Acquirer Authorization Requirements	See "AN 1853—Revised Standards—Push Payment Transactions Mandate and MoneySend MCC Expansion," 18 March 2019.  See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.  See "AN 1430—Revised Standards—Refund Transactions," 16 December 2019.

Chapter Number	Rule Name	Source or Explanation of Revisions
Chapter 2—Authorization and Clearing Requirements	2.2 Issuer Authorization Requirements	See “AN 1853—Revised Standards—Push Payment Transactions Mandate and MoneySend MCC Expansion,” 18 March 2019.  See “AN 1430—Revised Standards—Refund Transactions,” 16 December 2019.
Chapter 2—Authorization and Clearing Requirements	2.2.1 Issuer Host System Requirements  2.11.1 Full and Partial Reversals—Acquirer Requirements  2.13 Refund Transactions and Corrections <b>(Renamed)</b>  2.13.1 Refund Transactions—Acquirer Requirements <b>(Added)</b>  2.13.2 Refund Transactions—Issuer Requirements <b>(Added)</b>	See “AN 1430—Revised Standards—Refund Transactions,” 16 December 2019.
Chapter 2—Authorization and Clearing Requirements	2.12 Full and Partial Approvals <b>(Renamed)</b>	See “AN 2815—Revised Standards—Global Support of Partial Approval and Balance Response,” 18 October 2019.
Chapter 2—Authorization and Clearing Requirements	Canada Region  2.12 Full and Partial Approvals <b>(Renamed)</b>	See “AN 2815—Revised Standards—Global Support of Partial Approval and Balance Response,” 18 October 2019.
Chapter 2—Authorization and Clearing Requirements	Europe Region  2.1 Acquirer Authorization Requirements	See “AN 1430—Revised Standards—Refund Transactions,” 16 December 2019.
Chapter 2—Authorization and Clearing Requirements	Europe Region  2.1 Acquirer Authorization Requirements  2.2 Issuer Authorization Requirements	See “AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions,” 11 November 2019.

Chapter Number	Rule Name	Source or Explanation of Revisions
Chapter 2—Authorization and Clearing Requirements	Europe Region 2.2.2 Stand-In Processing Service	Clarified the participation requirements for an Issuer in Armenia, Azerbaijan, Belarus, Georgia, Israel, Kazakhstan, Kyrgyzstan, Russian Federation, Switzerland, Tajikistan, Turkey, Turkmenistan, or Uzbekistan.
Chapter 2—Authorization and Clearing Requirements	Europe Region 2.12 Full and Partial Approvals <b>(Renamed)</b>	See "AN 2815—Revised Standards—Global Support of Partial Approval and Balance Response," 18 October 2019.
Chapter 2—Authorization and Clearing Requirements	Europe Region 2.13.1 Refund Transactions—Acquirer Requirements <b>(Added)</b> 2.13.2 Refund Transactions—Issuer Requirements <b>(Added)</b>	See "AN 1430—Revised Standards—Refund Transactions," 16 December 2019.
Chapter 2—Authorization and Clearing Requirements	Europe Region 2.21 Co-badged Cards—Acceptance Brand Identifier	See "AN 2892—Revised Standards—Application of the Interchange Fee Regulation in Iceland," 13 August 2019.
Chapter 2—Authorization and Clearing Requirements	United States Region 2.12 Full and Partial Approvals <b>(Renamed)</b>	See "AN 2815—Revised Standards—Global Support of Partial Approval and Balance Response," 18 October 2019.
Chapter 3—Acceptance Procedures	3.3.1 Mastercard POS Transaction Authorization Procedures	See "AN 1430—Revised Standards—Refund Transactions," 16 December 2019.
Chapter 3—Acceptance Procedures	3.4 Mastercard Cardholder Verification Requirements	See "AN 3375—Revised Standards—New Cybersecurity Standards and Programs Chapter," 7 November 2019.
Chapter 3—Acceptance Procedures	3.6 Use of a PIN for Transactions at ATM Terminals and Bank Branch Terminals	See "AN 2726—Revised Standards—Cardless ATM Powered by Mastercard Transactions," 11 June 2019.
Chapter 3—Acceptance Procedures	3.8 POI Currency Conversion	See "AN 2042—Revised Standards—Point-of-Interaction Currency Conversion," 5 December 2019.

Chapter Number	Rule Name	Source or Explanation of Revisions
Chapter 3—Acceptance Procedures	3.14 Returned Products and Canceled Services	See “AN 1430—Revised Standards—Refund Transactions,” 16 December 2019.
	3.14.1 Refund Transactions	
	3.15 Transaction Records	
Chapter 3—Acceptance Procedures	Europe Region 3.2 Card-Not-Present Transactions	See “AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions,” 11 November 2019.
Chapter 3—Acceptance Procedures	Europe Region 3.3.2 Maestro POS Transaction Authorization Procedures	See “AN 1430—Revised Standards—Refund Transactions,” 16 December 2019.
Chapter 4—Card-Present Transactions	4.9 Quick Payment Service (QPS) Program—Mastercard POS Transactions Only	See “AN 2780—Revised Standards—Revised MCC Descriptions,” 18 June 2019.
Chapter 4—Card-Present Transactions	4.11.1 Automated Fuel Dispenser Transactions	See “AN 2697—Revised Standards—Electronic Commerce Transactions at Automated Fuel Dispensers,” 17 May 2019.
Chapter 4—Card-Present Transactions	Europe Region 4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions	See “AN 2598—Revised Standards—PSD2 Impacts on CAT Level 2, Level 3, and Level 4 Terminals for the EEA Countries,” 5 August 2019.
Chapter 4—Card-Present Transactions	Europe Region 4.10 Purchase with Cash Back Transactions	See “AN 2373—Revised Standards—Introduction of Purchase with Cash Back Service in Switzerland,” 23 January 2019.
Chapter 4—Card-Present Transactions	Europe Region 4.11 Transactions at Unattended POS Terminals	See “AN 2598—Revised Standards—PSD2 Impacts on CAT Level 2, Level 3, and Level 4 Terminals for the EEA Countries,” 5 August 2019.
Chapter 5—Card-Not-Present Transactions	5.4 Recurring Payment Transactions 5.9 Merchant-initiated Transactions—EEA Only <b>(Added)</b>	See “AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions,” 11 November 2019.

Chapter Number	Rule Name	Source or Explanation of Revisions
Chapter 5—Card-Not-Present Transactions	Europe Region	See "AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions," 11 November 2019.
	5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements	
	5.1.2 E-commerce Transactions—Issuer Requirements	
	5.4 Recurring Payment Transactions	
Chapter 5—Card-Not-Present Transactions	Europe Region	See "AN 2780—Revised Standards—Revised MCC Descriptions," 18 June 2019.
	5.5 Installment Billing for Domestic Transactions—Participating Countries Only	See "AN 2975—Revised Standards—Installment Payment Services in Certain Countries in the Europe Region," 22 November 2019.
Chapter 5—Card-Not-Present Transactions	Europe Region	See "AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions," 11 November 2019.
	5.9 Merchant-initiated Transactions—EEA Only <b>(Added)</b>	
Chapter 6—Payment Transactions	6.1 Payment Transactions	See "AN 1853—Revised Standards—Push Payment Transactions Mandate and MoneySend MCC Expansion," 18 March 2019.
		See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.
Chapter 6—Payment Transactions	6.1.1 Payment Transactions—Acquirer and Merchant Requirements	See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.
Chapter 6—Payment Transactions	6.1.2 Payment Transactions—Issuer Requirements	See "AN 1853—Revised Standards—Push Payment Transactions Mandate and MoneySend MCC Expansion," 18 March 2019.
	6.3 MoneySend Payment Transactions	
		See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.

Chapter Number	Rule Name	Source or Explanation of Revisions
Chapter 6—Payment Transactions	Europe Region 6.1 Payment Transactions 6.2 Gaming Payment Transactions	See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.
Chapter 6—Payment Transactions	Middle East/Africa Region 6.2 Gaming Payment Transactions	See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.
Chapter 6—Payment Transactions	United States Region 6.2 Gaming Payment Transactions	See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.  See "AN 2814—Revised Standards—U.S. Region Gaming Payment Transactions May Process as Electronic Commerce," 8 July 2019.
Chapter 7—Terminal Requirements	7.2.1 Terminal Function Keys for PIN Entry <b>(Renamed)</b> 7.4.6 POS Terminals Using Electronic Signature Capture Technology (ESCT) <b>(Added)</b>	See "AN 3375—Revised Standards—New Cybersecurity Standards and Programs Chapter," 7 November 2019.
Chapter 7—Terminal Requirements	Europe Region 7.4 POS Terminal Requirements	See "AN 2865—Revised Standards—Széchenyi Leisure Cards Issued as Mastercard Prepaid Cards," 16 August 2019.
Chapter 7—Terminal Requirements	Europe Region 7.5 ATM Terminal and Bank Branch Terminal Requirements	See "AN 3407—Revised Standards—ATM Withdrawal Limits in Kazakhstan," 3 December 2019.
Chapter 7—Terminal Requirements	Europe Region 7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements	See "AN 2978—Revised Standards—Contactless to Become Standard in ATMs in Czech Republic and Poland," 18 November 2019.
Appendix B—Compliance Zones	Compliance Zones	Updated table to reflect current contents of this manual.

Chapter Number	Rule Name	Source or Explanation of Revisions
Appendix C—Transaction Identification Requirements	Payment Transactions	See "AN 1853—Revised Standards—Push Payment Transactions Mandate and MoneySend MCC Expansion," 18 March 2019.  See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.
Appendix C—Transaction Identification Requirements	Electronic Commerce Transactions	See "AN 2697—Revised Standards—Electronic Commerce Transactions at Automated Fuel Dispensers," 17 May 2019.
Appendix D—Cardholder-Activated Terminal (CAT) Transactions	Dual Capacity for CAT 1 and CAT 2	See "AN 2955—Revised Standards—Automated Fuel Dispenser Transaction Chargeback Liability," 23 October 2019.
Appendix D—Cardholder-Activated Terminal (CAT) Transactions	CAT Level 1: Automated Dispensing Machines (CAT 1)	See "AN 2450—Revised Standards—Mastercard Consumer-Presented QR Transactions," 12 June 2019.
Appendix E—CVM Limit Amounts	Europe Region (Belarus and Turkey Only)	See "AN 2974—Revised Standards—Cardholder Verification Method Limit Changes for Belarus, Sweden, and Turkey," 5 September 2019.
Appendix E—CVM Limit Amounts	Europe Region Middle East/Africa Region	See "AN 2719—Revised Standards—CVM Limit Changes in Israel, Kuwait, Poland, and Slovenia," 30 April 2019.
Appendix E—CVM Limit Amounts	Latin America and the Caribbean Region	See "AN 3345—Revised Standards—CVM Limit Changes in Argentina and Uruguay," 23 October 2019.
Appendix F—Signage, Screen, and Receipt Text Display	Model Screen Displays for Offering Installment Payments <b>(Added)</b>  Model Receipt Texts for Installments <b>(Added)</b>	See "AN 2975—Revised Standards—Installment Payment Services in Certain Countries in the Europe Region," 22 November 2019.



Chapter Number	Rule Name	Source or Explanation of Revisions
Appendix H—Definitions	Account Holder <b>(Added)</b> Activity(ies) Area of Use Association Customer, Association Corporation System <b>(Added)</b> Customer Customer Report Digitization, Digitize ICA <b>(Added)</b> Interchange System License, Licensed Mastercard Digital Enablement Service Mastercard Token Mastercard Token Account Range MoneySend Payment Transaction <b>(Added)</b> Non-Mastercard Funding Source <b>(Added)</b> Non-Mastercard Receiving Account <b>(Added)</b> Non-Mastercard Systems and Networks Standards <b>(Added)</b> Originating Account Holder <b>(Added)</b> Originating Institution (OI) <b>(Added)</b> Participation Payment Account Reference (PAR) Payment Transaction Payment Transfer Activity(ies) (PTA) <b>(Added)</b>	See “AN 2305—Revised Standards—Payment Transfer Activity Rules,” 12 April 2019.

Chapter Number	Rule Name	Source or Explanation of Revisions
	Point of Interaction (POI)	
	Processed PTA Transaction <b>(Added)</b>	
	Program	
	PTA Account <b>(Added)</b>	
	PTA Account Number <b>(Added)</b>	
	PTA Account Portfolio <b>(Added)</b>	
	PTA Agreement <b>(Added)</b>	
	PTA Customer <b>(Added)</b>	
	PTA Originating Account <b>(Added)</b>	
	PTA Program <b>(Added)</b>	
	PTA Receiving Account <b>(Added)</b>	
	PTA Settlement Guarantee Covered Program <b>(Added)</b>	
	PTA Settlement Obligation <b>(Added)</b>	
	PTA Transaction <b>(Added)</b>	
	Receiving Account Holder <b>(Added)</b>	
	Receiving Agent <b>(Added)</b>	
	Receiving Customer <b>(Added)</b>	
	Receiving Institution <b>(Added)</b>	
	Token	
	Tokenization, Tokenize	
	Transaction Data	
Appendix H—Definitions	Solicitation, Solicit	See "AN 2305—Revised Standards—Payment Transfer Activity Rules," 12 April 2019.  See "AN 2760—Revised Standards—Extension of Area of Use Programs," 5 June 2019.

---

Chapter Number	Rule Name	Source or Explanation of Revisions
Appendix H—Definitions	Strong Customer Authentication (SCA) <b>(Added)</b>	See “AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions,” 11 November 2019.

---

## Applicability of Rules in this Manual

This manual contains Rules for Activities.

The Rules in this manual pertain to the processing of Transactions and Payment Transactions. As used herein, a Transaction means a transaction resulting from the use of a Mastercard®, Maestro®, or Cirrus® Card, Access Device, or Account, as the case may be. As used herein, a Payment Transaction means a Payment Transfer Activity (PTA) Transaction that transfers funds to an Account. A Payment Transaction is not a credit that reverses a previous purchase (includes MoneySend Payment Transactions).

For the purposes of Standards applicable to Payment Transactions, Issuer means the Receiving Institution (RI), and Acquirer means the Originating Institution (OI).

The below table describes the applicability of the Rules for particular types of Transactions or Payment Transactions. Please note that the term “POS Transaction” refers to a Transaction that occurs at a Merchant location, whether in a Card-present environment at an attended or unattended POS Terminal, or in a Card-not-present environment. In a Card-not-present environment, this may include electronic commerce (“e-commerce”), mail order, phone order, or recurring payment Transactions.

Rules relating to... <sup>1</sup>	Apply to...
Mastercard POS Transactions	A POS Transaction conducted with a Mastercard Card.
Maestro POS Transactions	A POS Transaction conducted with: <ul style="list-style-type: none"> <li>• A Maestro Card, or</li> <li>• A Mastercard Card issued using a BIN identified by the Corporation as “Debit Mastercard” and routed to the Mastercard® Single Message System.</li> </ul>
ATM Transactions	A Transaction conducted with a Mastercard, Maestro, or Cirrus Card at an ATM Terminal and routed to the Interchange System.
Manual Cash Disbursement Transactions	A cash withdrawal Transaction conducted at: <ul style="list-style-type: none"> <li>• A Customer financial institution teller or Bank Branch Terminal with a Mastercard Card, or</li> <li>• A Bank Branch Terminal with a Maestro or Cirrus Card and routed to the Interchange System.</li> </ul>
Mastercard Mobile Remote Payment (MMRP) Transactions	A POS Transaction performed by an enrolled consumer using a mobile device registered by the Issuer or its Service Manager and having Mastercard Mobile Remote Payment functionality. The consumer, as a Mastercard or Maestro Cardholder, initiates and authenticates payments by entering a PIN or mobile-specific credentials on the mobile device.

<sup>1</sup> If a particular brand or brands is not mentioned in a Rule that applies to Transactions, then the Rule applies to Mastercard, Maestro, and Cirrus.

---

Rules relating to... <sup>1</sup>	Apply to...
Payment Transactions	A PTA Transaction that transfers funds to an Account. A Payment Transaction is not a credit that reverses a previous purchase. Includes MoneySend Payment Transactions.

---

### Modifying Words and Acronyms

From time to time, the meanings of the above terms are modified by the addition of another word or acronym. For example, a Debit Mastercard POS Transaction means a Transaction resulting from the use of a Debit Mastercard Card at the point of sale (POS). However, for ease of use, not every modifying term is defined. While Mastercard alone interprets and enforces its Rules and other Standards, these *Transaction Processing Rules* endeavor to use defined terms and other terms and terminology in a plain manner that will be generally understood in the payments industry.

### Variations and Additions to the Rules for a Geographic Area

Variations and/or additions (“modifications”) to the Rules are applicable in geographic areas, whether a country, a number of countries, a region, or other area. In the event of a conflict between a Rule and a variation of that Rule, the modification is afforded precedence and is applicable. The Rules set forth in this manual are Standards and Mastercard has the sole right to interpret and enforce the Rules and other Standards.

---

<sup>1</sup> If a particular brand or brands is not mentioned in a Rule that applies to Transactions, then the Rule applies to Mastercard, Maestro, and Cirrus.

# Contents

<b>Summary of Changes, 19 December 2019.....</b>	<b>2</b>
--------------------------------------------------	----------

<b>Applicability of Rules in this Manual.....</b>	<b>12</b>
---------------------------------------------------	-----------

<b>Chapter 1: Connecting to the Interchange System and Authorization Routing.....</b>	<b>28</b>
---------------------------------------------------------------------------------------	-----------

1.1 Connecting to the Interchange System.....	30
1.2 Authorization Routing—Mastercard POS Transactions.....	30
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions.....	31
1.3.1 Routing Instructions and System Maintenance.....	31
1.3.2 Chip Transaction Routing.....	31
1.3.3 Domestic Transaction Routing.....	32
1.4 ATM Terminal Connection to the Interchange System.....	32
1.5 Gateway Processing.....	32
1.6 POS Terminal Connection to the Interchange System.....	33
Variations and Additions by Region.....	33
Asia/Pacific Region.....	33
1.4 ATM Terminal Connection to the Interchange System.....	33
1.6 POS Terminal Connection to the Interchange System.....	33
Canada Region.....	34
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions.....	34
1.3.3 Domestic Transaction Routing.....	34
1.4 ATM Terminal Connection to the Interchange System.....	34
Europe Region.....	34
1.1 Connecting to the Interchange System.....	34
1.2 Authorization Routing—Mastercard POS Transactions.....	35
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions.....	35
1.3.2 Chip Transaction Routing.....	35
1.3.3 Domestic Transaction Routing.....	35
1.4 ATM Terminal Connection to the Interchange System—SEPA Only.....	35
Latin America and the Caribbean Region.....	35
1.4 ATM Terminal Connection to the Interchange System.....	35
1.6 POS Terminal Connection to the Interchange System.....	36
United States Region.....	36
1.1 Connecting to the Interchange System.....	36
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions.....	36
1.3.1 Routing Instructions and System Maintenance.....	36
1.3.3 Domestic Transaction Routing.....	37

1.4 ATM Terminal Connection to the Interchange System.....	37
Additional U.S. Region and U.S. Territory Rules.....	37
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions.....	37

## **Chapter 2: Authorization and Clearing Requirements..... 39**

2.1 Acquirer Authorization Requirements.....	42
2.1.1 Acquirer Host System Requirements—U.S. Region Only.....	42
2.2 Issuer Authorization Requirements.....	43
2.2.1 Issuer Host System Requirements.....	43
2.2.2 Stand-In Processing Service.....	44
Accumulative Transaction Limits.....	44
Chip Cryptogram Validation in Stand-In.....	45
2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers.....	45
2.3 Authorization Responses.....	45
2.4 Performance Standards.....	46
2.4.1 Performance Standards—Acquirer Requirements.....	46
2.4.2 Performance Standards—Issuer Requirements.....	46
Issuer Failure Rate (Substandard Level 1).....	46
Issuer Failure Rate (Substandard Level 2).....	47
Calculation of the Issuer Failure Rate.....	47
2.5 Preauthorizations.....	47
2.5.1 Preauthorizations—Mastercard POS Transactions.....	47
2.5.2 Preauthorizations—Maestro POS Transactions.....	48
2.5.3 Preauthorizations—ATM and Manual Cash Disbursement Transactions.....	48
2.6 Undefined Authorizations.....	48
2.7 Final Authorizations.....	49
2.8 Message Reason Code 4808 Chargeback Protection Period.....	49
2.9 Multiple Authorizations.....	50
2.10 Multiple Clearing Messages.....	51
2.11 Full and Partial Reversals.....	52
2.11.1 Full and Partial Reversals—Acquirer Requirements.....	52
2.11.2 Full and Partial Reversals—Issuer Requirements.....	53
2.11.3 Reversal for Conversion of Approval to Decline.....	53
2.11.4 Reversal to Cancel Transaction.....	54
2.12 Full and Partial Approvals .....	54
2.13 Refund Transactions and Corrections.....	55
2.13.1 Refund Transactions—Acquirer Requirements.....	56
2.13.2 Refund Transactions—Issuer Requirements.....	56
2.14 Balance Inquiries.....	57
2.15 CVC 2 Verification for POS Transactions.....	58
2.16 CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless Transactions— Brazil Only.....	58

---

2.17 Euro Conversion—Europe Region Only.....	58
2.18 Transaction Queries and Disputes.....	58
2.18.1 Retrieval Requests and Fulfillments.....	58
2.18.2 Compliance with Dispute Procedures.....	59
2.19 Chargebacks for Reissued Cards.....	59
2.20 Correction of Errors.....	59
2.21 Co-badged Cards—Acceptance Brand Identifier.....	59
Variations and Additions by Region.....	59
Asia/Pacific Region.....	60
2.1 Acquirer Authorization Requirements.....	60
2.2 Issuer Authorization Requirements.....	60
2.2.1 Issuer Host System Requirements.....	60
2.5 Preauthorizations.....	60
2.5.2 Preauthorizations—Maestro POS Transactions.....	60
Canada Region.....	60
2.2 Issuer Authorization Requirements.....	60
2.12 Full and Partial Approvals.....	60
Europe Region.....	62
2.1 Acquirer Authorization Requirements.....	62
2.2 Issuer Authorization Requirements.....	63
2.2.2 Stand-In Processing Service.....	64
2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers.....	65
2.3 Authorization Responses.....	65
2.4 Performance Standards.....	65
2.4.2 Performance Standards—Issuer Requirements.....	65
2.5 Preauthorizations.....	65
2.5.2 Preauthorizations—Maestro POS Transactions.....	66
2.5.3 Preauthorizations—ATM and Manual Cash Disbursement Transactions.....	66
2.7 Final Authorizations.....	67
2.8 Message Reason Code 4808 Chargeback Protection Period.....	67
2.9 Multiple Authorizations.....	67
2.11 Full and Partial Reversals.....	68
2.11.1 Full and Partial Reversals—Acquirer Requirements.....	68
2.11.2 Full and Partial Reversals—Issuer Requirements.....	69
2.12 Full and Partial Approvals.....	69
2.13 Refund Transactions and Corrections.....	70
2.13.1 Refund Transactions—Acquirer Requirements.....	70
2.13.2 Refund Transactions—Issuer Requirements.....	70
2.14 Balance Inquiries.....	70
2.15 CVC 2 Verification for POS Transactions.....	71
2.17 Euro Conversion.....	71
2.21 Co-badged Cards—Acceptance Brand Identifier.....	72
Latin America and the Caribbean Region.....	73



2.16 CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless—Brazil Only...73	73
United States Region.....	73
2.1 Acquirer Authorization Requirements.....	73
2.1.1 Acquirer Host System Requirements.....	73
2.2 Issuer Authorization Requirements.....	73
2.2.1 Issuer Host System Requirements.....	74
2.2.2 Stand-In Processing Service.....	74
2.4 Performance Standards.....	75
2.4.2 Performance Standards—Issuer Requirements.....	76
2.5 Preauthorizations.....	76
2.5.2 Preauthorizations—Maestro POS Transactions.....	76
2.11 Full and Partial Reversals.....	76
2.11.1 Full and Partial Reversals—Acquirer Requirements.....	76
2.11.2 Full and Partial Reversals—Issuer Requirements.....	78
2.12 Full and Partial Approvals.....	78
2.14 Balance Inquiries.....	78

## **Chapter 3: Acceptance Procedures.....79**

3.1 Card-Present Transactions.....	82
3.1.1 Mastercard Card Acceptance Procedures.....	82
Suspicious Cards.....	83
3.1.2 Maestro Card Acceptance Procedures.....	83
3.2 Card-Not-Present Transactions.....	83
3.3 Obtaining an Authorization.....	83
3.3.1 Mastercard POS Transaction Authorization Procedures.....	83
Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions.....	84
Authorization When the Cardholder Adds a Gratuity.....	85
Card-Not-Present Transaction Declines.....	85
Use of Card Validation Code (CVC) 2.....	86
Capture Card Response.....	86
3.3.2 Maestro POS Transaction Authorization Procedures.....	86
3.4 Mastercard Cardholder Verification Requirements.....	87
CVM Not Required for Refund Transactions.....	88
Use of PIN for Mastercard Magnetic Stripe Transactions.....	88
3.5 Maestro Cardholder Verification Requirements.....	88
3.6 Use of a PIN for Transactions at ATM Terminals and Bank Branch Terminals.....	89
3.7 Use of a Consumer Device CVM.....	90
3.8 POI Currency Conversion.....	90
3.8.1 Cardholder Disclosure—Attended POS Terminal.....	91
3.8.2 Cardholder Disclosure—Unattended POS Terminal.....	91
3.8.3 Cardholder Disclosure—ATM Terminal.....	92
3.8.4 Cardholder Disclosure—Transaction Receipt Information.....	92

3.8.5 Transaction Processing Requirements.....	92
3.9 Multiple Transactions—Mastercard POS Transactions Only.....	93
3.10 Partial Payment—Mastercard POS Transactions Only.....	93
3.11 Specific Terms of a Transaction.....	94
3.11.1 Specific Terms of an E-commerce Transaction.....	94
3.12 Charges for Loss, Theft, or Damage—Mastercard POS Transactions Only.....	94
3.13 Providing a Transaction Receipt.....	95
3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements.....	96
3.13.2 ATM and Bank Branch Terminal Transaction Receipt Requirements.....	97
3.13.3 Primary Account Number (PAN) Truncation and Expiration Date Omission.....	98
3.13.4 Prohibited Information.....	98
3.13.5 Standard Wording for Formsets.....	98
3.14 Returned Products and Canceled Services.....	99
3.14.1 Refund Transactions.....	99
3.15 Transaction Records.....	101
3.15.1 Retention of Transaction Records.....	101
Variations and Additions by Region.....	101
Asia/Pacific Region.....	101
3.14 Returned Products and Canceled Services.....	102
3.14.1 Refund Transactions.....	102
Canada Region.....	102
Europe Region.....	102
3.1 Card-Present Transactions.....	102
3.1.1 Mastercard Card Acceptance Procedures.....	102
3.2 Card-Not-Present Transactions.....	102
3.3 Obtaining an Authorization.....	103
3.3.1 Mastercard POS Transaction Authorization Procedures.....	103
Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions.....	103
Authorization When the Cardholder Adds a Gratuity.....	103
3.3.2 Maestro POS Transaction Authorization Procedures.....	103
3.5 Maestro Cardholder Verification Requirements.....	104
3.8 POI Currency Conversion.....	104
3.13 Providing a Transaction Receipt.....	104
3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements.....	104
3.13.3 Primary Account Number (PAN) Truncation and Expiration Date Omission...	105
3.14 Returned Products and Canceled Services.....	105
3.14.1 Refund Transactions.....	105
Latin America and the Caribbean Region.....	105
3.5 Maestro Cardholder Verification Requirements.....	106
Middle East/Africa Region.....	106
3.14 Returned Products and Canceled Services.....	106

3.14.1 Refund Transactions.....	106
United States Region.....	106
3.3 Obtaining an Authorization.....	106
3.3.1 Mastercard POS Transaction Authorization Procedures.....	106
Authorization When the Cardholder Adds a Gratuity.....	106
3.5 Maestro Cardholder Verification Requirements.....	107
Additional U.S. Region and U.S. Territory Rules.....	107
3.14 Returned Products and Canceled Services.....	108
3.14.1 Refund Transactions.....	108

## **Chapter 4: Card-Present Transactions..... 109**

4.1 Chip Transactions at Hybrid Terminals.....	112
4.2 Offline Transactions Performed on Board Planes, Trains, and Ships.....	112
4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions—Europe Region Only.....	113
4.4 Contactless Transactions at POS Terminals.....	113
4.5 Contactless Transit Aggregated Transactions.....	114
4.5.1 Mastercard Contactless Transit Aggregated Transactions.....	114
4.5.2 Maestro Contactless Transit Aggregated Transactions.....	115
4.6 Contactless Transactions at ATM Terminals.....	115
4.7 Contactless-only Acceptance.....	116
4.8 Mastercard Consumer-Presented QR Transactions at POS Terminals.....	117
4.9 Quick Payment Service (QPS) Program—Mastercard POS Transactions Only.....	117
4.10 Purchase with Cash Back Transactions.....	118
4.11 Transactions at Unattended POS Terminals.....	119
4.11.1 Automated Fuel Dispenser Transactions.....	119
4.12 PIN-based Debit Transactions—United States Region Only.....	120
4.13 PIN-less Single Message Transactions—United States Region Only.....	120
4.14 Merchant-approved Maestro POS Transactions.....	120
4.15 Mastercard Manual Cash Disbursement Transactions.....	121
4.15.1 Non-discrimination Regarding Cash Disbursement Services.....	121
4.15.2 Maximum Cash Disbursement Amounts.....	121
4.15.3 Discount or Service Charges.....	122
4.15.4 Mastercard Acceptance Mark Must Be Displayed.....	122
4.16 Encashment of Mastercard Travelers Cheques.....	122
4.17 ATM Transactions.....	122
4.17.1 “Chained” Transactions.....	123
4.17.2 ATM Transaction Branding.....	123
4.18 ATM Access Fees.....	123
4.18.1 ATM Access Fees—Domestic Transactions.....	123
4.18.2 ATM Access Fees—Cross-border Transactions.....	123
4.18.3 ATM Access Fee Requirements.....	123

Transaction Field Specifications for ATM Access Fees.....	124
Non-discrimination Regarding ATM Access Fees.....	124
Notification of ATM Access Fee.....	124
Cancellation of Transaction.....	124
Sponsor Approval of Proposed Signage, Screen Display, and Receipt.....	124
ATM Terminal Signage.....	124
ATM Terminal Screen Display.....	125
ATM Transaction Receipts.....	125
4.19 Merchandise Transactions at ATM Terminals.....	126
4.19.1 Approved Merchandise Categories.....	126
4.19.2 Screen Display Requirement for Merchandise Categories.....	127
4.20 Shared Deposits—United States Region Only.....	127
Variations and Additions by Region.....	127
Asia/Pacific Region.....	127
4.10 Purchase with Cash Back Transactions.....	127
4.11 Transactions at Unattended POS Terminals.....	127
4.11.1 Automated Fuel Dispenser Transactions.....	127
4.18 ATM Access Fees.....	128
4.18.1 ATM Access Fees—Domestic Transactions.....	128
Canada Region.....	128
4.10 Purchase with Cash Back Transactions.....	128
4.11 Transactions at Unattended POS Terminals.....	129
4.11.1 Automated Fuel Dispenser Transactions.....	129
4.18 ATM Access Fees.....	129
4.18.1 ATM Access Fees—Domestic Transactions.....	129
Europe Region.....	129
4.1 Chip Transactions at Hybrid Terminals.....	129
4.2 Offline Transactions Performed on Board Planes, Trains, and Ships.....	129
4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions.....	129
4.4 Contactless Transactions at POS Terminals.....	130
4.5 Contactless Transit Aggregated Transactions.....	131
4.5.1 Mastercard Contactless Transit Aggregated Transactions.....	131
4.5.2 Maestro Contactless Transit Aggregated Transactions.....	131
4.10 Purchase with Cash Back Transactions.....	132
4.11 Transactions at Unattended POS Terminals.....	134
4.11.1 Automated Fuel Dispenser Transactions.....	135
4.14 Merchant-approved Maestro POS Transactions.....	136
4.15 Mastercard Manual Cash Disbursement Transactions.....	136
4.15.2 Maximum Cash Disbursement Amounts.....	136
4.18 ATM Access Fees.....	136
4.18.1 ATM Access Fees—Domestic Transactions.....	136
4.19 Merchandise Transactions at ATM Terminals.....	137
4.19.1 Approved Merchandise Categories.....	137

Latin America and the Caribbean Region.....	137
4.4 Contactless Transactions at POS Terminals.....	137
4.5 Contactless Transit Aggregated Transactions.....	137
4.5.2 Maestro Contactless Transit Aggregated Transactions.....	137
4.10 Purchase with Cash Back Transactions.....	138
4.18 ATM Access Fees.....	139
4.18.1 ATM Access Fees—Domestic Transactions.....	139
Middle East/Africa Region.....	140
4.10 Purchase with Cash Back Transactions.....	140
United States Region.....	141
4.1 Chip Transactions at Hybrid Terminals.....	141
4.10 Purchase with Cash Back Transactions.....	141
4.11 Transactions at Unattended POS Terminals.....	141
4.11.1 Automated Fuel Dispenser Transactions.....	142
4.12 PIN-based Debit Transactions.....	142
4.13 PIN-less Single Message Transactions.....	142
4.15 Mastercard Manual Cash Disbursement Transactions.....	143
4.15.2 Maximum Cash Disbursement Amounts.....	143
4.15.3 Discount or Service Charges.....	143
4.18 ATM Access Fees.....	144
4.18.1 ATM Access Fees—Domestic Transactions.....	144
4.19 Merchandise Transactions at ATM Terminals.....	144
4.19.1 Approved Merchandise Categories.....	144
4.20 Shared Deposits.....	144
4.20.1 Non-discrimination Regarding Shared Deposits.....	144
4.20.2 Terminal Signs and Notices.....	144
4.20.3 Maximum Shared Deposit Amount.....	144
4.20.4 Deposit Verification.....	144
4.20.5 ATM Terminal Clearing and Deposit Processing.....	145
4.20.6 Shared Deposits in Excess of USD 10,000.....	146
4.20.7 Notice of Return.....	146
4.20.8 Liability for Shared Deposits.....	146

## **Chapter 5: Card-Not-Present Transactions..... 147**

5.1 Electronic Commerce Transactions.....	149
5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements.....	149
5.1.2 E-commerce Transactions—Issuer Requirements.....	151
5.1.3 Use of Static AAV for Card-not-present Transactions.....	152
5.2 Mail Order and Telephone Order (MO/TO) Transactions.....	152
5.3 Credential-on-File Transactions.....	153
5.4 Recurring Payment Transactions.....	153

5.4.1 Recurring Payment Transactions for High-Risk Negative Option Billing Merchants.....	155
5.5 Installment Billing for Domestic Transactions—Participating Countries Only.....	156
5.5.1 Applicability of Rules.....	157
5.5.2 Definitions.....	157
5.5.3 Transaction Processing Procedures.....	158
5.6 Transit Transactions Performed for Debt Recovery.....	159
5.7 Use of Automatic Billing Updater.....	159
5.8 Authentication Requirements—Europe Region Only.....	160
5.9 Merchant-initiated Transactions—EEA Only.....	160
Variations and Additions by Region.....	160
Asia/Pacific Region.....	160
5.1 Electronic Commerce Transactions.....	160
5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements.....	161
5.1.2 E-commerce Transactions—Issuer Requirements.....	161
5.2 Mail Order and Telephone Order (MO/TO) Transactions.....	162
5.3 Credential-on-File Transactions.....	163
5.7 Use of Automatic Billing Updater.....	163
Canada Region.....	163
5.7 Use of Automatic Billing Updater.....	163
Europe Region.....	163
5.1 Electronic Commerce Transactions.....	163
5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements.....	163
5.1.2 E-commerce Transactions—Issuer Requirements.....	164
5.1.3 Use of Static AAV for Card-not-present Transactions.....	165
5.2 Mail Order and Telephone Order (MO/TO) Maestro Transactions.....	166
5.2.1 Definitions.....	166
5.2.2 Intracountry Maestro MO/TO Transactions—Cardholder Authority.....	167
5.2.3 Intracountry Maestro MO/TO Transactions—Transactions Per Cardholder Authority.....	167
5.2.4 Intracountry Maestro MO/TO Transactions—CVC 2/AVS Checks.....	167
5.3 Credential-on-File Transactions.....	168
5.4 Recurring Payment Transactions.....	168
5.5 Installment Billing for Domestic Transactions—Participating Countries Only.....	169
5.5.3 Transaction Processing Procedures.....	180
5.6 Transit Transactions Performed for Debt Recovery.....	181
5.7 Use of Automatic Billing Updater.....	181
5.7.1 Issuer Requirements.....	181
5.7.2 Acquirer Requirements.....	182
5.8 Authentication Requirements.....	184
5.8.1 Acquirer Requirements.....	184
5.8.2 Issuer Requirements.....	187
5.9 Merchant-initiated Transactions – EEA Only.....	187

Latin America and the Caribbean Region.....	188
5.1 Electronic Commerce Transactions.....	188
5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements.....	188
5.1.2 E-commerce Transactions—Issuer Requirements.....	189
5.7 Use of Automatic Billing Updater.....	189
Middle East/Africa Region.....	189
5.1 Electronic Commerce Transactions.....	189
5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements.....	189
5.1.2 E-commerce Transactions—Issuer Requirements.....	189
5.7 Use of Automatic Billing Updater.....	189
United States Region.....	190
5.7 Use of Automatic Billing Updater.....	190
<b>Chapter 6: Payment Transactions.....</b>	<b>191</b>
6.1 Payment Transactions.....	192
6.1.1 Payment Transactions—Acquirer and Merchant Requirements.....	192
6.1.2 Payment Transactions—Issuer Requirements.....	193
6.2 Gaming Payment Transactions.....	194
6.3 MoneySend Payment Transactions.....	194
Variations and Additions by Region.....	194
Europe Region.....	194
6.1 Payment Transactions.....	195
6.1.1 Payment Transactions—Acquirer and Merchant Requirements.....	195
6.1.2 Payment Transactions—Issuer Requirements.....	195
6.2 Gaming Payment Transactions.....	195
6.3 MoneySend Payment Transactions.....	198
Middle East/Africa Region.....	198
6.2 Gaming Payment Transactions.....	198
United States Region.....	199
6.2 Gaming Payment Transactions.....	199
<b>Chapter 7: Terminal Requirements.....</b>	<b>201</b>
7.1 Terminal Eligibility.....	204
7.2 Terminal Requirements.....	204
7.2.1 Terminal Function Keys for PIN Entry.....	205
7.2.2 Terminal Responses.....	206
7.2.3 Terminal Transaction Log.....	206
7.3 Contactless Payment Functionality.....	206
7.3.1 Contactless Reader Requirements.....	207
7.4 POS Terminal Requirements.....	207
7.4.1 Contactless-enabled POS Terminals.....	208

7.4.2 Contactless-only POS Terminals.....	209
7.4.3 Mobile POS (MPOS) Terminals.....	210
7.4.4 Mastercard Consumer-Presented QR-enabled POS Terminals.....	211
7.4.5 Signature-based Maestro POS Terminals.....	211
7.4.6 POS Terminals Using Electronic Signature Capture Technology (ESCT).....	211
7.5 ATM Terminal and Bank Branch Terminal Requirements.....	212
7.5.1 ATM Terminals.....	213
7.5.2 Bank Branch Terminals.....	213
7.5.3 Contactless Payment Functionality.....	213
7.6 Hybrid Terminal Requirements.....	213
7.6.1 Hybrid POS Terminal Requirements.....	214
Hybrid POS Terminal and Chip-only MPOS Terminal Displays.....	215
7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements.....	215
7.7 Mastercard Consumer-Presented QR Functionality.....	216
Variations and Additions by Region.....	216
Asia/Pacific Region.....	216
7.3 Contactless Payment Functionality.....	216
7.4 POS Terminal Requirements.....	217
7.4.3 Mobile POS (MPOS) Terminals.....	218
7.5 ATM Terminal and Bank Branch Terminal Requirements.....	218
7.6 Hybrid Terminal Requirements.....	219
Canada Region.....	219
7.3 Contactless Payment Functionality.....	219
7.4 POS Terminal Requirements.....	219
7.4.1 Contactless-enabled POS Terminals.....	219
7.4.3 Mobile POS (MPOS) Terminals.....	219
7.4.4 Mastercard Consumer-Presented QR-enabled POS Terminals.....	219
7.5 ATM Terminal and Bank Branch Terminal Requirements.....	220
Europe Region.....	220
7.1 Terminal Eligibility.....	220
7.2 Terminal Requirements.....	220
7.3 Contactless Payment Functionality.....	220
7.3.1 Contactless Reader Requirements.....	221
7.4 POS Terminal Requirements.....	221
7.4.1 Contactless-enabled POS Terminals.....	221
7.4.3 Mobile POS (MPOS) Terminals.....	224
7.4.5 Signature-based Maestro POS Terminals.....	225
7.5 ATM Terminal and Bank Branch Terminal Requirements.....	225
7.5.2 Bank Branch Terminals.....	226
7.6 Hybrid Terminal Requirements.....	226
7.6.1 Hybrid POS Terminal Requirements.....	226
7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements.....	226
Latin America and the Caribbean Region.....	227



7.3 Contactless Payment Functionality.....	227
7.4 POS Terminal Requirements.....	227
7.4.1 Contactless-enabled POS Terminals.....	228
7.6 Hybrid Terminal Requirements.....	228
Middle East/Africa Region.....	228
7.3 Contactless Payment Functionality.....	228
7.3.1 Contactless Reader Requirements.....	228
7.6 Hybrid Terminal Requirements.....	229
7.6.1 Hybrid POS Terminal Requirements.....	229
United States Region.....	229
7.3 Contactless Payment Functionality.....	229
7.4 POS Terminal Requirements.....	229
7.4.1 Contactless-enabled POS Terminals.....	229
7.4.3 Mobile POS (MPOS) Terminals.....	230
7.4.4 Mastercard Consumer-Presented QR-enabled POS Terminals.....	230
7.5 ATM Terminal and Bank Branch Terminal Requirements.....	230
7.6 Hybrid Terminal Requirements.....	230
Additional U.S. Region and U.S. Territory Rules.....	231
7.6 Hybrid Terminal Requirements.....	231
7.6.1 Hybrid POS Terminal Requirements.....	231
Hybrid POS Terminal and Chip-only MPOS Terminal Displays.....	231
<b>Appendix A: Geographic Regions.....</b>	<b>232</b>
Asia/Pacific Region.....	233
Canada Region.....	234
Europe Region.....	234
Single European Payments Area (SEPA).....	235
Latin America and the Caribbean Region.....	235
Middle East/Africa Region.....	236
United States Region.....	237
<b>Appendix B: Compliance Zones.....</b>	<b>238</b>
Compliance Zones.....	239
<b>Appendix C: Transaction Identification Requirements.....</b>	<b>244</b>
Transaction Date.....	245
Contactless Transactions.....	245
Contactless Transit Aggregated Transactions.....	246
Contactless-only Transactions.....	248
Quick Payment Service Transactions.....	250
Payment Transactions.....	251

Electronic Commerce Transactions.....	253
Electronic Commerce Transactions at Automated Fuel Dispensers .....	260
Digital Secure Remote Payment Transactions.....	263
Digital Secure Remote Payment Transactions Containing Chip Data.....	263
Digital Secure Remote Payment Transactions Containing UCAF Data.....	265
Partial Shipments or Recurring Payments Following Digital Secure Remote Payment Transactions.....	267
Mastercard Mobile Remote Payment Transactions.....	269
Mastercard Biometric Card Program Transactions.....	269
<b>Appendix D: Cardholder-Activated Terminal (CAT) Transactions.....</b>	<b>270</b>
CAT Transactions.....	271
CAT Level Requirements.....	272
Dual Capability for CAT 1 and CAT 2.....	272
CAT Level 1: Automated Dispensing Machines (CAT 1).....	272
CAT Level 2: Self-Service Terminal (CAT 2).....	273
CAT Level 3: Limited Amount Terminals (CAT 3).....	274
CAT Level 4: In-Flight Commerce (IFC) Terminals (CAT 4).....	276
CAT Level 6: Electronic Commerce Transactions (CAT 6).....	278
CAT Level 7: Transponder Transactions (CAT 7).....	278
CAT Level 9: Mobile POS (MPOS) Acceptance Device Transactions (CAT 9).....	279
<b>Appendix E: CVM Limit Amounts.....</b>	<b>280</b>
Overview.....	281
CVM Limit Amounts.....	281
<b>Appendix F: Signage, Screen, and Receipt Text Display.....</b>	<b>282</b>
Screen and Receipt Text Standards.....	284
Models for ATM Access Fee Notification at ATM Terminals.....	284
Models for Standard Signage Notification of an ATM Access Fee.....	285
Asia/Pacific Region.....	285
Australia.....	285
Canada Region.....	286
Europe Region.....	286
United Kingdom.....	287
Latin America and the Caribbean Region.....	288
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.....	288
Middle East/Africa Region.....	289
United States Region.....	290
Models for Generic Terminal Signage Notification of an ATM Access Fee.....	290

Asia/Pacific Region.....	290
Australia.....	291
Canada Region.....	292
Europe Region.....	292
United Kingdom.....	293
Latin America and the Caribbean Region.....	294
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.....	294
Middle East/Africa Region.....	295
United States Region.....	296
Models for Screen Display Notification of an ATM Access Fee.....	296
Asia/Pacific Region.....	296
Australia.....	297
Canada Region.....	298
Europe Region.....	298
United Kingdom.....	299
Latin America and the Caribbean Region.....	300
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.....	300
Middle East/Africa Region.....	301
United States Region.....	302
Model for an ATM Access Fee Transaction Receipt.....	303
Model Screens Offering POI Currency Conversion.....	303
Model Receipt for Withdrawal Completed with POI Currency Conversion.....	304
Model Screen Displays for Offering Installment Payments.....	304
Model Receipt Texts for Installments.....	311
<b>Appendix G: Best Practices.....</b>	<b>314</b>
Digital Goods Purchases.....	315
<b>Appendix H: Definitions.....</b>	<b>316</b>
<b>Notices.....</b>	<b>357</b>

# Chapter 1 Connecting to the Interchange System and Authorization Routing

*The following Standards apply with regard to connecting to the Interchange System and Authorization routing. Where applicable, modifications by region and/or country are provided at the end of this chapter in the section titled, "Variations and Additions by Region."*

1.1 Connecting to the Interchange System.....	30
1.2 Authorization Routing—Mastercard POS Transactions.....	30
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions.....	31
1.3.1 Routing Instructions and System Maintenance.....	31
1.3.2 Chip Transaction Routing.....	31
1.3.3 Domestic Transaction Routing.....	32
1.4 ATM Terminal Connection to the Interchange System.....	32
1.5 Gateway Processing.....	32
1.6 POS Terminal Connection to the Interchange System.....	33
Variations and Additions by Region.....	33
Asia/Pacific Region.....	33
1.4 ATM Terminal Connection to the Interchange System.....	33
1.6 POS Terminal Connection to the Interchange System.....	33
Canada Region.....	34
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions.....	34
1.3.3 Domestic Transaction Routing.....	34
1.4 ATM Terminal Connection to the Interchange System.....	34
Europe Region.....	34
1.1 Connecting to the Interchange System.....	34
1.2 Authorization Routing—Mastercard POS Transactions.....	35
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions.....	35
1.3.2 Chip Transaction Routing.....	35
1.3.3 Domestic Transaction Routing.....	35
1.4 ATM Terminal Connection to the Interchange System—SEPA Only.....	35
Latin America and the Caribbean Region.....	35
1.4 ATM Terminal Connection to the Interchange System.....	35
1.6 POS Terminal Connection to the Interchange System.....	36
United States Region.....	36
1.1 Connecting to the Interchange System.....	36
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions.....	36
1.3.1 Routing Instructions and System Maintenance.....	36

1.3.3 Domestic Transaction Routing..... 37

1.4 ATM Terminal Connection to the Interchange System..... 37

Additional U.S. Region and U.S. Territory Rules.....37

1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions..... 37

## 1.1 Connecting to the Interchange System

---

A Customer must maintain the necessary equipment and procedures to process Transactions and/or Payment Transactions and to connect to the Interchange System, using a telecommunications circuit established by the Interchange System that is equipped with back-up service. Before processing Transactions and/or Payment Transactions and on an ongoing basis thereafter, the Customer must perform testing and obtain any necessary certifications of its equipment, procedures, and Interchange System connections as may be required by Mastercard to ensure compatibility with its technical specifications then in effect.

Each Principal and Association must establish and maintain, at its own expense, a data processing facility that is capable of receiving, storing, processing, and communicating any Transaction and/or Payment 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 Customer's parent, its wholly-owned subsidiary, or an entity that is wholly owned, directly or indirectly, by the Customer's parent, or with the prior written agreement of Mastercard, by the Customer's designated third party agent.

**NOTE: Modifications to this Rule appear in the "Europe Region" and "United States Region" sections at the end of this chapter.**

## 1.2 Authorization Routing—Mastercard POS Transactions

---

On an ongoing basis, an Acquirer of Mastercard POS Transactions and any Customer providing Mastercard Manual Cash Disbursements must recognize and use all active Mastercard bank identification numbers (BINs) for purposes of obtaining Transaction authorizations, and obtain such authorizations on behalf of each of its Merchants as the Standards require. The Acquirer must use Account range files provided by the Corporation 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 Corporation. After downloading an updated Account range file from the Corporation, an Acquirer must return an acknowledgment file to the Corporation 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 either the 222100 to 272099 BIN range or 510000 to 559999 BIN range to the Interchange System for routing to the Issuer.

**NOTE: A modification to this Rule appears in the "Europe Region" section at the end of this chapter.**

## 1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions

---

An Acquirer must recognize and use all active Account ranges that are included in the Corporation's Financial Institution Table (FIT) or other Account range file obtained through the Corporation and must follow the Issuer's routing instructions, if any, set forth in those files. Such files must be used by the Acquirer, its Merchants, ATM Terminals, Bank Branch Terminals, and any entities that handle such 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 Corporation. After downloading an updated Account range file from the Corporation, an Acquirer must return an acknowledgment file to the Corporation confirming that:

- The Acquirer has updated its systems accordingly; and
- Each of the Acquirer's Merchants, ATM Terminals, Bank Branch Terminals, 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, an Acquirer of Maestro POS Transactions, ATM Transactions, and/or Manual Cash Disbursement Transactions occurring at Bank Branch Terminals must default route to the Interchange System any such Transaction not belonging to its proprietary network. The Interchange System determines whether or not the Transaction is being performed by a Cardholder.

**NOTE: Modifications to this Rule appear in the "Additional U.S. Region and U.S. Territories" section at the end of this chapter.**

### 1.3.1 Routing Instructions and System Maintenance

Each Customer or its Sponsor must:

1. Submit to the Corporation completed institution routing table (IRT) and institution definition file (IDF) input documents no later than five business days prior to the requested effective date of live processing via the Interchange System.
2. Notify the Corporation 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 Corporation of any scheduled downtime at least 24 hours in advance.

**NOTE: A variation to this Rule appears in the "United States Region" section at the end of this chapter.**

### 1.3.2 Chip Transaction Routing

Any chip-based ATM Transaction or Maestro POS Transaction generated by a Mastercard-branded Application Identifier (AID) must be routed through the Interchange System, or as otherwise approved by the Corporation.

This provision does not apply with respect to a Domestic Transaction for which the Issuer and Acquirer is the same Customer (an "on-us" Transaction).

**NOTE: A variation to this Rule appears in the "Europe Region" section at the end of this chapter.**

### 1.3.3 Domestic Transaction Routing

When a Card is used at an ATM Terminal or Bank Branch Terminal in the country in which such Card was issued and the only common brand appearing on both the Card and the ATM Terminal or Bank Branch Terminal is a Mark, the resulting Transaction:

1. Must be routed to the Interchange System; or
2. The Issuer of the Card must report and pay a Brand Fee for such Transaction.

This provision does not apply with respect to a Domestic Transaction for which the Issuer and Acquirer is the same Customer (an "on-us" Transaction).

**NOTE: Variations to this Rule appear in the "Canada Region," "Europe Region," and "United States Region" sections at the end of this chapter.**

## 1.4 ATM Terminal Connection to the Interchange System

---

Except as otherwise provided in the Standards, each Customer that acquires any ATM transactions must at all times make available for connection to the Interchange System, and in particular, the Mastercard® ATM Network, all of the eligible ATM Terminals established by that Customer (including its parents, subsidiaries, affiliates, and Sponsored entities) in the country in which the Customer is located and in every other country in which it has been Licensed to conduct ATM Transaction acquiring Activity.

A Customer Licensed only to conduct ATM Transaction acquiring Activity must make at least 75 percent of the ATM Terminals it establishes available for connection to the Interchange System.

**NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Canada Region," "Europe Region," "Latin America and the Caribbean Region," and "United States Region" sections at the end of this chapter.**

## 1.5 Gateway Processing

---

The Interchange System may be used for the routing of ATM transactions and settlement of funds pursuant to terms governing a card that does not bear the any of the Corporation's Marks if such card bears the mark of one of the following authorized Gateways:

1. PLUS System USA, Inc.
2. VISA USA, Inc.



The Interchange System technical specifications applicable to ATM Transactions apply to Gateway Processing. Error and dispute resolution is supported within Gateway Processing to the extent provided in the Standards that govern the individual Transaction. When a Gateway Customer uses the Mastercard® ATM Network for Gateway Processing, error and dispute resolution requests must be processed in accordance with the *Chargeback Guide*.

The Principal that submits an ATM transaction to the Mastercard® ATM Network for Gateway Processing is deemed to have consented to comply with all applicable Standards and to pay all applicable fees in connection with such transaction.

---

## 1.6 POS Terminal Connection to the Interchange System

---

**NOTE:** Rules on this subject appear in the “Asia/Pacific Region” and “Latin America and the Caribbean Region” sections at the end of this chapter.

---

## Variations and Additions by Region

---

The remainder of this chapter provides modifications to the Standards set out in this chapter. The modifications are organized by region or country and by applicable subject title.

---

### Asia/Pacific Region

---

The following modifications to the Rules apply in the Asia/Pacific Region or in a particular Region country or countries. Refer to Appendix A for the Asia/Pacific Region geographic listing.

#### 1.4 ATM Terminal Connection to the Interchange System

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

A Customer that acquires ATM Transactions must make available for connection to the Interchange System at least 75 percent of its eligible ATM Terminals in the Region within one year of the approval of its application for a License.

#### 1.6 POS Terminal Connection to the Interchange System

In the Asia/Pacific Region, a Customer that acquires POS Transactions must make available for connection to the Interchange System at least 75 percent of its eligible POS Terminals in the Region within one year of the approval of its application for a License.

## Canada Region

---

The following modifications to the Rules apply in the Canada Region. Refer to Appendix A for the Canada Region geographic listing.

### 1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions

#### 1.3.3 Domestic Transaction Routing

In the Canada Region, the Rule on this subject is modified as follows.

When a Card issued in the Canada Region is used at an ATM Terminal or Bank Branch Terminal located in the Canada Region and the only common brand appearing on both the Card and ATM Terminal or Bank Branch Terminal is a Mark:

1. The resulting Transaction must be routed to the Interchange System; or
2. The Issuer receiving such Transaction must report and pay a Brand Fee for such Transaction.

This provision does not apply with respect to a Transaction for which the Issuer and Acquirer is the same Customer (an “on-us” Transaction) or any Transaction processed between:

1. A Principal (or its Third Party Processor) and one of its Affiliates (or its Third Party Processor), or
2. Two Affiliates (or their Third Party Processors) Sponsored by the same Principal.

### 1.4 ATM Terminal Connection to the Interchange System

In the Canada Region, the Rule on this subject is modified as follows.

A Customer that acquires ATM Transactions must make available for connection to the Interchange System at least 75 percent of the eligible ATM Terminals established by it (including its parents, subsidiaries and affiliates) in each major Canadian metropolitan area in which at least 10,000 of its debit Cardholders reside. The Census Metropolitan Area (CMA) as defined by the Canadian government will be used as the measure.

## Europe Region

---

The following modifications to the Rules apply in the Europe Region or in a particular Region country or countries. Refer to Appendix A for the Europe Region, Non-Single European Payments Area (Non-SEPA) and Single European Payments Area (SEPA) geographic listing.

### 1.1 Connecting to the Interchange System

In the EEA, the Rule on this subject is modified as follows.

For the processing of Transactions in the EEA and, if required by applicable law or regulation, Payment Transactions in the EEA, a Customer may use any switch of its choice that is

registered with the Corporation. Back-up facilities are required and may be provided via its chosen switch.

Dual-message processing (i.e. separate messages for authorization and clearing) must be used. A Customer is not required to use the same switch for authorization and for clearing.

## **1.2 Authorization Routing—Mastercard POS Transactions**

In the EEA, the Rule on this subject is modified as follows.

An Acquirer must make sure that the registered switch that it uses for authorization recognizes all active Mastercard BINs and updates its systems using a current file obtained through the Corporation within six calendar days from the date that the updated Account range file is made available by the Corporation. The Acquirer must confirm to the Corporation that its chosen switch has updated its systems accordingly. The Acquirer may submit authorization requests via its chosen switch.

## **1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions**

### **1.3.2 Chip Transaction Routing**

The Rule on this subject does not apply to Intra-SEPA Transactions.

In the EEA, the Rule on this subject is modified as follows.

Intra-EEA Transactions and Intracountry Transactions in the EEA Transactions may be processed using the registered switch of the Customer's choice.

### **1.3.3 Domestic Transaction Routing**

In the EEA, the Rule on this subject is modified as follows.

Intra-EEA Transactions and Intracountry Transactions in the EEA may be processed using the registered switch of the Customer's choice.

## **1.4 ATM Terminal Connection to the Interchange System—SEPA Only**

Within SEPA, the Rule on this subject is modified as follows.

A Customer must at all times accept all Mastercard, Maestro, and Cirrus Cards at all ATM Terminals owned or established by that Customer (including its parents, subsidiaries, affiliates, and Sponsored entities) within SEPA if it accepts cards issued under other acceptance brands at those ATM Terminals.

## **Latin America and the Caribbean Region**

---

The following modifications to the Rules apply in the Latin America and the Caribbean Region. Refer to Appendix A for the Latin America and the Caribbean Region geographic listing.

## **1.4 ATM Terminal Connection to the Interchange System**

In the Latin America and the Caribbean Region, the Rule on this subject is modified as follows.

A Customer that acquires ATM Transactions must make available for connection to the Interchange System at least 75 percent of its eligible ATM Terminals in the Region within one year of the approval of its application for a License.

## 1.6 POS Terminal Connection to the Interchange System

In the Latin America and the Caribbean Region, a Customer that acquires POS Transactions must make available for connection to the Interchange System at least 75 percent of its eligible POS Terminals in the Region within one year of the approval of its application for a License.

## United States Region

---

The following modifications to the Rules apply in the United States (U.S.) Region. Refer to Appendix A for the U.S. Region geographic listing.

### 1.1 Connecting to the Interchange System

In the U.S. Region, the Rule on this subject is modified as follows.

Connection to the Interchange System for Maestro POS Transaction and ATM Transaction processing is limited to Principals or their Designees. As used herein, “Designee” means an entity authorized by the Corporation to connect to the Interchange System.

### 1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions

#### 1.3.1 Routing Instructions and System Maintenance

In the U.S. Region, the Rule on this subject is modified as follows.

With respect to ATM Transaction processing, a Customer must provide the Corporation with written notification of downtime at least 48 hours before any regularly scheduled maintenance event and within five business days following the occurrence of an emergency maintenance event. Written notification must include the date of the maintenance; the times at which the maintenance commences and concludes; a brief description of the reason for the maintenance; and for an emergency event, a description of the actions taken to prevent a reoccurrence of the event.

	Scheduled Maintenance	Emergency Maintenance
Permissible Maintenance Time frame	01:00 to 05:00 (New York time)	Anytime
Maximum Hours per Month	10	4
Maximum Hours per Week	5	2
Maximum Hours per Day	2	1

---

Scheduled Maintenance	Emergency Maintenance
Maximum Duration (in hours) of Event 2	1

---

### 1.3.3 Domestic Transaction Routing

In the U.S. Region, the Rule on this subject is modified as follows.

When a Card issued in the United States Region is used at an ATM Terminal located in the United States Region for a Transaction other than the purchase of merchandise or a service, and a Mark is a common brand, but not the only common brand, appearing on both the Card and the ATM Terminal, the resulting Transaction must be routed to:

1. The interchange system specified by the Issuer; or
2. The Corporation's Interchange System, if the Issuer has not specified to the Corporation a different interchange system for Transaction routing.

### 1.4 ATM Terminal Connection to the Interchange System

In the U.S. Region, the Rule on this subject is replaced with the following.

A Customer that acquires ATM Transactions must make available for connection to the Interchange System at least 75 percent of the eligible ATM Terminals established by it (including its parents, subsidiaries and affiliates) in each major United States metropolitan area in which at least 10,000 of its debit Cardholders reside. The Metropolitan Statistical Area (M.S.A.) as defined by the United States government will be used as the measure.

## Additional U.S. Region and U.S. Territory Rules

---

The following modifications to the Rules apply in the United States Region and in American Samoa, Guam, Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands (herein, "the U.S. Territories").

These Rules apply in addition to any that apply within the Asia/Pacific Region, with respect to Customers located in American Samoa, Guam, and Northern Mariana Islands; the Latin America and the Caribbean Region, with respect to Customers located in Puerto Rico and the U.S. Virgin Islands; and the United States Region, with respect to U.S. Region Customers.

### 1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions

In the U.S. Region and U.S. Territories, the Rule on this subject is modified as follows.

The Corporation offers Merchants located in the U.S. Region and U.S. Territories the option of routing POS transactions initiated with a debit card enhanced with Maestro functionality to the Mastercard® Single Message System. The Acquirer of a Merchant located in the U.S. Region or a U.S. Territory must support the Maestro routing indicator fields MS ATM (position 54) and MS POS (position 55) in the 80-byte Financial Institution Table (FIT) file. These fields

apply only when the Maestro Flag (position 42 in the FIT file) is **Y**. When the Maestro Flag is **N**, the Maestro routing indicator fields should be disregarded.

## Chapter 2 Authorization and Clearing Requirements

*The following Standards apply with regard to authorization processing and clearing requirements. Where applicable, modifications by region and/or country are provided at the end of this chapter in the section titled, "Variations and Additions by Region."*

2.1 Acquirer Authorization Requirements.....	42
2.1.1 Acquirer Host System Requirements—U.S. Region Only.....	42
2.2 Issuer Authorization Requirements.....	43
2.2.1 Issuer Host System Requirements.....	43
2.2.2 Stand-In Processing Service.....	44
Accumulative Transaction Limits.....	44
Chip Cryptogram Validation in Stand-In.....	45
2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers.....	45
2.3 Authorization Responses.....	45
2.4 Performance Standards.....	46
2.4.1 Performance Standards—Acquirer Requirements.....	46
2.4.2 Performance Standards—Issuer Requirements.....	46
Issuer Failure Rate (Substandard Level 1).....	46
Issuer Failure Rate (Substandard Level 2).....	47
Calculation of the Issuer Failure Rate.....	47
2.5 Preauthorizations.....	47
2.5.1 Preauthorizations—Mastercard POS Transactions.....	47
2.5.2 Preauthorizations—Maestro POS Transactions.....	48
2.5.3 Preauthorizations—ATM and Manual Cash Disbursement Transactions.....	48
2.6 Undefined Authorizations.....	48
2.7 Final Authorizations.....	49
2.8 Message Reason Code 4808 Chargeback Protection Period.....	49
2.9 Multiple Authorizations.....	50
2.10 Multiple Clearing Messages.....	51
2.11 Full and Partial Reversals.....	52
2.11.1 Full and Partial Reversals—Acquirer Requirements.....	52
2.11.2 Full and Partial Reversals—Issuer Requirements.....	53
2.11.3 Reversal for Conversion of Approval to Decline.....	53
2.11.4 Reversal to Cancel Transaction.....	54
2.12 Full and Partial Approvals .....	54
2.13 Refund Transactions and Corrections.....	55
2.13.1 Refund Transactions—Acquirer Requirements.....	56

2.13.2 Refund Transactions—Issuer Requirements.....	56
2.14 Balance Inquiries.....	57
2.15 CVC 2 Verification for POS Transactions.....	58
2.16 CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless Transactions—Brazil Only.....	58
2.17 Euro Conversion—Europe Region Only.....	58
2.18 Transaction Queries and Disputes.....	58
2.18.1 Retrieval Requests and Fulfillments.....	58
2.18.2 Compliance with Dispute Procedures.....	59
2.19 Chargebacks for Reissued Cards.....	59
2.20 Correction of Errors.....	59
2.21 Co-badged Cards—Acceptance Brand Identifier.....	59
Variations and Additions by Region.....	59
Asia/Pacific Region.....	60
2.1 Acquirer Authorization Requirements.....	60
2.2 Issuer Authorization Requirements.....	60
2.2.1 Issuer Host System Requirements.....	60
2.5 Preauthorizations.....	60
2.5.2 Preauthorizations—Maestro POS Transactions.....	60
Canada Region.....	60
2.2 Issuer Authorization Requirements.....	60
2.12 Full and Partial Approvals.....	60
Europe Region.....	62
2.1 Acquirer Authorization Requirements.....	62
2.2 Issuer Authorization Requirements.....	63
2.2.2 Stand-In Processing Service.....	64
2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers.....	65
2.3 Authorization Responses.....	65
2.4 Performance Standards.....	65
2.4.2 Performance Standards—Issuer Requirements.....	65
2.5 Preauthorizations.....	65
2.5.2 Preauthorizations—Maestro POS Transactions.....	66
2.5.3 Preauthorizations—ATM and Manual Cash Disbursement Transactions.....	66
2.7 Final Authorizations.....	67
2.8 Message Reason Code 4808 Chargeback Protection Period.....	67
2.9 Multiple Authorizations.....	67
2.11 Full and Partial Reversals.....	68
2.11.1 Full and Partial Reversals—Acquirer Requirements.....	68
2.11.2 Full and Partial Reversals—Issuer Requirements.....	69



---

2.12 Full and Partial Approvals.....	69
2.13 Refund Transactions and Corrections.....	70
2.13.1 Refund Transactions—Acquirer Requirements.....	70
2.13.2 Refund Transactions—Issuer Requirements.....	70
2.14 Balance Inquiries.....	70
2.15 CVC 2 Verification for POS Transactions.....	71
2.17 Euro Conversion.....	71
2.21 Co-badged Cards—Acceptance Brand Identifier.....	72
Latin America and the Caribbean Region.....	73
2.16 CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless—Brazil Only.....	73
United States Region.....	73
2.1 Acquirer Authorization Requirements.....	73
2.1.1 Acquirer Host System Requirements.....	73
2.2 Issuer Authorization Requirements.....	73
2.2.1 Issuer Host System Requirements.....	74
2.2.2 Stand-In Processing Service.....	74
2.4 Performance Standards.....	75
2.4.2 Performance Standards—Issuer Requirements.....	76
2.5 Preauthorizations.....	76
2.5.2 Preauthorizations—Maestro POS Transactions.....	76
2.11 Full and Partial Reversals.....	76
2.11.1 Full and Partial Reversals—Acquirer Requirements.....	76
2.11.2 Full and Partial Reversals—Issuer Requirements.....	78
2.12 Full and Partial Approvals.....	78
2.14 Balance Inquiries.....	78

## 2.1 Acquirer Authorization Requirements

---

An Acquirer and each of its Merchants must support POS Transactions (authorized online by the Issuer or offline by the chip), and a full reversal when performed to cancel a POS Transaction that the Acquirer cannot complete due to a technical problem. Effective 17 April 2020, an Acquirer must support the authorization of refund Transactions for all Mastercard, Debit Mastercard, and Maestro Account ranges acquired on the Dual Message System.

The Acquirer of a Merchant that accepts Maestro Cards must support Maestro POS Transactions that either automatically access the primary account or allow the Cardholder to choose to access the checking account or savings account ("account selection").

An Acquirer may also support, and its Merchants may optionally offer, the following Transaction/Payment Transaction and message types. An Acquirer that supports and any of its Merchants that offer an optional Transaction and/or Payment Transaction or message type must comply with the Rules applicable to the optional Transaction and/or Payment Transaction or message type that is supported or offered.

- Purchase with cash back Transactions (Debit Mastercard and Maestro only, unless otherwise specified for a country or Region)
- Merchant-approved Maestro POS Transactions
- Payment Transactions
- Maestro POS Transaction preauthorization and completion (single message processing)
- Partial approval
- Balance response (prepaid only)
- Full reversal, including cancellation, and partial reversal (Merchant-initiated at the POS Terminal)
- POS balance inquiry (Debit Mastercard and Maestro only)
- Maestro refund Transactions and/or corrections acquired on the Single Message System
- Offline chip processing of refund Transactions

If a Transaction that may be processed offline in accordance with the Terminal offline chip authorization limit cannot be processed offline for any reason, the Transaction must be processed online; if the Transaction cannot be processed online, then the Transaction must be declined. A Mastercard® Single Message System Acquirer may clear offline Chip Transaction by transmitting the required Transaction data in an online Financial Advice/0220 message or as part of a batch notification.

**NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," and "United States Region" sections at the end of this chapter.**

### 2.1.1 Acquirer Host System Requirements—U.S. Region Only

**NOTE: A Rule on this subject appears in the "United States Region" section at the end of this chapter.**

## 2.2 Issuer Authorization Requirements

---

The Issuer of a debit Card Program or of a credit Card Program that provides cash access at ATM Terminals and Bank Branch Terminals:

1. Must support POS Transaction authorizations and preauthorizations from a debit Cardholder's primary account, checking account, and savings account.
2. Must offer cash withdrawal and Merchandise Transactions from no account specified to debit Cardholders and cash advances to credit Cardholders.
3. May offer, at its option, balance inquiry to checking, savings, and credit card accounts; and transfers to and from checking and savings accounts.

A Chip Card Issuer that elects to process offline Chip Transactions must support offline purchase and refund Transactions. If an offline Transaction type is not offered to a Cardholder, the chip must send the Transaction online for authorization or decline the Transaction offline. An Issuer must accept a Chip Transaction cleared online by an Acquirer following an offline authorization.

Effective 18 October 2019, an Issuer must support the online authorization of refund Transactions for all Mastercard and Debit Mastercard Account ranges, with the exception of non-reloadable prepaid Account ranges.

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 conducted in the Canada, Europe, Latin America and the Caribbean, or Middle East/Africa Region when technical fallback from chip to magnetic stripe occurred.

**NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Canada Region," "Europe Region," and "United States Region" sections at the end of this chapter.**

### 2.2.1 Issuer Host System Requirements

An Issuer's host system interfaces must support the online processing of:

- POS Transactions
- Refund Transactions (for Mastercard® Single Message System processing and effective 18 October 2019, for both Mastercard Dual Message System and Single Message System processing)
- Partial approval requests
- Balance response
- Reversal and correction requests
- POS balance inquiries (if required in a country or Region)
- Cash withdrawals and the purchase of Merchandise with no account specified at ATM Terminals and Bank Branch Terminals; and

- Payment Transactions

**NOTE: Modifications to this Rule appear in the “Asia/Pacific Region” and “United States Region” sections at the end of this chapter.**

## 2.2.2 Stand-In Processing Service

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 **Mastercard Card Programs**, an Issuer must use the Stand-In Processing Service. Stand-In Parameters for Mastercard (including Debit Mastercard) Card Programs must be set at or above the Corporation’s default limits.

For all of its **Maestro and Cirrus Card Programs**, an Issuer must use the Stand-In Processing Service. This requirement does not apply if the Issuer commenced its use of an alternative on-behalf authorization service before 1 December 2003 and such service meets the Corporation’s performance standards as set forth in Rule 2.4.2. Stand-In Parameters for Maestro and Cirrus Card Programs must be set at or above the Corporation’s default limits.

In the event that fraudulent activity is detected with respect to a Mastercard BIN or BIN range, the Corporation, in its sole discretion and judgment, may take such action as the Corporation deems necessary or appropriate to safeguard the goodwill and reputation of the Corporation’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 Mastercard 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.

An Issuer’s use of the Stand-In Processing Service must include the following services:

- Card Validation Code 1 (CVC 1) Verification in Stand-In must be used for all Cards bearing a magnetic stripe;
- Dynamic CVC 3 Validation in Stand-In must be used for all contactless-enabled Cards and Access Devices that support Magnetic Stripe Mode Contactless Transactions; and
- *SecureCode* Dynamic AAV Verification in Stand-In must be used for all Mastercard Accounts and all e-commerce-enabled Maestro Accounts that are enrolled in *SecureCode*, unless the Mastercard *SecureCode* AAV Verification Service is used.

**NOTE: Modifications to this Rule appear in the “Europe Region” and “United States Region” sections at the end of this chapter.**

### Accumulative Transaction Limits

An Issuer at its option, may use daily Stand-In Processing Service Transaction limits (“accumulative limits”) for a Card Program that are higher than the applicable default limits set by the Corporation. Refer to the Stand-In Processing—Accumulative Global Parameters

(Form 041f) for the minimum (default) daily accumulative Transaction processing limit applicable to a particular Card Program.

### Chip Cryptogram Validation in Stand-In

An issuer must use Chip Cryptogram Validation in Stand-In Processing for all of its Chip Card Programs.

## 2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers

A Mastercard credit Card Issuer must maintain a 70 percent minimum ATM Transaction approval rate and manage individual denial category rates in compliance with the following Standards.

Category	Maximum Denial Rate	Reason Codes
Invalid PIN	13%	55
Insufficient Funds	10%	51
Invalid Transactions	14%	57
Exceed Limit	9%	61
Restricted Card	4%	62

The Issuer determines the maximum cash withdrawal limits applicable to its Cardholders; however, the Issuer must permit its Mastercard credit Cardholders to withdraw at least the equivalent of USD 200 daily if the available credit exists, and there is no other reason to deny the transactions.

To accommodate ATM Access Fees and currency conversions, the Issuer must authorize Transactions up to the equivalent of USD 10 or 10 percent, whichever is greater, more than the daily Transaction amount limit communicated to the Cardholder.

**NOTE: Modifications to this Rule appear in the “Europe Region” section at the end of this chapter.**

## 2.3 Authorization Responses

An Acquirer must comply with the authorization response wait time requirements set forth in “Maximum Response Times” in Chapter 2 of the *Single Message System Specifications* and in “Minimum Authorization Response Wait Time” in Chapter 4 of the *Authorization Manual*, as applicable.

An Issuer must comply with the authorization response requirements set forth in “Maximum Response Times” in Chapter 2 of the *Single Message System Specifications* manual and in “Routing Timer Values” in Chapter 5 of the *Authorization Manual*, as applicable. If the Issuer’s

response is not received within the required time frame, then the Transaction will time out and be forwarded via Stand-In Processing System or another alternate authorization provider as specified by the Issuer.

**NOTE: Modifications to this Rule appear in the “Europe Region” section at the end of this chapter.**

## 2.4 Performance Standards

An Issuer or Acquirer that fails to meet the Corporation’s authorization performance standards may be subject to the following noncompliance assessments.

Occurrence	Penalty
First occurrence	USD 15,000
Second occurrence within the 12-month period following the first occurrence	USD 15,000
Third and any subsequent occurrence within the twelve (12)-month period following the second occurrence	USD 20,000

After completion of a full calendar year without any violations, a subsequent violation is counted as a first violation.

### 2.4.1 Performance Standards—Acquirer Requirements

For Maestro POS Transactions and ATM Transactions, an Acquirer authorization failure rate that exceeds two percent for two consecutive months is deemed to be substandard authorization performance. The Acquirer authorization failure rate is based on Transactions processed through each Acquirer connection to the Interchange System and is calculated by taking the total number of Transactions declined due to invalid amount or format error divided by the total number of Transactions. The Acquirer failure rate is not applied until after the fourth calendar month of operation or upon processing 5,000 Maestro POS Transactions and/or and ATM Transactions in a calendar month, whichever occurs first.

### 2.4.2 Performance Standards—Issuer Requirements

An Issuer must comply with the following authorization performance standards.

#### Issuer Failure Rate (Substandard Level 1)

For Maestro POS Transactions and ATM Transactions, an Issuer authorization failure rate that exceeds two percent for two consecutive months is deemed to be substandard level 1 performance. The Issuer failure rate is not applied until after the fourth calendar month of

operation or upon processing 5,000 Maestro POS Transactions and/or ATM Transactions in a calendar month, whichever occurs first.

### **Issuer Failure Rate (Substandard Level 2)**

For Maestro POS Transactions and ATM Transactions, an Issuer authorization failure rate that exceeds three percent for two consecutive months is deemed to be substandard level 2 performance. The Issuer failure rate is not applied until after the fourth calendar month of operation or upon processing 5,000 Maestro POS Transactions and/or ATM Transactions in a calendar month, whichever occurs first.

### **Calculation of the Issuer Failure Rate**

The Issuer authorization failure rate for Maestro POS Transactions and ATM Transactions is calculated by taking the total number of Transactions declined due to Issuer unavailability, malfunction, or timeout divided by the total number of Transactions.

**NOTE: Modifications to this Rule appear in the "Europe Region" and "United States Region" sections at the end of this chapter.**

## **2.5 Preauthorizations**

---

A Processed Transaction authorization request is properly identified as a preauthorization when DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains a value of **4**.

**NOTE: An addition to this Rule appears in the "Europe Region" section at the end of this chapter.**

### **2.5.1 Preauthorizations—Mastercard POS Transactions**

An Acquirer is advised to identify a Mastercard 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.

All clearing messages corresponding to a preauthorization must be presented within **30 calendar days** of the authorization approval date.

### 2.5.2 Preauthorizations—Maestro POS Transactions

A Maestro POS Transaction preauthorization is performed to obtain the Issuer's approval of an estimated or Cardholder-requested Transaction amount, prior to submission of a request for authorization of the final amount.

1. The Acquirer must ensure that preauthorizations (in the physical environment) are initiated using a Card reader, with PIN or signature as the Cardholder verification method.
2. The Issuer must accept all preauthorization completions provided the actual amount of the completion is less than or equal to the amount approved in the preauthorization. Use of the PIN or signature and the use of the card reader are not required in the preauthorization completion.
3. If the Issuer does not receive a preauthorization completion within 20 minutes of the preauthorization, the preauthorization approval is void, except as provided for in Rule 4.14, "Merchant-approved Maestro POS Transactions."
4. The Acquirer is not responsible for preauthorization completions that occurred within two hours of the initial Transaction that were stored and forwarded because of technical problems between the Acquirer and the Interchange System, or the Interchange System and the Issuer.

**NOTE: Modifications to this Rule appear in the "Europe Region" section at the end of this chapter.**

### 2.5.3 Preauthorizations—ATM and Manual Cash Disbursement Transactions

**NOTE: A Rule on this subject appears in the "Europe Region" section at the end of this chapter.**

## 2.6 Undefined Authorizations

---

**NOTE: This Rule does not apply in the Europe Region.**

A Processed Transaction authorization request is identified as undefined when DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction status) contains a value of **0** and DE 48, subelement 61 (POS Data Extended Condition Codes), subfield 5 (Final Authorization Indicator) contains a value of **0** or is not present.

A Mastercard POS Transaction authorization request may be identified as undefined if:

1. Authorization is requested for an amount great than zero; **and**
2. The final Transaction amount may differ from the authorized amount; **and**



3. 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 Terminal failure).

All clearing messages corresponding to an undefined authorization must be presented within **seven calendar days** of the authorization approval date.

If an Acquirer submits at least 100,000 Domestic Transaction authorization requests per month to the Interchange System, then the number of undefined Domestic Transaction authorization requests submitted by the Acquirer in any one month must not exceed **20 percent** of its total Domestic Transaction authorization requests submitted in the same month.

## 2.7 Final Authorizations

---

A Processed Transaction authorization request is properly identified as a final authorization when DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains a value of **0** and DE 48 (Additional Data), subelement 61 (POS Data Extended Condition Codes), subfield 5 contains a value of **1**.

Use of the final authorization is **optional** outside of the Europe Region. However, if an Acquirer or Merchant uses the final authorization, then in a dual message environment:

1. Any Transaction corresponding to an authorization identified as a final authorization must be presented for clearing within seven calendar days of the authorization approval date; and
2. The presented Transaction amount must equal the authorized amount.

An Acquirer is advised to identify a Mastercard 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).

**NOTE: A modification to this Rule appears in the “Europe Region” section at the end of this chapter.**

## 2.8 Message Reason Code 4808 Chargeback Protection Period

---

A message reason code 4808 (Authorization-related Chargeback) chargeback protection period applies to each Mastercard POS Transaction as follows.

Each Mastercard POS Transaction identified as a...	Has a message reason code 4808 chargeback protection period of...
Preauthorization	30 calendar days from the authorization approval date <sup>2</sup>
Undefined authorization	Seven calendar days from the authorization approval date
Final authorization	Seven calendar days from the authorization approval date

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 a particular Transaction, at the latest.

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 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.

No fraud-related or other chargeback rights or Transaction processing requirements are effected by the message reason code 4808 chargeback protection period, unless otherwise indicated.

**NOTE: Modifications to this Rule appear in the "Europe Region" section at the end of this chapter.**

## 2.9 Multiple Authorizations

The following requirements apply to Mastercard 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, by populating DE 48, subelement 63 (Trace ID) of each additional authorization request with the DE 63 (Network Data), subfield 1 (Financial Network Code) and subfield 2 (Banknet Reference Number) and DE 15 (Date, Settlement) data from the

<sup>2</sup> 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. Refer to Chapter 4 for Contactless Transit Aggregated Transaction processing procedures.

initial approved Authorization Request Response/0110 message. 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.

**NOTE: An addition to this Rule appears in the "Europe Region" section at the end of this chapter.**

## 2.10 Multiple Clearing Messages

A Mastercard® Dual Message System Acquirer has the option of linking multiple presentments with partial amounts to one approved authorization. This option is not available to a Mastercard® Single Message System Acquirer. The following requirements apply to Mastercard and Debit Mastercard Transactions acquired in the Mastercard® Dual Message System:

1. In the First Presentment/1240 message, the Acquirer may populate DE 25 (Message Reason Code) with either of the following values:
  - a. **1403** (Previously approved authorization—partial amount, multi-clearing); or
  - b. **1404** (Previously approved authorization—partial amount, final clearing).  
For a Debit Mastercard Issuer that receives Mastercard® Single Message System-generated Financial Transaction Advice/0220 messages, the value of 1403 or 1404, if populated, will appear in DE 60 (Advice Reason Code), subfield 2 (Advice Reason Detail Code).
2. Upon receipt of a clearing message containing a value of 1403 or 1404, the Issuer must match the clearing message to the authorization message by comparing the data contained in the following fields:
  - a. DE 63 (Transaction Life Cycle ID), subfield 2 (Trace ID) of the First Presentment/1240 message; and
  - b. DE 63 (Network Data), subfield 2 (Banknet Reference Number) and DE 15 (Date, Settlement) of the Authorization Request/0100 message.
3. Upon matching a clearing message to an authorization message, the Issuer must adjust any hold on the availability of funds in the Cardholder's Account in accordance with its standard Account management practice for cleared amounts:

If the clearing message contains a value of...	Then the Issuer is advised to...
1403	Release the hold placed on the Cardholder's Account in connection with the approved authorization by the amount in DE 6 (Amount, Cardholder Billing).

---

If the clearing message contains a value of...	Then the Issuer is advised to...
1404	Release any unused funds in connection with the approved authorization.

---

All multi-clearing messages must be presented within the applicable clearing time frame, in order to avoid an Authorized-related or Late Presentment chargeback.

## 2.11 Full and Partial Reversals

---

A reversal message sent for the full Transaction amount cancels the original authorization request.

**NOTE: Modifications to this Rule appear in the “Europe Region” section at the end of this chapter.**

### 2.11.1 Full and Partial Reversals—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/1240 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 Merchant 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/1240 message is submitted within 24 hours of finalization of the Transaction.

The reversal requirement does not apply to automated fuel dispenser (MCC 5542) Transactions or to Contactless transit aggregated or transit debt recovery Transactions.

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.

**NOTE: Modifications to this Rule appear in the “Europe Region” and “United States Region” sections at the end of this chapter.**

### **ATM Transactions**

An Acquirer must not automatically generate a full or partial reversal of an authorized ATM Transaction when the ATM Terminal indicates that the Transaction was not completed because the Cardholder failed to collect some or all of the cash dispensed.

## **2.11.2 Full and Partial Reversals—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 Mastercard or Maestro Account in the amount specified within 60 minutes of matching the reversal message to the original authorization request message.

**NOTE: Modifications to this Rule appear in the “Europe Region” and “United States Region” sections at the end of this chapter.**

## **2.11.3 Reversal for Conversion of Approval to 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 (CNP) Mastercard or Maestro POS 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, 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 as a Third Party Processor (TPP) as described in Chapter 7 of the *Mastercard Rules*. The systematic decline by an Acquirer or Merchant of CNP Transactions arising from particular Cards, Issuers, or geographic locations is a violation of Rule 5.10.1 of the *Mastercard Rules*.

#### **2.11.4 Reversal to Cancel Transaction**

A single message POS Transaction may be cancelled prior to its completion by use of a "CANCEL" or "STOP" key on the POS Terminal. If either the Cardholder or Merchant cancels the Transaction, or a technical failure occurs involving a magnetic stripe Transaction, either before or after the authorization request has been forwarded to the Issuer, the Cardholder and Merchant must be informed; there must be no record of a Transaction; and a reversal advice message must be sent to the Issuer.

If after sending an authorization request, the POS Terminal does not receive a response, the POS Terminal must 'time-out' and send an automatic reversal. In such event, the Cardholder and Merchant must be informed; the attempted Transaction must be recorded; and a reversal advice message must be sent to the Issuer with a response code.

### **2.12 Full and Partial Approvals**

---

The Acquirer and each of its Merchants that support partial approvals must establish an education program for Merchant staff, including but not limited to POS Terminal operators, relating to the acceptance of multiple payment methods for a single purchase.

An Issuer must not respond to a cash withdrawal or purchase with cash back Transaction authorization request with a partial approval. 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.

Unless an earlier date applies in the Customer's country or Region, a Customer must provide partial approval as follows:

1. Effective 20 October 2020, an Issuer must support partial approval for all prepaid Mastercard, all Debit Mastercard (including prepaid), and all Maestro Account ranges.
2. Effective 20 October 2020, an Acquirer must support a newly-deployed POS Terminal that is EMV-certified and identified with any of the MCCs listed below, and must support partial approval for all Card-present Transactions conducted at that attended POS Terminal with a Mastercard or Maestro prepaid or debit Account range.

3. Effective 1 April 2023, an Acquirer must support all POS Terminals identified with any of the MCCs listed below, and must support partial approval for all Card-present Transactions conducted at that attended POS Terminal with a Mastercard or Maestro debit or prepaid Account range.

MCC	Description
5310	Discount Stores
5311	Department Stores
5411	Grocery Stores, Supermarkets
5541	Service Stations (with or without Ancillary Services)
5542	Fuel Dispenser, Automated
5621	Women's Ready to Wear Stores
5691	Men's and Women's Clothing Stores
5732	Electronic Sales
5812	Eating Places, Restaurants
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5999	Miscellaneous and Specialty Retail Stores

**NOTE: Additions to this Rule appear in the "Canada Region," "Europe Region" and "United States Region" sections at the end of this chapter.**

## 2.13 Refund Transactions and Corrections

A refund Transaction is a payment processed by a Merchant to a Cardholder's Account upon the return of goods or cancellation of services previously purchased by the Cardholder from the Merchant using the same Account. A refund Transaction may be a dual or single message Transaction and contains a value of 20 in DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code).

A correction is a single message authorization request containing a value of 20 in DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) that is used in a Card-present environment following a single message POS Transaction approval to remedy a Merchant or Cardholder error. A correction must be performed as a Card-read Transaction

initiated by or on behalf of the Cardholder; the Transaction may be completed without a Cardholder verification method. The Acquirer assumes the risk for this message type.

**NOTE: Modifications to this Rule appear in the “Europe Region” and “United States Region” sections at the end of this chapter.**

### 2.13.1 Refund Transactions—Acquirer Requirements

Effective 17 April 2020, an Acquirer must technically support the online authorization of refund Transactions. The Acquirer must identify a refund Transaction as a final authorization, as described in Rule 2.7.

The First Presentment/1240 message of a refund Transaction occurring on or after 17 April 2020 must be submitted for clearing within five calendar days of the refund Transaction date.

Refer to Rule 2.11.1 regarding refund Transaction reversals.

#### Original Purchase Identifier

When possible, the Acquirer is recommended to populate DE 48, subelement 63 (Trace ID) of the refund Transaction authorization request message with a unique identifier from the original purchase Transaction, consisting of the values in DE 63 (Network Data), subfield 1 (Financial Network Code); DE 63, subfield 2 (Banknet Reference Number); and DE 15 (Date, Settlement) of the purchase Transaction authorization approval response message. The presence of this identifier may assist the Issuer in linking the refund to a prior purchase and help to avoid Credit Not Processed disputes.

**NOTE: Modifications to this Rule appear in the “Europe Region” section at the end of this chapter.**

### 2.13.2 Refund Transactions—Issuer Requirements

Effective 18 October 2019, for all Mastercard Cards except non-reloadable prepaid Cards, an Issuer must be able to receive and respond to an Authorization Request/0100 or Financial Transaction Request/0200 message for a refund Transaction.

#### Response Code Values

An Issuer is advised to provide a value of 00 (Approved or completed successfully) in DE 39 (Response Code) if the Account is open, so that the refund Transaction can be completed.

The following DE 39 values are invalid for refund Transactions and must not be used in the Issuer's response to a refund Transaction authorization request:

- 10 (Partial approval)
- 51 (Insufficient funds/over credit limit)

An Issuer may only use a value of 57 (Transaction not permitted to issuer/cardholder) in DE 39 for a non-reloadable Prepaid Card Program. An Issuer is advised to register the Prepaid Card



Program as non-reloadable using the Prepaid Card Program registration process on Mastercard Connect before using this response code value.

An Issuer must not decline a refund Transaction solely due to a message format error or the absence of chip-related data.

### **Posting of Funds to the Cardholder's Account**

Within one business day of the Issuer's receipt of the First Presentment/1240 message or Financial Transaction Advice/0220 message for a refund Transaction, the Issuer must post the funds to the Cardholder's Account or adjust the Account's "open-to-buy", as applicable. The Issuer may place a temporary hold on the funds to the extent allowed under applicable law if the Issuer determines that the circumstances or account history warrant the delay.

### **Pending Refund Transaction Information**

Effective 17 April 2020, an Issuer must make information about pending refund Transactions available to Cardholders upon through at least one delivery channel, such as in its online banking or other Cardholder-facing applications or by means of Transaction alerts. The information must be displayed in a manner similar to that used for a pending purchase Transaction.

In the case of dual message refund Transactions, the Issuer is advised to ensure that the refund Transaction amount is treated and displayed as a pending credit, until the clearing record has been received and matched to the authorization. The Issuer should clearly communicate that the funds due as a result of a refund Transaction will only be deposited to the Cardholder's Account upon receipt of such funds by the Issuer. If an Issuer releases the funds to the Cardholder before receiving the clearing record, the Issuer will be liable for the Cardholder's use of such funds.

**NOTE: Modifications to this Rule appear in the "Europe Region" section at the end of this chapter.**

## **2.14 Balance Inquiries**

---

The balance inquiry functionality of a Terminal allows a Cardholder to check the available balance of funds in an Account. Balance inquiries are identified with a value of 30 in DE 3, subfield 1 of authorization messages.

All Terminals that offer a balance inquiry functionality to debit cardholders of Competing EFT POS Networks and other competing networks must offer the same balance inquiry functionality to debit Cardholders.

A Terminal that offers balance inquiry must provide the Cardholder an opportunity to receive a receipt reflecting (and may also display) Account balance information. Each ATM Terminal and Bank Branch Terminal must display, as part of the screen information, or must print on the

receipt, the currency symbol of the local currency or three-character alpha ISO country code in which the balance amount is given, beside each balance inquiry amount.

**NOTE: Additions to this Rule appear in the “Asia/Pacific Region,” “Europe Region” and “United States Region” sections at the end of this chapter.**

## 2.15 CVC 2 Verification for POS Transactions

---

A Merchant must not prompt or otherwise require a Mastercard Cardholder to enter CVC 2 information when a Chip Card or Contactless Payment Device is used to complete a Chip Transaction at a POS Terminal or MPOS Terminal. This Rule also applies to Mastercard Consumer-Presented QR Transactions.

Refer to Chapter 3 of the *Security Rules and Procedures* manual for CVC 2 requirements.

**NOTE: An addition to this Rule appears in the “Europe Region” section at the end of this chapter.**

## 2.16 CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless Transactions—Brazil Only

---

**NOTE: A Rule on this subject pertaining to Brazil appears in the “Latin America and the Caribbean Region” section at the end of this chapter.**

## 2.17 Euro Conversion—Europe Region Only

---

**NOTE: A Rule on this subject appears in the “Europe Region” section at the end of this chapter.**

## 2.18 Transaction Queries and Disputes

---

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

### 2.18.1 Retrieval Requests and Fulfillments

The Issuer has the right to request the Acquirer’s retrieval of documentation for any Transaction presented by the Acquirer for clearing, with the following exceptions:

- Any ATM Transaction; and

- Any Cardholder-Activated Terminal (CAT) Level 1, 2, or 3 Transaction acquired within the Europe Region.

The Acquirer must provide the TID within 30 calendar days of:

- The Central Site Business Date of the Issuer's retrieval request; or
- The retrieval request submission date, if the Transaction was not cleared via the Global Clearing Management System (GCMS).

## 2.18.2 Compliance with Dispute Procedures

The Corporation administers procedures set forth in the *Chargeback Guide* that enable a Customer to seek redress against another Customer for failure to comply with the Standards applicable to a Transaction. Any filing by or on behalf of a Customer 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.

## 2.19 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.

## 2.20 Correction of Errors

---

If a Customer has been unjustly enriched because of an error, the Customer must reimburse the amount with which it has been enriched to the Customer or Customers that have suffered the corresponding loss.

## 2.21 Co-badged Cards—Acceptance Brand Identifier

---

**NOTE: A Rule on this subject appears in the "Europe Region" section at the end of this chapter.**

## Variations and Additions by Region

---

The remainder of this chapter provides modifications to the Standards set out in this chapter. The modifications are organized by region or country and by applicable subject title.

## Asia/Pacific Region

---

The following modifications to the Rules apply in the Asia/Pacific Region or in a particular Region country or countries. Refer to Appendix A for the Asia/Pacific Region geographic listing.

### 2.1 Acquirer Authorization Requirements

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

An Acquirer must support Maestro POS Transactions that access the primary account and may also allow the Cardholder to select a checking or savings account (“account selection”).

### 2.2 Issuer Authorization Requirements

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

An Issuer may decline authorization of a Transaction when technical fallback from chip to magnetic stripe occurred.

#### 2.2.1 Issuer Host System Requirements

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

A Maestro Card Issuer’s host system interfaces must support POS balance inquiry.

### 2.5 Preauthorizations

#### 2.5.2 Preauthorizations—Maestro POS Transactions

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

The Acquirer is not liable for preauthorization completions that occurred within 20 minutes of the initial Maestro POS Transaction but were subsequently stored and forwarded because of technical problems between the Interchange System and the Issuer.

## Canada Region

---

The following modifications to the Rules apply in the Canada Region. Refer to Appendix A for the Canada Region geographic listing.

### 2.2 Issuer Authorization Requirements

In the Canada Region, the Rule on this subject is modified as follows.

An Issuer must decline authorization of a Transaction conducted in the Canada Region when technical fallback from chip to magnetic stripe occurred.

### 2.12 Full and Partial Approvals

In the Canada Region, the Rule on this subject is modified as follows.

1. An Issuer must support partial approval for all prepaid Mastercard and all Debit Mastercard Accounts.
2. An Acquirer must support partial approval for Card-present Transactions occurring at a Merchant in a category listed below with a Debit Mastercard or prepaid Mastercard Account range.

<b>MCC</b>	<b>Description</b>
4812	Telecommunication Equipment Including Telephone Sales
4814	Telecommunication Services including but not limited to prepaid phone services and recurring phone services
4816	Computer Network/Information Services
5200	Home Supply Warehouse Stores
5310	Discount Stores
5311	Department Stores
5331	Variety Stores
5411	Grocery Stores, Supermarkets
5499	Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores
5541	Service Stations (with or without Ancillary Services)
5542	Fuel Dispenser, Automated
5621	Women's Ready To Wear Stores
5631	Women's Accessory And Specialty Stores
5641	Children's And Infant's Wear Stores
5651	Family Clothing Stores
5661	Shoe Stores
5691	Men's And Women's Clothing Stores
5732	Electronic Sales
5734	Computer Software Stores
5735	Record Shops
5812	Eating Places, Restaurants
5814	Fast Food Restaurants

MCC	Description
5912	Drug Stores, Pharmacies
5921	Package Stores, Beer, Wine, Liquor
5941	Sporting Goods Stores
5942	Book Stores
5945	Game, Toy, and Hobby Shops
5947	Gift, Card, Novelty, and Souvenir Shops
5977	Cosmetic Stores
5999	Miscellaneous And Specialty Retail Stores
7399	Business Services—not elsewhere classified
8999	Professional Services—not elsewhere classified
9399	Government Services—not elsewhere classified

## Europe Region

The following modifications to the Rules apply in the Europe Region or in a particular Region country or countries. Refer to Appendix A for the Europe Region, Non-Single European Payments Area (Non-SEPA) and Single European Payments Area (SEPA) geographic listing.

### 2.1 Acquirer Authorization Requirements

In the Europe Region, the Rule on this subject is modified as follows.

An Acquirer must ensure that any authorization request for an amount greater than zero is identified as either a preauthorization or as a final authorization.

In the United Kingdom and Ireland, the requirement for an Acquirer to support the authorization of refund Transactions for Account ranges acquired on the Dual Message System does not apply until 22 April 2022.

The reference to the Single Message System does not apply in the EEA.

### PSD2 Strong Customer Authentication (SCA) Requirements

Effective 1 July 2020, if the Issuer and the Acquirer are in the EEA but the Merchant is not, EMV 3DS authentication requests must include the EMV 3DS version 2.1 Merchant Data, with Field 3 containing the Acquirer country code. In other cases, it is recommended to provide the Acquirer country code in the EMV 3DS version 2.1 Merchant Data Field 3.

The Issuer and its Access Control Server are advised to use the Acquirer country code in the EMV 3DS version 2.1 Merchant Data Field 3 to determine if SCA is required. If the Acquirer country is not provided, the Issuer is advised to use the Merchant country to determine if SCA is required.

The following Rules apply to Intra-EEA Transactions and to Intracountry Transactions in the EEA.

Effective 14 September 2020, for the authorization of a Remote Electronic Transaction, authentication using EMV 3DS and Identity Check is required and may be omitted only if an Acquirer exemption to SCA applies or if another SCA compliant method is used (e.g., delegation to the Merchant, exemption under Article 17 of the RTS applied with the Merchant's knowledge).

When SCA by the Issuer is not required, or when it has been delegated, the Acquirer must indicate the reason in the appropriate field of the authorization message as specified by the registered switch of the Customer's choice.

Effective 14 September 2020, an Acquirer which allows its e-commerce Merchants to request a Transaction Risk Analysis (TRA) exemption must set the TRA exemption flag for such Merchants when registering them for the Identity Check Program in the Identity Solutions Services Management (ISSM) tool.

In order to optimize authorization approval rates for Transactions that benefit from an Acquirer exemption, a Merchant is advised to send an EMV 3DS authentication request with the Acquirer exemption flag.

Effective 1 July 2020, both Acquirers and Issuers must support the Acquirer exemption flag in EMV 3DS authentication requests as follows:

- In EMV 3DS version 2.1, Challenge Indicator value 02/No Challenge and EMV 3DS version 2.1 Merchant Data Field 1 (SCA Exemptions) with value 05/No SCA Requested, Transaction Risk Analysis performed.
- Effective with EMV 3DS version 2.2, Challenge Indicator value 05/No SCA Requested, Transaction Risk Analysis performed.

Effective 1 July 2020, an Acquirer of e-commerce Merchants that accept corporate Cards, and an Issuer of such Cards must support the EMV 3DS version 2.1 Merchant Data flag in EMV 3DS authentication requests. This flag indicates if the conditions for the exemption under Article 17 of the RTS are met, so that this exemption can be applied by the Issuer. The flag is in the EMV 3DS version 2.1 Merchant Data Field 4 (Secure Corporate Payment).

## **2.2 Issuer Authorization Requirements**

In the EEA, the Rule on this subject is modified as follows.

An Issuer must indicate that the Transaction type is not permitted to the Cardholder in the field of the authorization response and using the values specified by the registered switch of the Issuer's choice.

The following Rules apply to Intra-EEA Transactions and to Intracountry Transactions in the EEA.

## **PSD2 SCA Requirements**

Effective 1 July 2020, an Issuer must be able to process the Low Risk Merchant Indicator in authorization request messages, as specified by the registered switch of the Customer's choice.

If the Low Risk Merchant Indicator is present and populated in the authorization message, then the Issuer must neither automatically decline the authorization request nor require the Cardholder to authenticate the Transaction unless: a) its Transaction monitoring suggests a high risk of fraud, or b) in the case of a low-value payment, the Transaction counters are exceeded.

If an authentication request contains the Acquirer exemption flag or the delegation flag, the Issuer must neither automatically decline the authentication request nor require the Cardholder to authenticate the Transaction unless: a) its Transaction monitoring suggests a high risk of fraud, or b) in the case of a low-value payment, the Transaction counters are exceeded.

## **2.2.2 Stand-In Processing Service**

In the Europe Region, the Rule on this subject is modified as follows.

For all of its Maestro and Cirrus Card Programs, an Issuer must use the Stand-In Processing Service. This requirement does not apply if the Issuer commenced its use of an alternative on-behalf authorization service before 17 September 2008 and such service meets the Corporation's performance standards as set forth in Rule 2.4.2. Stand-In Parameters for Maestro and Cirrus Card Programs must be set at or above the Corporation's default limits.

The requirement to use CVC 1 Verification in Stand-In service, to take effect on 1 April 2017, does not apply to Maestro Chip-only Cards, as such term is defined in Rule 6.11 in Chapter 12 of the *Mastercard Rules*.

## **Smart Authentication Stand-In**

Effective 18 October 2019, an Issuer in Israel, Switzerland, or Turkey must participate in Smart Authentication Stand-In.

Effective 1 April 2020, an Issuer in Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Tajikistan, Russian Federation (except domestic authentication processed by NSPK), Turkmenistan, or Uzbekistan must participate in Smart Authentication Stand-In.

In the EEA, the Rule on this subject is modified as follows.

An Issuer is not required to participate in the Stand-in Processing Service unless so required by the registered switch of the Issuer's choice.

The registered switch of the Issuer's choice must provide a back-up service that is able to approve authorization requests on the Issuer's behalf. The Stand-in Processing Service may be used for this purpose. The Issuer must set its parameters in the back-up service of its chosen switch at or above the default limits established by the Corporation for Mastercard, Maestro and Cirrus Card Programs.



### **2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers**

In the EEA, the Rule on this subject is modified as follows.

The decline reason codes in the table in this Rule are replaced by the corresponding reason codes specified by the registered switch of the Issuer's choice.

## **2.3 Authorization Responses**

In the Europe Region, the Rule on this subject is modified as follows.

An Issuer must comply with the authorization response requirements set forth in "Routing Timer Values" in Chapter 5 of the Authorization Manual. If the Issuer's response is not received within the required time frame, then the Transaction will time out and be forwarded via the Stand-In Processing System or, when permitted under Rule 2.2.2, another alternate authorization provider as specified by the Issuer.

## **2.4 Performance Standards**

### **2.4.2 Performance Standards—Issuer Requirements**

In the Europe Region, the Rule on this subject is replaced with the following.

For all Transactions, an Issuer authorization failure rate that exceeds one percent for two months in any six-month period is deemed to be substandard performance. The Issuer failure rate is not applied until after the Issuer's fourth calendar month of operation or upon the Issuer's processing of 5,000 Transactions in a calendar month, whichever occurs first. The Issuer failure rate is calculated by taking the sum of ISO 8583 response codes 31—issuer signed off, 82—time out at Issuer host, and 96—system malfunction, and dividing by the total number of Transactions processed through the Issuer connection to the Interchange System.

An Issuer that has been designated as having substandard performance:

1. May be subject to noncompliance assessments as set forth in Rule 2.4; and
2. Will be mandated to implement the Stand-In Processing Service. Chip Issuers mandated to implement the Stand-In Processing Service will also be required to register for M/Chip Cryptogram Validation in Stand-In.

## **2.5 Preauthorizations**

In the Europe Region, the Rule on this subject is modified as follows.

In a dual message environment, the Acquirer must identify each Processed Transaction authorization request as either a preauthorization or a final authorization.

Preauthorizations occurring at an automated fuel dispenser and identified with MCC 5542 (Automated Fuel Dispenser) must be performed as described in Rule 4.11.1.

In the EEA, the Rule on this subject is modified as follows.

The authorization request must be identified as a preauthorization in the field and with the value specified by the registered switch of the Issuer's choice.

### 2.5.2 Preauthorizations—Maestro POS Transactions

In the Europe Region, the Rule on this subject is modified as follows.

Preauthorizations are permitted for Card-not-present Maestro POS Transactions when completed in accordance with the requirements set forth below. Preauthorizations are not permitted for Maestro POS Transactions conducted in any Card-present environment, with the exception of automated fuel dispenser Transactions and Contactless transit aggregated Transactions.

The Acquirer must ensure that the authorization request for a Card-not-present Maestro POS Transaction for an amount greater than zero is identified as a preauthorization if:

1. Authorization is requested for an estimated amount; **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 to determine if an authorization must be coded as a preauthorization.

Any Card-not-present Maestro POS Transaction clearing message corresponding to a preauthorization must be presented within **seven calendar days** of the authorization approval date. The presented Transaction amount must equal the approved amount.

### 2.5.3 Preauthorizations—ATM and Manual Cash Disbursement Transactions

In the Europe Region, the Acquirer must ensure that any ATM Transaction or Manual Cash Disbursement Transaction authorization request for an amount greater than zero is identified as a preauthorization if:

1. Authorization is requested for an estimated amount; **or**
2. The Transaction might not be completed for reasons other than technical failure or lack of full issuer approval; for example, 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 to determine if an authorization must be coded as a preauthorization.

Any ATM Transaction or Manual Cash Disbursement Transaction corresponding to an authorization identified as a preauthorization must be presented within **seven calendar days** of the authorization approval date. The presented Transaction amount must equal the authorized amount.

## 2.7 Final Authorizations

In the Europe Region, the Acquirer must ensure that any authorization request for an amount greater than zero is identified as a final authorization if:

- The Transaction may no longer 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); and
- The authorization being requested is for the final Transaction amount.

In the EEA, the Rule on this subject is modified as follows.

The authorization request must be identified as a final authorization in the field and with the value specified by the registered switch of the Issuer's choice.

## 2.8 Message Reason Code 4808 Chargeback Protection Period

In the Europe Region, the Rule on this subject is modified as follows.

The following message reason code 4808 (Authorization-related Chargeback) chargeback protection periods apply with respect to each approved authorization.

Each approved...	Has a message reason code 4808 chargeback protection period of...
Preauthorization of a Mastercard POS Transaction	Thirty (30) calendar days from the authorization approval date <sup>3</sup>
Preauthorization of a Maestro POS Transaction, ATM Transaction, or Manual Cash Disbursement Transaction	Seven (7) calendar days from the authorization approval date
Final authorization	Seven (7) calendar days from the authorization approval date

## 2.9 Multiple Authorizations

In the Europe Region, the Rule on this subject is modified as follows.

To extend the duration of the message reason code 4808 chargeback protection period afforded by an approved preauthorization of a Mastercard or Maestro Transaction, a Merchant or Acquirer may later submit an additional preauthorization request for the same Transaction. If the preauthorization request is for a zero amount, it extends the duration of the message reason code 4808 chargeback protection period with no change in the guaranteed Transaction amount. If the preauthorization request is for an amount higher than zero, it both extends the duration of the message reason code 4808 chargeback protection period and

<sup>3</sup> 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. Refer to Chapter 4 for Contactless Transit Aggregated Transaction processing procedures.

incrementally increases, by the amount of the new preauthorization request, the guaranteed Transaction amount to which the message reason code 4808 chargeback protection period applies. If the message reason code 4808 chargeback protection period has already expired, the new preauthorization request must be for the full Transaction amount rather than an incremental amount.

In each preauthorization request subsequent to the initial preauthorization request, the Acquirer must include a unique identifier from the initial approved preauthorization, by populating DE 48, subelement 63 (Trace ID) of each subsequent authorization request with the DE 63 (Network Data), subfield 1 (Financial Network Code) and subfield 2 (Banknet Reference Number) and DE 15 (Date, Settlement) data from the initial approved Authorization Request Response/0110 message. This unique identifier from the initial approved preauthorization must also be included in the Transaction clearing record.

Upon receipt of the Transaction clearing record, the Issuer must use the unique identifier to match the initial and any additional approved preauthorizations to the Transaction.

In the EEA, the Rule on this subject is additionally modified as follows.

The Acquirer must populate a unique identifier from the initial approved authorization of a Transaction in the appropriate field of additional authorizations and of the Transaction clearing record, in accordance with the specifications of the registered switch of the Acquirer's choice.

## **2.11 Full and Partial Reversals**

In the EEA, the Rule on this subject is modified as follows.

References to Reversal Request/0440 and Acquirer Reversal Advice/0420 messages are replaced by the corresponding message types of the registered switch of the Customer's choice.

### **2.11.1 Full and Partial Reversals—Acquirer Requirements**

In the Europe Region, the Rule on this subject is modified as follows.

With respect to POS Transactions and Merchandise Transactions, the Acquirer or Merchant must submit a reversal message to the Issuer within 24 hours of:

- The cancellation of a previously authorized Transaction, 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 clearing message is submitted within 24 hours of finalization of the Transaction.

The reversal requirement does not apply to Transactions occurring at a Merchant identified with MCC 5542 (Fuel Dispenser, Automated) or to Contactless transit aggregated Transactions or transit debt recovery Transactions.

The requirement for the Acquirer to ensure that a Merchant submits a reversal within 30 calendar days for a preauthorization or seven calendar days for a final authorization does not apply in the Europe Region.

The Acquirer of a Merchant located in **Italy** that is identified with an MCC listed in the table below and that accepts Mastercard or Debit Mastercard Cards must support full and partial reversals performed at the POI and whenever, for technical reasons, the Acquirer is unable to communicate the authorization response to the Merchant, for all prepaid Debit Mastercard and all prepaid Mastercard Card Account ranges:

<b>MCC</b>	<b>Description</b>
5310	Discount Stores
5311	Department Stores
5411	Grocery Stores, Supermarkets
5541	Service Stations (with or without Ancillary Services)
5542	Fuel Dispenser, Automated
5621	Women's Ready to Wear Stores
5691	Men's and Women's Clothing Stores
5732	Electronic Sales
5812	Eating Places, Restaurants
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5999	Miscellaneous and Specialty Retail Stores

### **2.11.2 Full and Partial Reversals—Issuer Requirements**

In Italy, the Rule on this subject is modified as follows.

An Issuer in **Italy** must support full and partial reversals for all prepaid Mastercard and all prepaid Debit Mastercard Card Account ranges.

## **2.12 Full and Partial Approvals**

In the Europe Region, the Rule on this subject is modified as follows.

A Customer must support partial approvals at Merchants identified with MCC 5542 (Fuel Dispenser, Automated) for all Mastercard Account ranges if the Customer supports partial approvals for Maestro or any other debit brand, as described in Rule 4.11.1.

An Issuer in the United Kingdom must support partial approval for all prepaid Mastercard, Debit Mastercard (including prepaid), and Maestro Account ranges.

An Acquirer, with respect to Merchants located in the United Kingdom, must:

1. For each Merchant in any of the categories listed below, with respect to Card-present Transactions at attended POS Terminals, support partial approval in its host system for all prepaid Mastercard, Debit Mastercard (including prepaid), and Maestro Account ranges; and
2. Effective 20 October 2020, ensure that each Merchant in any of the categories listed below, with respect to Card-present Transactions at attended POS Terminals, supports partial approval for all prepaid Mastercard, Debit Mastercard (including prepaid), and Maestro Account ranges.

#### **MCC Description**

- 5310 Discount Stores
- 5311 Department Stores
- 5411 Grocery Stores, Supermarkets
- 5541 Service Stations (with or without Ancillary Services)
- 5542 Fuel Dispenser, Automated
- 5621 Women's Ready to Wear Stores
- 5691 Men's and Women's Clothing Stores
- 5732 Electronic Sales
- 5812 Eating Places, Restaurants
- 5814 Fast Food Restaurants
- 5912 Drug Stores, Pharmacies
- 5999 Miscellaneous and Specialty Retail Stores

## **2.13 Refund Transactions and Corrections**

### **2.13.1 Refund Transactions—Acquirer Requirements**

In the EEA, the Rule on this subject is modified as follows.

References to First Presentment/1240 messages are replaced by the corresponding message type of the registered switch of the Customer's choice.

### **2.13.2 Refund Transactions—Issuer Requirements**

In the EEA, the Rule on this subject is modified as follows.

References to Authorization Request/0100 messages and data fields are replaced by the corresponding message type and data fields of the registered switch of the Customer's choice.

## **2.14 Balance Inquiries**

In the Europe Region, the Rule on this subject is modified as follows.

It is strongly recommended that an Issuer in the **Europe Region** support domestic, inter-European, and intra-European balance inquiries conducted at ATM Terminals.

If an Issuer provides balance inquiries for its Cardholders at its own ATM Terminals, it must also support balance inquiries at the ATM Terminals of other Customers in the Europe Region.

An Issuer may distinguish among Cards according to their category (for example, debit, credit).

In the EEA, the Rule on this subject is modified as follows.

A balance inquiry must be identified in the message type and field and with the value specified by the registered switch of the Customer's choice.

## 2.15 CVC 2 Verification for POS Transactions

In the Europe Region, the following applies to Mastercard POS Transactions:

An Acquirer must ensure that each of its Merchants that has exceeded 100 basis points in fraudulent Card-not-present (CNP) Transactions for two consecutive calendar months:

1. For all MO/TO Transactions, captures and transmits the CVC 2 value to the Issuer for validation; and
2. For all e-commerce Transactions, captures and transmits the CVC 2 value to the Issuer for validation or becomes Mastercard *SecureCode*™-enabled.

The Acquirer must ensure that the Merchant complies with this requirement within 120 days following the second trigger month.

An Issuer must not authorize a Mastercard POS Transaction identified as a mail order, phone order, or e-commerce Transaction if the CVC 2 transmitted by the Acquirer does not match the CVC 2 on file with the Issuer corresponding to the Mastercard Account in question (that is, DE 48, subelement 87 of the Authorization Request Responses/0110 message = "N").

In the **UK, Ireland, and France**, the following applies to Maestro Intracountry POS Transactions:

If an Issuer receives CVC 2 data in the authorization request and it is invalid (for example, the CVC 2 field is not blank and the data does not match the data held on the Issuer's records), the authorization request must be declined. The Issuer cannot use a fraud-related message reason code to charge back a Transaction after approving an authorization request for the Transaction that contained invalid CVC 2 data.

In the EEA, the Rule on this subject is modified as follows.

The value indicating a non-match of the CVC 2 must be populated in the field and with the value specified by the registered switch of the Customer's choice.

## 2.17 Euro Conversion

In the Europe Region, Transactions submitted into interchange that take place in countries that convert to the euro must be submitted in the euro. To allow a grace period for exceptional cases, the Interchange System will not reject Transactions submitted in currencies that have been replaced by the euro within six months after the transition period.

Within this six-month period, an Issuer may not reject or charge back Transactions submitted in currencies that the euro has replaced exclusively on grounds that such Transactions have not been submitted in euro.

## 2.21 Co-badged Cards—Acceptance Brand Identifier

The following Rules apply for Intracountry POS Transactions in the EU, Iceland, Norway, and Serbia, and for Cross-border POS Transactions between Iceland, Norway, Serbia, and an EU country, completed on Cards that are co-badged with another payment scheme than Mastercard or Maestro at Merchants that accept the other payment scheme as well as Mastercard and/or Maestro.

### All Transactions

When the acceptance brand is Mastercard or Maestro, the Customer must ensure that the acceptance brand selected by the Cardholder at the POI is accurately captured and recorded for each Transaction.

If the acceptance brand selected by the Cardholder is not transported or available, then the Transaction must be identified as Mastercard or Maestro if the Card or Account was issued under a BIN or BIN range assigned to the Corporation.

The Corporation has the right to review the selected acceptance brand when auditing a Customer's Transaction records, for example if reported volumes seem to be inaccurate.

### Chip Transactions

A Chip Transaction is a Mastercard or Maestro Transaction when an acceptance brand identifier that uniquely relates to Mastercard or Maestro is sent by the Terminal to the Acquirer. The acceptance brand identifier is transmitted in the Dedicated File Name (DF Name).

All chip-capable Terminals must capture and transmit the DF Name when the Chip Transaction is a Mastercard or Maestro Transaction.

An Acquirer must itself transport, and must ensure that the registered switch of its choice transports, the DF Name to the Issuer in the authorization and clearing message for a Mastercard or Maestro Chip Transaction.

Each Customer must store the DF Name along with other Transaction data and must rely on the DF Name to identify that a Chip Transaction is a Mastercard or Maestro Transaction.

### Electronic Commerce Transactions

The Acquirer and Merchant must rely on the acceptance brand selected by the Cardholder to identify that a Transaction is a Mastercard or Maestro Transaction.

An Acquirer must itself transport, and must ensure that the registered switch of its choice transports, the acceptance brand to the Issuer in the authorization and clearing message for a Mastercard or Maestro Transaction.

Each Customer must store the acceptance brand along with other Transaction data and must rely on the acceptance brand to identify that a Transaction is a Mastercard or Maestro Transaction.



## Latin America and the Caribbean Region

---

The following modifications to the Rules apply in the Latin America and the Caribbean Region. Refer to Appendix A for the Latin America and the Caribbean Region geographic listing.

### 2.16 CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless—Brazil Only

In Brazil, for each Maestro Magnetic Stripe Mode Contactless Transaction, the Issuer must verify the dynamic CVC 3 value in the authorization request and provide the result in the response message.

## United States Region

---

The following modifications to the Rules apply in the United States (U.S.) Region. Refer to Appendix A for the U.S. Region geographic listing.

### 2.1 Acquirer Authorization Requirements

In the U.S. Region, the Rule on this subject is modified as follows.

An Acquirer must support POS balance inquiry for all prepaid Debit Mastercard and prepaid Maestro Accounts.

#### 2.1.1 Acquirer Host System Requirements

An Acquirer in the U.S. Region must ensure that its POS Terminal host systems and those of its Service Providers:

1. Are capable of processing Contact Chip Transactions and Contactless Transactions (including both EMV Mode Contactless Transactions and Magnetic Stripe Mode Contactless Transactions;
2. Support the transmission of Contact Chip Transaction and Contactless Transaction messages in accordance with the Standards;
3. Support PIN (both online and offline), signature, and no Cardholder verification method (CVM) as CVM options for Chip Transactions, regardless of whether each Hybrid POS Terminal connected to the Acquirer host system supports all of 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 Corporation, with respect to each Interchange System network interface, as enabled for Contact Chip Transaction and Contactless Transaction processing.

### 2.2 Issuer Authorization Requirements

In the U.S. Region, the Rule on this subject is modified as follows.

A Maestro Card Issuer must also support:

- Partial approval from primary account, checking account, savings account, and pooled account
- Full and partial reversal
- POS balance response for prepaid Accounts

Each Maestro and Cirrus Card Issuer must offer cash withdrawal from a savings account and from a checking account, and may optionally offer Shared Deposit to a savings account and to a checking account.

An Issuer may decline authorization of a Transaction when technical fallback from chip to magnetic stripe occurred.

### **2.2.1 Issuer Host System Requirements**

In the U.S. Region, the Rule on this subject is modified as follows.

A Maestro Card Issuer's host system interfaces must support POS balance inquiry.

### **2.2.2 Stand-In Processing Service**

In the U.S. Region, the following requirements apply with respect to Mastercard Card Programs.

For all Mastercard Card Programs, an Issuer must use the Stand-In Processing Service. For all Mastercard Card Programs except Debit Mastercard Card Programs, Stand-In Parameters must be set at or above the Corporation's default limits.

In the event that fraudulent activity is detected with respect to a BIN or BIN range, the Corporation, in its sole discretion and judgment, may take such action as the Corporation deems necessary or appropriate to safeguard the goodwill and reputation of the Corporation'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 BIN or BIN range.

For Debit Mastercard Card Programs, the following requirements apply:

1. For all Transactions identified with a TCC of C, P, T, U, or Z, the Transaction category code (TCC) limit may be set below the Corporation's default value.
2. For all Card-not-present Transactions, the TCC limit may be set below the Corporation's default value.
3. For Card-present Transactions identified with a TCC of A, F, H, O, R, or X and effected with a Debit Mastercard Card (standard), the TCC limit may be set below the Corporation's default value to an amount no less than USD 50.
4. For Card-present Transactions identified with a TCC of A, F, H, O, R, or X and effected with a Debit Mastercard Card (enhanced), the TCC limit may be set below the Corporation's default value to an amount no less than USD 100.
5. For Card-present Transactions identified with a TCC of A, C, F, H, O, R, or X and effected with a Debit Mastercard BusinessCard Card or Debit Mastercard Professional Card, the TCC limit may be set below the Corporation's default value to an amount no less than USD 400.

6. For Debit Mastercard Card (standard) Programs, the accumulative limits may be set below the Corporation's default values as follows.

Day	Minimum Transaction Count	Recommended Transaction Count	Minimum Transaction Amount
1	4	6	USD 50
2	6	12	USD 100
3	6	18	USD 150
4	6	24	USD 200

7. For Debit Mastercard Card (enhanced) Programs, the accumulative limits may be set below the Corporation's default values as follows.

Day	Minimum Transaction Count	Recommended Transaction Count	Minimum Transaction Amount
1	4	6	USD 100
2	6	12	USD 200
3	6	18	USD 300
4	6	24	USD 400

8. For Debit Mastercard Business Card Card and Debit Mastercard Professional Card Programs, the accumulative Limits may be set below the Corporation's default values as follows.

Day	Minimum Transaction Count	Recommended Transaction Count	Minimum Transaction Amount
1	4	4	USD 750
2	6	6	USD 1,000
3	6	6	USD 1,000
4	6	6	USD 1,000

## 2.4 Performance Standards

## 2.4.2 Performance Standards—Issuer Requirements

In the U.S. Region, the Rule on this subject is replaced with the following.

An Issuer authorization failure rate for Maestro POS Transactions and ATM Transactions that exceeds two percent (2%) in any given calendar month is deemed to be substandard performance. The Issuer failure rate is not applied until after the Issuer's fourth calendar month of operation or upon the Issuer's processing of 5,000 Transactions in a calendar month, whichever occurs first. Refer to "Calculation of the Issuer Failure Rate" in this chapter for the formula used to calculate the Issuer authorization failure rate.

## 2.5 Preauthorizations

### 2.5.2 Preauthorizations—Maestro POS Transactions

In the U.S. Region, the Rule on this subject is modified as follows.

The Acquirer is not liable for preauthorization completions that occurred within 20 minutes of the initial Maestro POS Transaction but were subsequently stored and forwarded because of technical problems between the Acquirer and the Interchange System, or the Interchange System and the Issuer.

No CVM is required for a PIN-less Single Message Transaction preauthorization.

## 2.11 Full and Partial Reversals

### 2.11.1 Full and Partial Reversals—Acquirer Requirements

In the U.S. Region, the Rule on this subject is modified as follows.

For Merchants in the categories listed in the following table, the Acquirer must ensure that with respect to the acceptance of Debit Mastercard Cards, the Merchant supports full and partial reversals performed at the POI and whenever, for technical reasons, the Acquirer is unable to communicate the authorization response to the Merchant.

MCC	Description
4111	Transportation—Suburban and Local Commuter Passenger, including Ferries
4812	Telecommunication Equipment including Telephone Sales
4814	Telecommunication Services
4816	Computer Network/Information Services
4899	Cable, Satellite, and Other Pay Television and Radio Services
5111	Stationery, Office Supplies
5200	Home Supply Warehouse Stores
5300	Wholesale Clubs

<b>MCC</b>	<b>Description</b>
5310	Discount Stores
5311	Department Stores
5331	Variety Stores
5399	Miscellaneous General Merchandise Stores
5411	Grocery Stores, Supermarkets
5499	Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores
5541	Service Stations (with or without Ancillary Services)
5542	Fuel Dispenser, Automated
5732	Electronic Sales
5734	Computer Software Stores
5735	Record Shops
5812	Eating Places, Restaurants
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5921	Package Stores, Beer, Wine, and Liquor
5941	Sporting Goods Stores
5942	Book Stores
5943	Office, School Supply and Stationery Stores
5999	Miscellaneous and Specialty Retail Stores
7829	Motion Picture-Video Tape Production-Distribution
7832	Motion Picture Theaters
7841	Video Entertainment Rental Stores
7996	Amusement Parks, Carnivals, Circuses, Fortune Tellers
7997	Clubs—Country Membership
8011	Doctors—not elsewhere classified
8021	Dentists, Orthodontists

MCC	Description
8041	Chiropractors
8042	Optometrists, Ophthalmologists
8043	Opticians, Optical Goods, and Eyeglasses
8062	Hospitals
8099	Health Practitioners, Medical Services—not elsewhere classified
7999	Recreation services—not elsewhere classified
8999	Professional Services—not elsewhere classified
9399	Government Services—not elsewhere classified

### 2.11.2 Full and Partial Reversals—Issuer Requirements

In the U.S. Region, the Rule on this subject is modified as follows.

For all Debit Mastercard Card Account ranges, an Issuer must support full and partial reversals.

## 2.12 Full and Partial Approvals

In the U.S. Region, the Rule on this subject is modified as follows.

A Customer must provide partial approval authorization services as set forth below:

1. For all Debit Mastercard Account ranges, the Issuer must support partial approvals.
2. For all Debit Mastercard and Maestro Account ranges, the Acquirer of a Merchant identified with MCC 5542 (Fuel Dispenser, Automated) must support partial approvals.
3. For Merchants in the categories listed in the table provided in “Full and Partial Reversals” in this U.S. Region section, the Acquirer and each such Merchant must support partial approvals for Card-present Transactions occurring at attended POS Terminals for all Debit Mastercard and Maestro Account ranges.

## 2.14 Balance Inquiries

In the U.S. Region, the Rule on this subject is modified as follows.

The Acquirer must ensure that a balance inquiry is initiated through the use of a PIN and a magnetic stripe reader and is performed only at Cardholder-operated Terminals.

## Chapter 3 Acceptance Procedures

*The following Standards apply with regard to Card acceptance at the Point of Interaction (POI). Where applicable, variations or additions by region and/or country are provided at the end of this chapter in the section titled, "Variations and Additions by Region."*

3.1 Card-Present Transactions.....	82
3.1.1 Mastercard Card Acceptance Procedures.....	82
Suspicious Cards.....	83
3.1.2 Maestro Card Acceptance Procedures.....	83
3.2 Card-Not-Present Transactions.....	83
3.3 Obtaining an Authorization.....	83
3.3.1 Mastercard POS Transaction Authorization Procedures.....	83
Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions.....	84
Authorization When the Cardholder Adds a Gratuity.....	85
Card-Not-Present Transaction Declines.....	85
Use of Card Validation Code (CVC) 2.....	86
Capture Card Response.....	86
3.3.2 Maestro POS Transaction Authorization Procedures.....	86
3.4 Mastercard Cardholder Verification Requirements.....	87
CVM Not Required for Refund Transactions.....	88
Use of PIN for Mastercard Magnetic Stripe Transactions.....	88
3.5 Maestro Cardholder Verification Requirements.....	88
3.6 Use of a PIN for Transactions at ATM Terminals and Bank Branch Terminals.....	89
3.7 Use of a Consumer Device CVM.....	90
3.8 POI Currency Conversion.....	90
3.8.1 Cardholder Disclosure—Attended POS Terminal.....	91
3.8.2 Cardholder Disclosure—Unattended POS Terminal.....	91
3.8.3 Cardholder Disclosure—ATM Terminal.....	92
3.8.4 Cardholder Disclosure—Transaction Receipt Information.....	92
3.8.5 Transaction Processing Requirements.....	92
3.9 Multiple Transactions—Mastercard POS Transactions Only.....	93
3.10 Partial Payment—Mastercard POS Transactions Only.....	93
3.11 Specific Terms of a Transaction.....	94
3.11.1 Specific Terms of an E-commerce Transaction.....	94
3.12 Charges for Loss, Theft, or Damage—Mastercard POS Transactions Only.....	94
3.13 Providing a Transaction Receipt.....	95
3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements.....	96

3.13.2 ATM and Bank Branch Terminal Transaction Receipt Requirements.....	97
3.13.3 Primary Account Number (PAN) Truncation and Expiration Date Omission.....	98
3.13.4 Prohibited Information.....	98
3.13.5 Standard Wording for Formsets.....	98
3.14 Returned Products and Canceled Services.....	99
3.14.1 Refund Transactions.....	99
3.15 Transaction Records.....	101
3.15.1 Retention of Transaction Records.....	101
Variations and Additions by Region.....	101
Asia/Pacific Region.....	101
3.14 Returned Products and Canceled Services.....	102
3.14.1 Refund Transactions.....	102
Canada Region.....	102
Europe Region.....	102
3.1 Card-Present Transactions.....	102
3.1.1 Mastercard Card Acceptance Procedures.....	102
3.2 Card-Not-Present Transactions.....	102
3.3 Obtaining an Authorization.....	103
3.3.1 Mastercard POS Transaction Authorization Procedures.....	103
Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions.....	103
Authorization When the Cardholder Adds a Gratuity.....	103
3.3.2 Maestro POS Transaction Authorization Procedures.....	103
3.5 Maestro Cardholder Verification Requirements.....	104
3.8 POI Currency Conversion.....	104
3.13 Providing a Transaction Receipt.....	104
3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements.....	104
3.13.3 Primary Account Number (PAN) Truncation and Expiration Date Omission.....	105
3.14 Returned Products and Canceled Services.....	105
3.14.1 Refund Transactions.....	105
Latin America and the Caribbean Region.....	105
3.5 Maestro Cardholder Verification Requirements.....	106
Middle East/Africa Region.....	106
3.14 Returned Products and Canceled Services.....	106
3.14.1 Refund Transactions.....	106
United States Region.....	106
3.3 Obtaining an Authorization.....	106
3.3.1 Mastercard POS Transaction Authorization Procedures.....	106
Authorization When the Cardholder Adds a Gratuity.....	106



---

3.5 Maestro Cardholder Verification Requirements.....	107
Additional U.S. Region and U.S. Territory Rules.....	107
3.14 Returned Products and Canceled Services.....	108
3.14.1 Refund Transactions.....	108

## 3.1 Card-Present Transactions

---

A Card-present Transaction occurs when the Cardholder has presented a Card or Access Device to a Merchant or Customer representative in a face-to-face environment, or uses a Card or Access Device to initiate a Transaction at an ATM Terminal or unattended POS Terminal.

A Card-present Transaction conducted at a Terminal should be processed using the highest level of technology supported by both the Card or Access Device and the Terminal, as follows:

1. If a Chip Card or Access Device is presented at a Card-reading Hybrid Terminal, complete the Transaction in accordance with the technical specifications set forth in the *M/Chip Requirements for Contact and Contactless*; or
2. If a Card is presented at a magnetic stripe-reading Terminal that is not chip-enabled, ensure that the Card's magnetic stripe is "read" by the Terminal.

Each Transaction must be authorized as described in Rule 3.3.

### 3.1.1 Mastercard Card Acceptance Procedures

The following procedures apply to the face-to-face acceptance of a Mastercard Card (but not an Access Device).

A Mastercard Card is not required to be accepted 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.

The following steps may be performed to determine the validity of a Mastercard Card:

- Check for the presence of the Mastercard or Debit Mastercard hologram, as applicable, the Mastercard HoloMag™, or the Premium Brand Mark.
- If the POS Terminal displays the PAN encoded on the magnetic stripe, then compare the last four digits of the PAN on the Card with the four-digit truncated PAN displayed on the POS Terminal.
- If signature is obtained, and if a signature panel is present on the Card, and if a signature is present on the signature panel, check whether the signature on the Transaction receipt appears to match the signature on the Card.

The following steps are required for all face-to-face unique Transactions (TCC of U) and Manual Cash Disbursement Transactions, unless PIN or CDCVM is used as the CVM:

- Request personal identification in the form of an unexpired, official government document (for example, a passport, identification document, or driver's license) that bears the Cardholder's signature, the Cardholder's photograph, or both.
- Check whether the signature, if present, on the personal identification appears to match the signature on the Card, if a signature panel is present on the Card, and if a signature is present on the signature panel.

- Compare the photograph, if present, with the person presenting the Card.
- Record the personal identification type and number on the Transaction receipt.

### **Suspicious Cards**

When suspicious that a presented Mastercard Card may not be valid, the Merchant or Customer accepting the Card should follow the Acquirer's "Code 10" (suspicious Card) procedures, which may include placing a value of 1 (Suspected fraud [merchant suspicious—code 10]) in DE 61, subfield 8 (Transaction Security) of the authorization request message.

**NOTE: A modification to this Rule appears in the "Europe Region" section at the end of this chapter.**

## **3.1.2 Maestro Card Acceptance Procedures**

A Maestro Card must not be accepted if neither the magnetic stripe nor the contact or contactless chip on the Card can be read for any reason.

Electronic key entry of Maestro Card information into a POS Terminal is permitted only for refund Transactions. An Issuer is not responsible for a Maestro POS Transaction if the PAN was manually entered into the POS Terminal and the approved Transaction was subsequently determined to have arisen through use of a fraudulent Card and/or unauthorized use of a PIN.

## **3.2 Card-Not-Present Transactions**

---

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, or Credential-on-file Transaction.

A Merchant must not refuse to complete a Mastercard e-commerce Transaction solely because the Cardholder does not have a digital certificate or other secured protocol.

**NOTE: A Rule variation on this subject appears in the "Europe Region" section at the end of this chapter.**

## **3.3 Obtaining an Authorization**

---

With respect to securing authorizations, an Acquirer must treat all Transactions at a Merchant in the same manner.

### **3.3.1 Mastercard POS Transaction Authorization Procedures**

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. This requirement does not apply to:

- Contactless transit aggregated or transit debt recovery Transactions;

- Automated fuel dispenser (AFD) Transactions (MCC 5542); or
- An authorization requested for an amount otherwise approved by the Cardholder as the final Transaction amount.

Refer to Chapter 2 for requirements relating to the proper identification of a Processed Transaction authorization request for an amount greater than zero as a preauthorization (in all Regions), undefined authorization (in all Regions except the Europe Region), or final authorization (in all Regions).

A Merchant must obtain an online authorization from the Issuer for all Transactions, with the following exceptions:

1. Transactions at a CAT 3 device.

**NOTE: The maximum Transaction amount for magnetic stripe-based Transactions at CAT 3 devices, including Magnetic Stripe Mode Contactless Transactions, is zero (except in Hong Kong and Macao, where the maximum Transaction amount is HKD 500 and MOP 500, respectively). The maximum Transaction amount for Contact Chip and EMV Mode Contactless Transactions is EUR 50 in the Europe Region and USD 40 outside of the Europe Region.**

2. Chip Transactions authorized offline by the EMV chip, including both Contact Chip and EMV mode Contactless Transactions, when the Transaction amount is equal to or less than USD 200, or EUR 200 for a Merchant in the Europe Region.
3. Refund Transactions.

A Merchant or its Acquirer may obtain a voice authorization from the Issuer, with the understanding that the authorization code obtained in a voice authorization is not a valid remedy to an authorization-related chargeback.

Terminal offline chip authorization limits are published in Chapter 5 of the *Quick Reference Booklet*.

For additional authorization message requirements, including how a Merchant or Acquirer may convert an Issuer's approval of a Card-not-present Transaction believed in good faith to be fraudulent to a decline, refer to Chapter 2.

**NOTE: A modification to this Rule appears in the "Europe Region" section at the end of this chapter.**

### **Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions**

Lodging, cruise line, and vehicle rental Merchants may request an authorization for an estimated Transaction amount, and may submit subsequent authorization requests for any additional estimated amounts as needed. For more information, refer to Rule 2.9.

Vehicle rental Merchants:

1. May 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; and

2. Before the Cardholder enters into a rental agreement, the Merchant must disclose to the Cardholder the amount of the authorization request to be sent to the Issuer.

Charges for loss, theft, or damage must be processed separately.

The Transaction amount of a lodging, cruise line, or vehicle rental Processed Transaction must not exceed the authorized amount. If the Merchant obtains a preauthorization for an estimated amount, and the Transaction amount exceeds the authorized amount, the Merchant may request an incremental authorization. In connection with such Transactions, the Issuer must not place a hold on the Cardholder's Account in excess of the authorized amount.

**NOTE: A modification to this Rule appears in the "Europe Region" section at the end of this chapter.**

### **Authorization When the Cardholder Adds a Gratuity**

When a **preauthorization** (in all Regions) or an **undefined authorization** (in all Regions except the Europe Region) is obtained:

- If the Transaction is a Card-Not-Present Transaction, Chip/PIN Transaction, Contactless Transaction, or Mastercard Consumer-Presented Quick Response (QR) Transaction, any gratuity must be included in the authorization request. A gratuity must not be added after authorization is obtained.
- For all other Transaction types, including signature-based magnetic stripe and Chip Transactions, a gratuity may be added after authorization is obtained.
  - If the gratuity does not exceed 20 percent of the authorized amount, then no additional authorization is needed.
  - If the gratuity exceeds 20 percent of the authorized amount, then the Merchant may request an incremental authorization for the amount in excess of the authorized amount.

For all Transactions, if the authorization request message contains the Partial Approval Terminal Support Indicator, and the authorization request response message contains a value of 10 (Partial Approval) in DE 39 and a partial approval amount in DE 6, the Transaction amount must not exceed the authorized amount.

The Issuer must not place a hold on the Cardholder's Account in excess of the total authorized amount (inclusive of the 20 percent tolerance, if applicable, or any incremental authorization).

**NOTE: Modifications to this Rule appear in the "Europe Region" and "United States Region" sections at the end of this chapter.**

### **Card-Not-Present Transaction Declines**

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.

Response Code Value	Description
04	Capture card
14	Invalid card number
15	Invalid issuer
41	Lost card
43	Stolen card
54	Expired card

### Use of Card Validation Code (CVC) 2

In a Card-not-present environment, a Merchant may request a Card validation code (CVC) 2 verification from the Issuer, as a means to check the validity of a Mastercard Card.

All non-face-to-face gambling Transactions (MCC 7995) conducted with a Mastercard Card must include the CVC 2 value in DE 48 (Additional Data—Private Use), subelement 92 (CVC 2) of the Authorization Request/0100 message.

CVC 2 data must not be stored by the Merchant, its Acquirer, or any Service Provider. Refer to section 3.10 of the *Security Rules and Procedures* manual for additional CVC 2 requirements.

### 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.

## 3.3.2 Maestro POS Transaction Authorization Procedures

A Merchant must obtain an online authorization from the Issuer or its agent for all Maestro magnetic stripe POS Transactions. With respect to Maestro Chip Transactions, the Terminal offline chip authorization limits published in Chapter 5 of the *Quick Reference Booklet* apply. A Merchant must obtain an online authorization for a Chip Transaction that exceeds the published Terminal offline chip authorization limit and whenever the Card or the Hybrid POS Terminal requires online authorization. Before completing a Chip Transaction for which online authorization is required or requested, the Merchant must obtain a Transaction Certificate (TC) and related data.

For additional authorization message requirements, including how a Merchant or Acquirer may convert an Issuer's approval of a Card-not-present Transaction believed in good faith to be fraudulent to a decline, refer to Chapter 2.

**NOTE: An addition to this Rule appears in the “Europe Region” section at the end of this chapter.**

## 3.4 Mastercard Cardholder Verification Requirements

In a face-to-face Transaction environment, the Merchant Terminal must support signature as a Cardholder verification method (CVM) for a Mastercard POS Transaction.

Unless PIN, Consumer Device CVM (CDCVM), successful Cardholder authentication on a Mastercard Biometric Card, or “No CVM” is used as the CVM in accordance with the Standards, the Merchant may request that the Cardholder sign the Merchant’s copy of the Transaction receipt.

For a Mastercard Contactless Transaction that...	Then....
Is less than or equal to the applicable contactless CVM limit	“No CVM” is the only CVM option. The Merchant must not request that the Cardholder sign the Merchant’s copy of the Transaction receipt.
Exceeds the applicable contactless CVM limit	<p>The CVM may be any of the following, provided both the Card or Access Device and the POS Terminal support the CVM:</p> <ul style="list-style-type: none"> <li>• Signature—When signature is selected as the CVM, the Merchant may request the Cardholder’s signature</li> <li>• Online PIN</li> <li>• Consumer Device CVM (CDCVM)</li> </ul>

With respect to Mastercard POS Transactions conducted by a Merchant using an MPOS Terminal or a Chip-only MPOS Terminal:

1. If the MPOS Terminal or Chip-only MPOS Terminal does not support electronic signature capture and cannot print a paper Transaction receipt, then signature is not required; and
2. If the Merchant has less than USD 100,000 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. Refer to Rule 7.4.3 regarding restrictions on the use of certain MPOS Terminal types.)

In a Card-not-present Transaction environment, the Merchant may complete the Transaction without using a CVM.

Refer to Appendix D for CVM requirements at unattended POS Terminals.

### **CVM Not Required for Refund Transactions**

No CVM is required for a refund Transaction. However, when a PIN is used as the CVM for a refund Transaction conducted at a Hybrid POS Terminal, the Merchant must obtain a successful PIN validation.

### **Use of PIN for Mastercard Magnetic Stripe Transactions**

Mastercard may authorize the use of a PIN for Mastercard magnetic stripe Transactions at selected Merchant types, POS Terminal types, or Merchant locations in specific countries.

Acquirers and Merchants that support PIN-based Mastercard magnetic stripe Transactions must provide Cardholders with the option of a signature-based Transaction, unless the Transaction occurs at a CAT 1 device or at a CAT 3 device with offline PIN capability for Chip Transactions. At a CAT 1 device, use of a PIN is required.

Each PIN-capable POS Terminal must meet specific requirements for PIN processing wherever an approved implementation of PIN for magnetic stripe Transactions takes place. When applicable, each Transaction must be initiated with a Card in conjunction with the PIN entered by the Cardholder at the Terminal. The Acquirer must be able to transmit the PIN in the Authorization Request/0100 or Financial Transaction Request/0200 message in compliance with all applicable PIN security Standards.

Acquirers must control Terminals equipped with PIN entry devices (PEDs) or encrypting PIN pads (EPPs). If a Terminal is capable of prompting for the PIN, the Acquirer must include the PIN and full magnetic stripe-read data in the Authorization Request/0100 message. A Cardholder must not be required to disclose a PIN, other than by private entry into a secure PED.

An Issuer should refer to the *Authorization Manual* for information about optional PIN verification during Stand-In Processing.

## **3.5 Maestro Cardholder Verification Requirements**

---

For each Card-present Maestro POS Transaction, PIN must be used as the CVM, whether magnetic stripe or chip is used to initiate the Transaction, except in the case of:

1. A properly presented Contactless Transaction for which no CVM is required or when Consumer Device CVM (CDCVM) has been successfully completed;
2. No-CVM Transactions conducted in the Europe Region; and
3. A Transaction occurring at a Hybrid POS Terminal in a country in which the Corporation has consented to the use of offline PIN as the minimum CVM for a Chip Transaction and signature as the CVM for a magnetic stripe Transaction.

At present, the Corporation has given such consent to Customers in:

1. Andorra
2. Belgium
3. Estonia



- 
4. Finland
  5. France
  6. Ireland
  7. Israel
  8. Latvia
  9. Lithuania
  10. Monaco
  11. Portugal
  12. Spain
  13. United Kingdom

As of 1 January 2020, Estonia, Latvia, and Lithuania will be removed from the above list.

An Issuer must not decline authorization of a Transaction solely because the PIN was verified in an offline mode or because the Transaction occurred in a country where the Corporation has granted Customers a waiver allowing the use of a signature-based CVM instead of a PIN-based CVM. An Issuer must accept and properly process (by performing an individual risk assessment on) each Transaction verified using a signature-based CVM in the same manner as the Issuer would if the Transaction had been verified using a PIN-based CVM.

**NOTE: Modifications to this Rule appear in the “Europe Region,” “Latin America and the Caribbean Region,” and “United States Region” sections at the end of this chapter.**

### 3.6 Use of a PIN for Transactions at ATM Terminals and Bank Branch Terminals

---

The following requirements apply with respect to Transactions occurring at ATM Terminals and Bank Branch Terminals.

1. At an ATM Terminal and when a Maestro or Cirrus Card or PIN-preferring Mastercard Card is accepted at a Bank Branch Terminal, the Cardholder must be verified by a PIN, whether magnetic stripe or chip is used to initiate the Transaction.
2. For magnetic stripe Transactions, PIN verification must be online.
3. For a Cardless ATM Transaction, the Cardholder must be verified by Consumer Device CVM (CDCVM) and may also be verified by PIN.

A Cardless ATM Transaction is identified in Authorization Request/0100 and Financial Transaction Request/0200 messages with:

- Data Element (DE) 22 (POS Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) = 09 (PAN/Token entry via electronic commerce containing DSRP cryptogram in DE 55 (Integrated Circuit Card [ICC] System-Related Data)
- DE 18 (Merchant Type) = 6011 (Automated Cash Disbursements—Customer Financial Institution)
- DE 48 (Additional Data—Private Use), Transaction Category Code = Z (Automated Cash Disbursement)

- DE 48, subfield 28 (Cardless ATM Order ID) = a 10-digit order ID provided by Mastercard Cardless engine
- 4. 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.

### 3.7 Use of a Consumer Device CVM

---

A Consumer Device CVM (CDCVM) may only be used as a CVM for Transactions if:

1. The CDCVM has been qualified by Mastercard, as set forth in Chapter 3 of the *Security Rules and Procedures*; 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.

### 3.8 POI Currency Conversion

---

For purposes of these POI currency conversion Rules, billing currency is the currency in which the Card was issued.

POI currency conversion is a service that may be offered by a Merchant or Acquirer. The service enables a Cardholder to decide whether a Transaction should be completed in either the local currency or the billing currency. POI currency conversion is also referred to as dynamic currency conversion, or DCC. If POI currency conversion is used for a Transaction, the foreign exchange rate is applied by the Merchant or Acquirer.

When POI currency conversion is offered, the Transaction currency is the currency selected by the Cardholder at the Point-of-Sale (POS) Terminal, ATM Terminal, or Bank Branch Terminal.

An Acquirer that intends to acquire Transactions on which POI currency conversion has been performed first must register with the Corporation to do so.

POI currency conversion must not be offered on a Contactless Transaction that is equal to or less than the applicable CVM limit or on any Contactless transit aggregated Transaction for which a ceiling limit applies. POI currency conversion optionally may be offered on a Contactless Transaction that exceeds the CVM limit.

POI currency conversion must not be offered on any ATM or face-to-face Transaction effected with Mastercard and Maestro Prepaid Cards that have single or multi-currency features or that are otherwise identified in the Mastercard Parameter Extract (MPE) as ineligible for POI currency conversion.

POI currency conversion must not be offered on any Mastercard and Maestro branded debit Card that is a multi-currency Card where the Issuer's associated account range for all cross-border Card-present Transactions volume of a full calendar year is equal to or greater than fifty percent of its total Card-present Transaction volume in the same year.

POI currency conversion may be offered, subject to all of the following conditions:

- No specific currency conversion method may be implemented as the default option, except that when POI currency conversion is offered on the Internet, a currency conversion option may be pre-selected;
- A Cardholder may not be required or encouraged (i.e., "steered") in any manner to use POI currency conversion. For example, a POS Terminal must not ask or require a Cardholder to choose to have the Transaction completed in a particular currency, whether by selecting "YES" or "NO" or by displaying different currency selections in red and green colors, or otherwise; and
- The offer complies with the following Attended POS Terminal, Unattended POS Terminal, or ATM Terminal Cardholder disclosure requirements, as applicable.

**NOTE: A modification to this Rule appears in the "Europe Region" section at the end of this chapter.**

### 3.8.1 Cardholder Disclosure—Attended POS Terminal

Before an authorization or preauthorization request for the Transaction is submitted, and before the Cardholder decides the currency in which the Transaction is to be completed:

- The Cardholder must be clearly informed that the Cardholder has the right to choose the currency in which the Transaction will be completed;
- The Cardholder must be clearly informed of each of the following:
  - Transaction amount in the local currency;
  - Transaction amount in the billing currency;
  - Currency conversion rate to be applied should the Transaction be completed in the billing currency; and
- The Merchant must honor the choice of the Cardholder.

### 3.8.2 Cardholder Disclosure—Unattended POS Terminal

Before an authorization or preauthorization request for the Transaction is submitted, and before the Cardholder decides the currency in which the Transaction is to be completed, the POS Terminal must clearly indicate to the Cardholder:

- The Cardholder has the right to choose the currency in which the Transaction will be completed;
- Transaction amount in the local currency;
- Transaction amount in the billing currency;
- A separate and equivalent button (or other means) available for the Cardholder to select which currency is to be used to complete the Transaction;

- Currency conversion rate to be applied should the Transaction be completed in the billing currency; and
- Before the Cardholder is asked to select a currency in which the Transaction is to be completed, the unattended POS Terminal must clearly disclose the following, verbatim, to the Cardholder: "MAKE SURE YOU UNDERSTAND THE COSTS OF CURRENCY CONVERSION AS THEY MAY BE DIFFERENT DEPENDING ON WHETHER YOU SELECT YOUR HOME CURRENCY OR THE TRANSACTION CURRENCY."

If an unattended POS Terminal cannot comply with the Cardholder disclosure requirements set forth above, the Merchant must satisfy the requirements by some alternative means designed to ensure that the Cardholder understands the POI currency conversion before the Cardholder is asked to decide the currency the Transaction is to be completed in.

### 3.8.3 Cardholder Disclosure—ATM Terminal

Each screen message of an ATM Terminal offering POI currency conversion must include:

- A clear message advising the Cardholder of an option to complete the Transaction in either the local currency or the Cardholder's billing currency;
- The requested cash withdrawal amount reflected in both the local currency and the Cardholder's billing currency;
- Any other fee that can be charged in the event the cardholder selects POI currency conversion;
- Total amount comprised of the cash withdrawal amount and access fee;
- The currency conversion rate to be applied should the Transaction be completed in the Cardholder's billing currency; and
- Before the Cardholder is asked to select a currency in which the Transaction is to be completed, the Terminal must clearly disclose the following, verbatim, to the Cardholder: "MAKE SURE YOU UNDERSTAND THE COSTS OF CURRENCY CONVERSION AS THEY MAY BE DIFFERENT DEPENDING ON WHETHER YOU SELECT YOUR HOME CURRENCY OR THE TRANSACTION CURRENCY."

### 3.8.4 Cardholder Disclosure—Transaction Receipt Information

If the Cardholder has chosen to use the POI currency conversion service to complete the Transaction, the Cardholder must be offered a Transaction receipt that discloses all of the following:

- The total Transaction amount in the local currency;
- The total Transaction amount in the converted currency as agreed to by the Cardholder;
- The currency symbol or code of each; and
- The currency conversion rate used.

### 3.8.5 Transaction Processing Requirements

The currency chosen by the Cardholder must be indicated as the Transaction currency in DE 49 of Transaction messages.

The POI currency conversion indicator, pre-conversion currency, and amount must be provided in DE 54 of Financial Transaction/0200 messages and First Presentment/1240 messages.

If the Cardholder does not choose to have the Transaction completed in the Cardholder's billing currency, the Transaction must be completed and processed in the local currency.

A refund Transaction must be processed in the same currency used when the returned goods or canceled services were purchased.

Before offering POI currency conversion at an ATM Terminal, the Acquirer must either submit the proposed screen messages and a sample receipt to the Corporation for review and potential approval or implement screen messages and receipts in the form shown in Appendix F.

**NOTE: The Mastercard standard disclaimer is shown in Screen 2 of "Model Screens Offering POI Currency Conversion," Appendix F.**

---

### 3.9 Multiple Transactions—Mastercard POS Transactions Only

---

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 may 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 may 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.

---

### 3.10 Partial Payment—Mastercard POS Transactions Only

---

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.

### 3.11 Specific Terms of a Transaction

---

The Merchant may 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 may 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.

#### 3.11.1 Specific Terms of an E-commerce Transaction

In an e-commerce Transaction:

1. A Cardholder may accept 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.

### 3.12 Charges for Loss, Theft, or Damage—Mastercard POS Transactions Only

---

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. For CVM requirements, see Rule 3.4.

- A fully authenticated *SecureCode* or Identity Check 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 may 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.

### 3.13 Providing a Transaction Receipt

---

A Transaction receipt (also called a Transaction Information Document, or TID) must be provided to the Cardholder upon completion of a Transaction as required by and in a form that is compliant with the Standards and applicable law or regulation.

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.

#### At POS Terminals

At a POS Terminal (including any MPOS or CAT device unless otherwise stated), a copy of the 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 QPS Transaction or Contactless Transaction that is equal to or less than the CVM limit or Contactless transit aggregated Transaction ceiling limit amount, as applicable, 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.

The following POS Terminal types are 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:

- A POS Terminal identified as a CAT 1, CAT 2, or CAT 3 device and using MCC 5499 (Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores); and
- An unattended contactless-only POS Terminal (see Rule 4.7 for information about contactless-only acceptance).

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.

A contactless-only POS Terminal identified as a CAT 1, CAT 2, or CAT 3 device and using MCC 8398 (Organizations, Charitable and Social Service) offering a Transaction equal to or less than USD 15 (or local currency equivalent) may 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 CAT device prior to the Transaction being completed.

An in-flight POS Terminal identified as a CAT 4 device must provide a Transaction receipt, as described in Appendix D.

#### **At ATM and Bank Branch Terminals**

A receipt must be provided for a cash withdrawal or other financial Transaction occurring at an ATM or, if technically feasible, a Bank Branch Terminal. ATM cash withdrawals without receipts are allowed only when the device is out of paper, the Cardholder being duly advised.

**NOTE: A variation to this Rule provision appears in the “Europe Region” section at the end of this chapter.**

#### **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 may be sent to the Cardholder by email or other electronic means.

### **3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements**

All of the following information must be included on a Transaction receipt:

1. The “doing business as” (DBA) Merchant name, city, state/province, and country, or the financial institution location as provided in DE 43 (Card Acceptor Name/Location).
2. The Transaction type (retail sale, cash disbursement, refund).
3. The primary account number (PAN), in compliance with Rule 3.13.3. When an Access Device is presented, the Transaction receipt must display the PAN (in truncated form) for the Account accessed by means of that Contactless Payment Device, which may differ from the PAN on a Card linked to the same Account. If available, the truncated Card PAN may also be displayed for informational purposes.
4. A description and the price of each product and service purchased or returned, including applicable taxes, in detail sufficient to identify the Transaction.
5. The total Transaction amount and Transaction currency. If no currency is identified on the Transaction receipt, the Transaction is deemed to have taken place in the currency that is legal tender at the POI.



6. The Transaction date. (For Transaction date requirements, see Appendix C.)
7. For Card-present Mastercard POS Transactions completed with a manual imprinter, a legible imprint of the Card (unless the Card is unembossed).
8. The authorization approval code, if obtained from the Issuer. If multiple authorizations are obtained over the course of the Transaction (as may occur for lodging, cruise line, or vehicle rental Transactions), all authorization numbers, the amounts authorized, and the date of each authorization must be included.
9. For a Chip Transaction, the application identifier (AID) and the application preferred name or application label.
10. For face-to-face Mastercard unique Transactions and Mastercard Manual Cash Disbursement Transactions, with the exception of Card-read Transactions where a non-signature CVM is used or when successful Cardholder authentication on a Mastercard Biometric Card occurs, a description of the unexpired, official government document provided as identification by the Cardholder, including any serial number, expiration date, jurisdiction of issue, consumer name (if not the same name as present on the Card), and consumer address.
11. For signature-based Transactions occurring at a Merchant that chooses to perform or is required by applicable law or regulation to perform signature collection, adequate space for the Cardholder's signature on the Merchant's copy (and optionally on the Cardholder's copy).  
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 or no CVM is used. The Transaction receipt may optionally indicate that successful PIN or CDCVM verification has occurred.

If a receipt is produced following an unsuccessful Transaction attempt, the receipt must indicate the response or failure reason.

**NOTE: An addition to this Rule appears in the "Europe Region" section at the end of this chapter.**

### 3.13.2 ATM and Bank Branch Terminal Transaction Receipt Requirements

All of the following information must be included on a Transaction receipt:

1. Identification of the Acquirer (for example, the institution name or logotype).
2. The ATM or Bank Branch Terminal location.
3. The Transaction amount (in a dual currency environment, the Transaction currency must be identified on the receipt; in all other environments, the Transaction currency symbol is recommended).
4. The Transaction time and date.
5. The primary account number (PAN), in compliance with Rule 3.13.3. When an Access Device is presented, the Transaction receipt must display the PAN (in truncated form) for the Account accessed by means of that Contactless Payment Device, which may differ from the PAN on a Card linked to the same Account. If available, the truncated Card PAN may also be displayed for informational purposes.

6. The Transaction type (cash disbursement).
7. The Transaction sequence number.
8. An electronic recording of the magnetic stripe-read or chip-read Card data.
9. For a Chip Transaction, the application label and, at the Acquirer's discretion, the Transaction certificate (in its entirety) and related data.
10. For Merchandise Transactions only, a statement that the Transaction was for the purchase of products or services.

An ATM or Bank Branch Terminal must clearly describe, by receipt, screen information, or both, the action taken by the Issuer in response to a Cardholder's request (approved or rejected).

### 3.13.3 Primary Account Number (PAN) Truncation and Expiration Date Omission

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 Corporation 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.

**NOTE: Modifications to this Rule appear in the "Europe Region" section at the end of this chapter.**

### 3.13.4 Prohibited Information

The Transaction receipt or 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 validation code 2 (CVC 2).

### 3.13.5 Standard Wording for Formsets

A formset is a Transaction receipt produced by a manual imprinter. The following wording, in English, the local language, or both (or words to similar effect) should appear on the Cardholder copy of a formset:

"IMPORTANT—retain this copy for your records."

In addition, the following wording (or words to similar effect) should appear on each copy of a formset for the specified Transaction type.

**Retail Sale and Manual Cash Disbursement Transactions—**"The Issuer of the Card identified on this receipt is authorized to pay the amount shown as 'total' upon proper

presentation. I promise to pay such total (together with any other charges due thereon) subject to and in accordance with the agreement governing the use of such Card.”

**Refund Transactions—**“I request that the above Cardholder account be credited with the amount shown as ‘total’ because of the return of, or adjustments on, the goods, services, or other items of value described.”

## 3.14 Returned Products and Canceled Services

---

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 following applies:

- If a Mastercard Card was used, the Merchant may 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). A cash, check, or prepaid card refund is permitted for involuntary refunds by airlines or other Merchants when required by law.
- If a Maestro Card was used, a Merchant may offer a price adjustment by means of a credit, provided the credit is posted 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 (but be aware that if an Access Device was used, the PAN on a Card linked to the same Account may not match the PAN on the receipt). If the Card used to make the purchase is not available, or the Merchant’s refund Transaction authorization request is declined, the Merchant must act in accordance with its policy for adjustments, refunds, returns, or the like, which may include providing a cash, check, or prepaid card refund.

**NOTE: A modification to this Rule appears in the “Europe Region” section at the end of this chapter.**

### 3.14.1 Refund Transactions

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.

When the original purchase was...	Then the refund Transaction...
A Chip Transaction	<p>May be completed without Chip Card authentication, Cardholder verification (CVM), or online authorization from the Issuer. No Transaction cryptogram will be produced for a refund Transaction. Refer to the <i>M/Chip Requirements</i> manual for details.</p> <p>A Merchant may initiate an online authorization request for a refund Transaction occurring on or after 17 April 2020. Chip data is not required for an online-authorized refund Transaction.</p>
A dual message magnetic stripe Transaction	<p>May be completed without CVM or online authorization from the Issuer.</p> <p>A Merchant may initiate an online authorization request for a refund Transaction occurring on or after 17 April 2020. Magnetic stripe data is not required for an online-authorized refund Transaction.</p>
A single message magnetic stripe Transaction	<p>May be completed without CVM. In a Card-present environment, the Card must be read by the POS Terminal; in a Card-not-present environment, the Card data may be key-entered. Authorization is required; an Issuer must not decline the authorization request solely because no PIN was present in the authorization message.</p>

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 Cardholder must be provided a copy of the refund Transaction receipt containing:

- The date of the refund;
- A description of the returned products, canceled services, or adjustment made; and
- The amount of the refund.

**NOTE: Modifications to this Rule appear in the “Europe Region,” “Middle East/Africa Region,” and “Additional U.S. Region and U.S. Territory Rules” sections at the end of this chapter.**

## 3.15 Transaction Records

---

Each Transaction record must reflect a valid and accurate Transaction date, as defined in Appendix C. 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 Mastercard POS Transactions:

1. The Merchant must submit each purchase and refund 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 purchase Transaction records completed with manually recorded (imprinted or handwritten) Card data must submit such Transaction records to its Acquirer within 21 calendar days of the Transaction date.
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 Credit Not Processed chargeback.

Upon receiving the Transaction record, the Acquirer must present the Transaction within the applicable presentment timeframe in order to avoid a Late Presentment chargeback. A refund Transaction occurring on or after 17 April 2020 must be presented within five calendar days of the refund Transaction date. Refer to the *Chargeback Guide* and *GCMS Reference Manual* for more information.

### 3.15.1 Retention of Transaction Records

The Acquirer must retain a record of each Transaction it receives or sends for a minimum of 13 months, or such longer period as may be required by applicable law or regulation. During that period, the Acquirer must provide a copy of the Transaction receipt to the Issuer upon request.

## Variations and Additions by Region

---

The remainder of this chapter provides modifications to the Standards set out in this chapter. The modifications are organized by region or country and by applicable subject title.

### Asia/Pacific Region

---

The following modifications to the Rules apply in the Asia/Pacific Region or in a particular Region country or countries. Refer to Appendix A for the Asia/Pacific Region geographic listing.

## 3.14 Returned Products and Canceled Services

### 3.14.1 Refund Transactions

In Australia, the Rule on this subject is modified as follows.

When the original purchase Transaction includes a surcharge, the refund Transaction must include the full or prorated surcharge amount.

## Canada Region

---

## Europe Region

---

The following modifications to the Rules apply in the Europe Region or in a particular Region country or countries. Refer to Appendix A for the Europe Region, Non-Single European Payments Area (Non-SEPA) and Single European Payments Area (SEPA) geographic listing.

## 3.1 Card-Present Transactions

### 3.1.1 Mastercard Card Acceptance Procedures

#### Accepting a Mastercard Card

#### Suspicious Cards

In the EEA, the Rule on this subject is modified as follows.

A suspicious Card must be identified in the field of the authorization message and with the value specified by the registered switch of the Customer's choice.

## 3.2 Card-Not-Present Transactions

The following Rule variation applies with respect to Merchants located in the Europe Region.

A Merchant must not refuse to complete a Remote Electronic Transaction solely because the Issuer does not request Strong Customer Authentication (SCA), as Issuer exemptions from SCA may apply.

A Merchant must not refuse to complete a Remote Electronic Transaction solely because the Issuer does not support *SecureCode* or the Mastercard Identity Check Program, given that the Issuer may use alternative technical solutions for SCA.

The *SecureCode* liability shift applies equally to EMV 3DS as to 3DS 1.0.2. With regard to intra-EEA Transactions and Intracountry Transactions in the EEA, this liability shift applies when the Issuer approves an EMV 3DS authentication. Effective 18 October 2019, this liability shift applies also when the Merchant attempts an EMV 3DS authentication and the Issuer does not decline. Refer to the *Chargeback Guide* for more information on the *SecureCode* liability shift.

Before 18 October 2019, with regard to intra-EEA Transactions and Intracountry Transactions in the EEA, a Merchant may only use EMV 3DS if the Issuer BIN range is enrolled in EMV 3DS.

## **3.3 Obtaining an Authorization**

### **3.3.1 Mastercard POS Transaction Authorization Procedures**

In the EEA, Contactless transit aggregated and transit debt recovery Transactions and automated fuel dispenser (AFD) Transactions (MCC 5542) are not excluded from the requirement for a Merchant to inform the Cardholder of any estimated amount for which authorization will be requested and to obtain the Cardholder's consent to the amount before initiating the authorization request. As an example, a Merchant may comply with this information requirement by allowing the Cardholder to select the preauthorization amount at the Terminal or via a clearly readable sticker or other notice placed at the Point-of-Interaction (POI).

At an unattended POS Terminal, the Cardholder may express consent to the amount by continuing with the Transaction.

#### **Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions**

In the EEA, the Rule on this subject is modified as follows.

A partial approval must be identified in the field and with the value specified by the registered switch of the Customer's choice.

#### **Authorization When the Cardholder Adds a Gratuity**

In the EEA, the Rule on this subject is modified as follows.

A partial approval must be identified in the field and with the value specified by the registered switch of the Customer's choice.

### **3.3.2 Maestro POS Transaction Authorization Procedures**

In the Europe Region, the Rule on this subject is modified as follows.

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. This requirement does not apply to:

- Contactless transit aggregated Transactions and transit debt recovery Transactions,
- Automated fuel dispenser (AFD) Transactions (MCC 5542), or
- An authorization requested for an amount otherwise confirmed by the Cardholder to be the final Transaction amount.

In the EEA, the above Rule is modified as follows.

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 also for Contactless transit aggregated or transit debt recovery Transactions and for automated fuel dispenser (AFD) Transactions (MCC 5542). As an example, a Merchant may comply with this information requirement by allowing the

Cardholder to select the preauthorization amount at the Terminal or via a clearly readable sticker or other notice placed at the Point of Interaction.

At an unattended POS Terminal, the Cardholder may express consent to the amount by continuing with the Transaction.

To extend the duration of the reason code 4808 chargeback protection period afforded for each approved authorization, the Merchant may submit additional authorization requests for the same Transaction on later dates, as described in Rule 2.1.

An authorization is not required for a dual message Maestro refund Transaction until 17 April 2020.

### **3.5 Maestro Cardholder Verification Requirements**

In the Europe Region, the Rule on this subject is modified as follows.

The Cardholder must be verified by a PIN for each Contactless Transaction conducted in the Europe Region with a Card issued in the Europe Region that exceeds the applicable Contactless Transaction CVM limit amount.

### **3.8 POI Currency Conversion**

In the EEA, the Rule on this subject is modified as follows.

The currency chosen by the Cardholder and the pre-conversion currency and amount must be identified in the fields specified by the registered switch of the Customer's choice.

The POI currency conversion indicator must be populated in the field and with the value specified by the registered switch of the Customer's choice.

### **3.13 Providing a Transaction Receipt**

In the Europe Region, the first paragraph of the Rule on this subject, as it applies to ATM Terminals, is modified as follows.

For every completed Transaction, an ATM Terminal with receipt printing capability must make a receipt available to the Cardholder, either automatically or upon the Cardholder's request. A cash withdrawal without a printed receipt at an ATM Terminal is allowed only if the device is out of paper and the Cardholder is advised prior to the Transaction that a printed receipt is not available.

#### **3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements**

In the Europe Region, the Rule on this subject is modified as follows.

A Terminal may print the Transaction amount in the Transaction currency and a maximum of one different currency on the Transaction receipt.

The Transaction amount printed in a different currency must appear at the bottom of the receipt with a clear indication that it is being provided only for information purposes.



---

### 3.13.3 Primary Account Number (PAN) Truncation and Expiration Date Omission

In the **Netherlands**, the Rule on this subject is replaced with the following:

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 a maximum of four of the last seven digits of the PAN. All non-reflected digits of the PAN must be replaced with fill characters, such as "X," "\*", or "#."

The Corporation strongly recommends that if a POS Terminal generates a Merchant copy of the Transaction receipt, the Merchant copy should also reflect a maximum of four of the last seven digits of the PAN, replacing all non-reflected digits with fill characters that are neither blank spaces nor numeric characters, such as "X," "\*", or "#."

### 3.14 Returned Products and Canceled Services

For intra-European and inter-European Transactions, the Rule on this subject is modified as follows:

If a Merchant agrees to provide a refund or price adjustment, it may provide the refund or price adjustment by any means.

#### 3.14.1 Refund Transactions

For intra-European and inter-European Transactions, the Rule on this subject is modified as follows:

1. For each refund Transaction, a service fee is paid by the Issuer to the Acquirer. Such fee is independent of the interchange fee associated with the corresponding POS Transaction.
2. The refund Transaction may be used to return the unused gambling value to the Cardholder, up to the amount of the original purchase occurring on a Maestro Card. The Gaming Payment Transaction must be used to transfer gambling winnings to the Cardholder.
3. A refund of a Maestro Transaction may be processed to a Card as a MO/TO Transaction using manual key entry of the PAN and without reading the magnetic stripe or chip on the Card. An Issuer must technically support Maestro refund Transactions processed as MO/TO Transactions.
4. A Transaction printout must be generated for a refund Transaction, with the exception of a refund processed as a MO/TO Transaction.

---

## Latin America and the Caribbean Region

The following modifications to the Rules apply in the Latin America and the Caribbean Region. Refer to Appendix A for the Latin America and the Caribbean Region geographic listing.

### 3.5 Maestro Cardholder Verification Requirements

In the Latin America and the Caribbean Region, the Rule on this subject is modified as follows.

The Cardholder must be verified by a PIN for:

- Each Maestro Contactless Transaction conducted in Brazil, Chile, or Colombia with a Card issued in Brazil, Chile, or Colombia that exceeds the applicable Contactless Transaction CVM limit amount, and
- Each Maestro Magnetic Stripe Mode Contactless Transaction conducted in Brazil with a Card issued in Brazil that exceeds BRL 50. A CVM is not required for a Magnetic Stripe Mode Contactless Transaction that is less than or equal to BRL 50.

## Middle East/Africa Region

---

The following modifications to the Rules apply in the Middle East/Africa Region. Refer to Appendix A for the Middle East/Africa Region geographic listing.

### 3.14 Returned Products and Canceled Services

#### 3.14.1 Refund Transactions

In Angola, Botswana, Comoros, Democratic Republic of the Congo, Djibouti, Eritrea, Ethiopia, Ghana, Gambia, Lesotho, Liberia, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Nigeria, Rwanda, Seychelles, Sierra Leone, Somalia, South Sudan, Swaziland, Tanzania, Uganda, Zambia, and Zimbabwe, the Rule on this subject is modified as follows with respect to Maestro POS Transaction refunds:

The refund Transaction may be used to return the unused gambling value to the Cardholder, up to the amount of the original purchase occurring on a Maestro Card. The Gaming Payment Transaction must be used to transfer gambling winnings to the Cardholder.

## United States Region

---

The following modifications to the Rules apply in the United States (U.S.) Region. Refer to Appendix A for the U.S. Region geographic listing.

### 3.3 Obtaining an Authorization

#### 3.3.1 Mastercard POS Transaction Authorization Procedures Authorization When the Cardholder Adds a Gratuity

In the U.S. Region, the Rule on this subject is replaced with the following.

When a preauthorization or an undefined authorization is obtained:

- If the Transaction is a Chip/PIN Transaction, Contactless Transaction, Mastercard Consumer-Presented QR Transaction, or Card-not-present Transaction identified other than as

described below, any gratuity must be included in the authorization request. A gratuity must not be added to the authorized amount.

- If the Transaction is a Card-not-present Transaction identified with MCC 5812 (Eating Places, Restaurants) or MCC 5814 (Fast Food Restaurants), a gratuity may be added after authorization is obtained, as follows:
  - If the gratuity does not exceed 20 percent of the authorized amount, then no additional authorization is needed.
  - If the gratuity exceeds 20 percent of the authorized amount, then the Merchant may request an incremental authorization for the amount in excess of the authorized amount.
- For all other Transaction types, including signature-based magnetic stripe Transactions and Chip Transactions, a gratuity may be added after authorization is obtained, as follows:
  - If the gratuity does not exceed 20 percent of the authorized amount, then no additional authorization is needed.
  - If the gratuity exceeds 20 percent of the authorized amount, then the Merchant may request an incremental authorization for the amount in excess of the authorized amount.

For all Transactions, if the authorization request message contains the Partial Approval Terminal Support Indicator, and the authorization request response message contains a value of 10 (Partial Approval) in DE 39 and a partial approval amount in DE 6, the Transaction amount must not exceed the authorized amount.

The Issuer must not place a hold on the Cardholder's Account in excess of the total authorized amount or implied authorized amount (inclusive of the 20 percent tolerance, when applicable).

### 3.5 Maestro Cardholder Verification Requirements

In the U.S. Region, the Rule on this subject is modified as follows.

The Cardholder must be verified by a PIN for each Maestro Contactless Transaction that exceeds the applicable Contactless Transaction CVM limit amount.

No PIN is required when a POS Transaction is conducted as described in "PIN-less Single Message Transactions" in Chapter 4.

---

### Additional U.S. Region and U.S. Territory Rules

The following variations and additions to the Rules apply in the United States Region and in American Samoa, Guam, Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands (herein, "the U.S. Territories").

These Rules apply in addition to any that apply within the Asia/Pacific Region, with respect to Customers located in American Samoa, Guam, and Northern Mariana Islands; the Latin America and the Caribbean Region, with respect to Customers located in Puerto Rico and the U.S. Virgin Islands; and the United States Region, with respect to U.S. Region Customers.

## **3.14 Returned Products and Canceled Services**

### **3.14.1 Refund Transactions**

In the U.S. Region and U.S. Territories, the Rule on this subject is modified as follows.

The refund Transaction must include a full or prorated Brand-Level Surcharge or Product-Level Surcharge amount, as the terms Brand-Level Surcharge and Product-Level Surcharge are defined in Rule 5.11.2 of the *Mastercard Rules*, when the original purchase Transaction included a Brand-Level Surcharge or Product-Level Surcharge.

## Chapter 4 Card-Present Transactions

*The following Standards apply with regard to Transactions that occur in a Card-present environment, at attended or unattended Terminals. Where applicable, modifications by region and/or country are provided at the end of this chapter in the section titled, "Variations and Additions by Region."*

4.1 Chip Transactions at Hybrid Terminals.....	112
4.2 Offline Transactions Performed on Board Planes, Trains, and Ships.....	112
4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions—Europe Region Only.....	113
4.4 Contactless Transactions at POS Terminals.....	113
4.5 Contactless Transit Aggregated Transactions.....	114
4.5.1 Mastercard Contactless Transit Aggregated Transactions.....	114
4.5.2 Maestro Contactless Transit Aggregated Transactions.....	115
4.6 Contactless Transactions at ATM Terminals.....	115
4.7 Contactless-only Acceptance.....	116
4.8 Mastercard Consumer-Presented QR Transactions at POS Terminals.....	117
4.9 Quick Payment Service (QPS) Program—Mastercard POS Transactions Only.....	117
4.10 Purchase with Cash Back Transactions.....	118
4.11 Transactions at Unattended POS Terminals.....	119
4.11.1 Automated Fuel Dispenser Transactions.....	119
4.12 PIN-based Debit Transactions—United States Region Only.....	120
4.13 PIN-less Single Message Transactions—United States Region Only.....	120
4.14 Merchant-approved Maestro POS Transactions.....	120
4.15 Mastercard Manual Cash Disbursement Transactions.....	121
4.15.1 Non-discrimination Regarding Cash Disbursement Services.....	121
4.15.2 Maximum Cash Disbursement Amounts.....	121
4.15.3 Discount or Service Charges.....	122
4.15.4 Mastercard Acceptance Mark Must Be Displayed.....	122
4.16 Encashment of Mastercard Travelers Cheques.....	122
4.17 ATM Transactions.....	122
4.17.1 "Chained" Transactions.....	123
4.17.2 ATM Transaction Branding.....	123
4.18 ATM Access Fees.....	123
4.18.1 ATM Access Fees—Domestic Transactions.....	123
4.18.2 ATM Access Fees—Cross-border Transactions.....	123
4.18.3 ATM Access Fee Requirements.....	123

Transaction Field Specifications for ATM Access Fees.....	124
Non-discrimination Regarding ATM Access Fees.....	124
Notification of ATM Access Fee.....	124
Cancellation of Transaction.....	124
Sponsor Approval of Proposed Signage, Screen Display, and Receipt.....	124
ATM Terminal Signage.....	124
ATM Terminal Screen Display.....	125
ATM Transaction Receipts.....	125
4.19 Merchandise Transactions at ATM Terminals.....	126
4.19.1 Approved Merchandise Categories.....	126
4.19.2 Screen Display Requirement for Merchandise Categories.....	127
4.20 Shared Deposits—United States Region Only.....	127
Variations and Additions by Region.....	127
Asia/Pacific Region.....	127
4.10 Purchase with Cash Back Transactions.....	127
4.11 Transactions at Unattended POS Terminals.....	127
4.11.1 Automated Fuel Dispenser Transactions.....	127
4.18 ATM Access Fees.....	128
4.18.1 ATM Access Fees—Domestic Transactions.....	128
Canada Region.....	128
4.10 Purchase with Cash Back Transactions.....	128
4.11 Transactions at Unattended POS Terminals.....	129
4.11.1 Automated Fuel Dispenser Transactions.....	129
4.18 ATM Access Fees.....	129
4.18.1 ATM Access Fees—Domestic Transactions.....	129
Europe Region.....	129
4.1 Chip Transactions at Hybrid Terminals.....	129
4.2 Offline Transactions Performed on Board Planes, Trains, and Ships.....	129
4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions.....	129
4.4 Contactless Transactions at POS Terminals.....	130
4.5 Contactless Transit Aggregated Transactions.....	131
4.5.1 Mastercard Contactless Transit Aggregated Transactions.....	131
4.5.2 Maestro Contactless Transit Aggregated Transactions.....	131
4.10 Purchase with Cash Back Transactions.....	132
4.11 Transactions at Unattended POS Terminals.....	134
4.11.1 Automated Fuel Dispenser Transactions.....	135
4.14 Merchant-approved Maestro POS Transactions.....	136
4.15 Mastercard Manual Cash Disbursement Transactions.....	136
4.15.2 Maximum Cash Disbursement Amounts.....	136

---

4.18 ATM Access Fees.....	136
4.18.1 ATM Access Fees—Domestic Transactions.....	136
4.19 Merchandise Transactions at ATM Terminals.....	137
4.19.1 Approved Merchandise Categories.....	137
Latin America and the Caribbean Region.....	137
4.4 Contactless Transactions at POS Terminals.....	137
4.5 Contactless Transit Aggregated Transactions.....	137
4.5.2 Maestro Contactless Transit Aggregated Transactions.....	137
4.10 Purchase with Cash Back Transactions.....	138
4.18 ATM Access Fees.....	139
4.18.1 ATM Access Fees—Domestic Transactions.....	139
Middle East/Africa Region.....	140
4.10 Purchase with Cash Back Transactions.....	140
United States Region.....	141
4.1 Chip Transactions at Hybrid Terminals.....	141
4.10 Purchase with Cash Back Transactions.....	141
4.11 Transactions at Unattended POS Terminals.....	141
4.11.1 Automated Fuel Dispenser Transactions.....	142
4.12 PIN-based Debit Transactions.....	142
4.13 PIN-less Single Message Transactions.....	142
4.15 Mastercard Manual Cash Disbursement Transactions.....	143
4.15.2 Maximum Cash Disbursement Amounts.....	143
4.15.3 Discount or Service Charges.....	143
4.18 ATM Access Fees.....	144
4.18.1 ATM Access Fees—Domestic Transactions.....	144
4.19 Merchandise Transactions at ATM Terminals.....	144
4.19.1 Approved Merchandise Categories.....	144
4.20 Shared Deposits.....	144
4.20.1 Non-discrimination Regarding Shared Deposits.....	144
4.20.2 Terminal Signs and Notices.....	144
4.20.3 Maximum Shared Deposit Amount.....	144
4.20.4 Deposit Verification.....	144
4.20.5 ATM Terminal Clearing and Deposit Processing.....	145
4.20.6 Shared Deposits in Excess of USD 10,000.....	146
4.20.7 Notice of Return.....	146
4.20.8 Liability for Shared Deposits.....	146

## 4.1 Chip Transactions at Hybrid Terminals

---

A Customer must comply with the Standards set forth in the *MI/Chip Requirements* manual, as modified from time to time, when deploying Hybrid Terminals and processing Chip Transactions. For information about chip-related incentive interchange rates, see the applicable regional *Interchange Manual*.

A Chip Transaction must occur at a Hybrid Terminal and be authorized by the Issuer or the chip, resulting in the generation of a unique Transaction Certificate (TC). The Acquirer must send the EMV chip data in DE 55 (Integrated Circuit Card [ICC] System-Related Data) of the Authorization Request/0100 or Financial Transaction Request/0200 message and in DE 55 of the First Presentment/1240 message. A value of 2 or 6 must also be present in position 1 of the three-digit service code in DE 35 (Track 2 Data) of the Authorization Request/0100 or Financial Transaction/0200 message.

As used in this Rule, the following terms have the meanings described:

- “PIN-capable Hybrid POS Terminal” means a Hybrid POS Terminal that is capable at a minimum of performing offline PIN verification when a PIN-preferring Chip Card is presented. It may also be capable of online PIN verification and if attended, must accept signature.
- “PIN-preferring Chip Card” means a Chip Card that has been personalized so that the offline PIN CVM option appears in the Card’s CVM list with a higher priority than the signature option, indicating that PIN is preferred to signature at any POS Terminal that supports PIN.

A chip/PIN Transaction is a Chip Transaction that is processed at a PIN-capable Hybrid POS Terminal with a PIN-preferring Chip Card and completed with offline or online PIN as the CVM. The Cardholder may retain control of the Card while a chip/PIN Transaction is performed.

A non-face-to-face Chip Transaction processed using a Cardholder-controlled remote device is permitted if the Acquirer has received an Application Authentication Cryptogram (AAC) and the Issuer’s approval of the Merchant’s authorization request.

For information about counterfeit and lost/stolen/never-received-issue chip liability shifts, see the *Chargeback Guide*.

**NOTE: Modifications to this Rule appear in the “Europe Region” and “United States Region” sections at the end of this chapter.**

## 4.2 Offline Transactions Performed on Board Planes, Trains, and Ships

---

A Customer may process a Chip Transaction that takes place at the offline-only Hybrid POS Terminal of a Merchant with no fixed location (for example, aboard a plane, train or ship), if all the following conditions are satisfied:



1. The Hybrid POS Terminal has no online capability and does not perform fallback procedures from chip to magnetic stripe.
2. The Hybrid POS Terminal prompted for PIN as the CVM and the EMV chip provided offline verification of the PIN entered by the Cardholder.
3. The Hybrid POS Terminal recommended Transaction approval. If the Hybrid POS Terminal recommends against Transaction approval based on its own risk parameters, the Transaction must not proceed.
4. If a **Mastercard Card** was presented, the Card declined the offline authorization request. The Acquirer processes such declined Transactions at the risk of receiving authorization-related chargebacks. If a **Maestro Card** was presented, the Merchant processed the Transaction offline as a Merchant-approved Maestro POS Transaction.
5. The Merchant is identified with one of the following MCCs:
  - a. MCC 4111 (Transportation—Suburban and Local Commuter Passenger, including Ferries)
  - b. MCC 4112 (Passenger Railways)
  - c. MCC 5309 (Duty Free Stores)
6. If applicable, the Acquirer provides in the First Presentment/1240 message:
  - a. The value of F (Offline Chip) in DE 22 (Point of Service Entry Mode), subfield 7 (Card Data Input Mode).
  - b. The Application Authentication Cryptogram (AAC) in DE 55.

**NOTE: Modifications to this Rule appear in the “Europe Region” section at the end of this chapter.**

## 4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions—Europe Region Only

**NOTE: A Rule on this subject appears in the “Europe Region” section at the end of this chapter.**

## 4.4 Contactless Transactions at POS Terminals

When a Contactless Transaction is conducted at a POS Terminal in an amount that does not exceed the applicable Contactless Transaction CVM limit amount, as defined by Merchant location in Appendix E:

- The Transaction must be completed without Cardholder verification (“No CVM” as the CVM); and
- The provision of a Transaction receipt to the Cardholder is at the Merchant’s option. The Merchant must provide a receipt at the Cardholder’s request.

As an exception to the above, a CVM must be obtained for any purchase with cash back or quasi-cash Transaction completed by means of contactless payment functionality.

As an exception to the above, a contactless-only POS Terminal identified as a CAT 1, CAT 2, or CAT 3 device and using MCC 8398 (Organizations, Charitable and Social Service) offering a Transaction equal to or less than USD 15 (or local currency equivalent) may 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 CAT device prior to the Transaction being completed.

There is no maximum Transaction amount for a Contactless Transaction conducted at a POS Terminal.

For CVM requirements, see Rules 3.4, 3.5, and 3.7. For Contactless Transaction identification requirements, see Appendix C.

**NOTE: Modifications to this Rule appear in the “Europe Region” and “Latin America and the Caribbean Region” sections at the end of this chapter. Refer to “CVC 3 Verification” in the “Latin America and the Caribbean Region” section for a related Rule.**

## 4.5 Contactless Transit Aggregated Transactions

---

A Contactless transit aggregated Transaction must not exceed the applicable Contactless transit aggregated Transaction limit, as defined in Appendix E.

### 4.5.1 Mastercard Contactless Transit Aggregated Transactions

Mastercard Contactless transit Transactions are permitted only in connection with specific MCCs and can be pre-funded, real-time authorized, aggregated, or for debt recovery.

A Mastercard Contactless transit aggregated Transaction occurs when the transit Merchant's Acquirer generates a First Presentment/1240 message combining one or more contactless taps performed with one Mastercard Account at one transit Merchant. A “tap” means the Cardholder's tap of the Card or Contactless Payment Device on the contactless reader of the POS Terminal with each ride taken. In order for the transit Merchant to receive chargeback protection, all of the following must occur:

1. The Merchant must send a properly identified Authorization Request/0100 message (which can be for any amount).
2. The Issuer must approve the Transaction.
3. The combined amount of the taps must be equal to or less than the applicable chargeback protection amount.
4. The maximum time period from the first tap until the First Presentment/1240 message is generated must be 14 calendar days or less.

Upon the Cardholder's request, the Merchant must provide a list of the taps (the date and fare for each ride taken) that were combined into a First Presentment/1240 message.

For Mastercard Contactless transit aggregated Transaction identification requirements, see Appendix C.

**NOTE: Modifications to this Rule appear in the “Europe Region” section at the end of this chapter.**

#### 4.5.2 Maestro Contactless Transit Aggregated Transactions

A Maestro Contactless transit aggregated Transaction occurs when the Acquirer generates a Financial Transaction Request/0200 message for an estimated or maximum amount in connection with the use of one Maestro Account at one transit Merchant. A Maestro Contactless transit aggregated Transaction must be processed as follows:

1. The Merchant sends a Financial Transaction Request/0200 message with a value of 06 in DE 48, subelement 64, subfield 1 (Transit Transaction Type Indicator) for an estimated or maximum amount not to exceed the applicable Contactless transit aggregated Transaction ceiling limit amount.
2. The Issuer must approve the Transaction.
3. The Cardholder may make subsequent taps for additional rides; these taps will not be sent to the Issuer for authorization. The combined amount of the taps must be equal to or less than the applicable Contactless transit aggregated Transaction ceiling limit amount.
4. When the limit is reached or within three calendar days, the Merchant totals the value of all taps and generates an Acquirer Reversal Advice/0420 to reverse any unused funds.

The Merchant must inform the Cardholder that the amount held from the available funds in the Account may be greater than the cost of a single fare, and the Merchant must inform the Cardholder of the amount of time that the Merchant requires to reverse all unused funds. This information may be provided on the Merchant's Website, included in call center scripts, and/or displayed within the transit Merchant's system. The Merchant must also provide specific tap information to the Cardholder upon request.

For Maestro Contactless transit aggregated Transaction identification requirements, refer to Appendix C.

**NOTE: Variations to this Rule appear in the “Europe Region” and “Latin America and the Caribbean Region” sections at the end of this chapter.**

#### 4.6 Contactless Transactions at ATM Terminals

---

A Contactless Transaction conducted at an ATM Terminal must always use online PIN as the CVM.

There is no maximum Transaction amount for a Contactless Transaction occurring at an ATM Terminal.

## 4.7 Contactless-only Acceptance

---

When approved by Mastercard (either on a country-by-country or case-by-case basis), an Acquirer may sponsor Merchants that deploy POS Terminals or MPOS Terminals that utilize only contactless payment functionality. In such event, the Acquirer must ensure that, should any of its Merchants approved by Mastercard to deploy POS Terminals or MPOS Terminals that utilize only contactless payment functionality subsequently deploy POS Terminals or MPOS Terminals with contact payment functionality, such POS Terminals and MPOS Terminals accept and properly process Transactions.

Mastercard has approved the following for contactless-only acceptance:

1. Merchants that deploy unattended POS Terminals that are identified as Cardholder-activated Terminals (CATs), including but not limited to vending machines, parking meters, and fare collection devices.
2. Subject to Corporation approval on a case-by-case basis, Merchants operating mass events, festivals, and sports arenas located in Hungary, Poland, Romania, and the United Kingdom under the following MCCs:
  - a. MCC 7941—Athletic Fields, Commercial Sports, Professional Sports Clubs, Sports Promoters
  - b. MCC 7929—Bands, Orchestras, and Miscellaneous Entertainers not elsewhere classified
  - c. MCC 5811—Caterers
  - d. MCC 7922—Theatrical Producers (except Motion Pictures), Ticket Agencies
  - e. MCC 7999—Recreational Services—not elsewhere classified
3. Merchants located in Hungary, Poland and Romania that use MCC 5994—News Dealers and Newsstands.
4. Merchants located in Hungary that use MCC 5462—Bakeries or MCC 5441—Candy, Nut, Confectionery Stores.
5. Merchants that use MCC 8398—Organizations, Charitable and Social Service.

Unattended POS Terminals that utilize only contactless payment functionality are not required to provide a 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. 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). The manner in which to request a receipt must be clearly displayed at the Merchant location.

As an exception to the above, a contactless-only POS Terminal identified as a CAT 1, CAT 2, or CAT 3 device and using MCC 8398 (Organizations, Charitable and Social Service) offering a Transaction equal to or less than USD 15 (or local currency equivalent) may 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 CAT device prior to the Transaction being completed.

For requirements related to the identification of Contactless-only Transactions occurring at an unattended POS Terminal, see Appendix C. For CAT identification requirements, see Appendix D.

## 4.8 Mastercard Consumer-Presented QR Transactions at POS Terminals

---

A Mastercard Consumer-Presented QR Transaction is effected through a Cardholder-presented QR Code and by the Merchant capture of the QR Code containing the Transaction Data required to initiate a Transaction. For each Mastercard Consumer-Presented QR Transaction:

- There is no maximum Transaction amount.
- The Transaction must be authorized online by the Issuer.
- The Acquirer must send a properly identified Authorization Request/0100 message or Financial Transaction Request /0200 message.
- The Transaction must be completed with CDCVM. CDCVM is the only valid CVM for Mastercard Consumer-Presented QR Transactions.

For more information about Mastercard Consumer-Presented QR Transactions, refer to the Mastercard Cloud-Based Payments (MCBP) documentation and the *MI/Chip Requirements for Contact and Contactless* manual.

## 4.9 Quick Payment Service (QPS) Program—Mastercard POS Transactions Only

---

A Quick Payment Service (QPS) Transaction is a magnetic stripe-based or contact chip-based face-to-face Mastercard POS Transaction approved by the Issuer that occurs at a Merchant in an eligible Merchant category and for an amount equal to or less than the applicable QPS Transaction CVM limit amount, as defined by Merchant location in Appendix E. For each QPS Transaction:

- “No CVM” replaces signature as the Cardholder Verification Method (CVM); and
- The automatic provision of a Transaction receipt to the Cardholder is at the Merchant’s option. The Merchant must provide a receipt at the Cardholder’s request.

All Merchants using attended POS Terminals are eligible to participate in the QPS program, except those identified with any of the following MCCs:

- 4829—Money Transfer
- 6010—Manual Cash Disbursements—Customer Financial Institution
- 6050—Quasi Cash—Customer Financial Institution
- 6051—Quasi Cash—Merchant
- 6540—POI Funding Transactions
- 7802—Government Licensed Horse/Dog Racing
- 7995—Gambling Transactions

- 9405—Intra-Government Purchases—Government Only

The QPS program does not apply to Transactions conducted at unattended POS Terminals or in a Card-not-present environment.

The QPS program does not impact CVM requirements. A Hybrid POS Terminal must prompt for PIN when a PIN-preferring Chip Card is presented.

## 4.10 Purchase with Cash Back Transactions

---

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. A purchase with cash back Transaction is a Transaction arising from the use of a Debit Mastercard Card (but not any other type of Mastercard Card) or a Maestro Card.
2. 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.
3. 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.
4. 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.
5. 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. For Debit Mastercard purchase with cash back Transactions, a maximum cash back amount must be established that does not exceed USD 100 or the local currency equivalent.
  - e. For Maestro signature-verified and cross-border purchase with cash back Transactions, a maximum cash back amount must be established that does not exceed USD 100 or the local currency equivalent. Maestro signature-verified purchase with cash back Transactions may be conducted in signature waiver countries only.
6. The Acquirer must obtain online authorization approval for the full Transaction amount; support for authorization of the purchase amount only is optional.
7. The authorization and clearing messages of each purchase with cash back Transaction must comply with the following requirements:

- a. The Transaction must be identified with a value of 09 (purchase with cash back) in DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type).
- b. The purchase amount, cash back amount, and total Transaction amount must be in the same currency.
- c. The total Transaction amount (inclusive of the purchase and cash back amounts) must be transmitted in DE 4 (Amount, Transaction).
- d. The cash back amount must be transmitted in DE 54 (Amounts, Additional).

**NOTE: Variations to this Rule appear in the “Asia/Pacific Region,” “Canada Region,” “Europe Region,” “Latin America and the Caribbean Region,” “Middle East/Africa Region,” and “United States Region” sections at the end of this chapter.**

## 4.11 Transactions at Unattended POS Terminals

---

A POS Transaction occurring at an unattended POS Terminal is a non-face-to-face Transaction, since no Merchant representative is present at the time of the Transaction. Examples of unattended POS Terminals include ticket dispensing machines, vending machines, automated fuel dispensers, toll booths, and parking meters.

A Mastercard POS Transaction that occurs at an unattended POS Terminal must be identified as a Cardholder-Activated Terminal (CAT) Transaction, as described in Appendix D.

Transaction messages used at unattended POS Terminals must communicate to the Cardholder, at a minimum, the following:

- Invalid Transaction
- Unable to Route
- Invalid PIN—re-enter (if PIN entry is supported)
- Capture Card (if Card retention is supported)

**NOTE: Modifications to this Rule appear in the “Europe Region” section at the end of this chapter.**

### 4.11.1 Automated Fuel Dispenser Transactions

An automated fuel dispenser Transaction is identified with MCC 5542 (Automated Fuel Dispenser) and a CAT level indicator of CAT 1, CAT 2, or CAT 6.

Refer to Appendix C regarding the identification of electronic commerce Transactions occurring at automated fuel dispensers.

Refer to Appendix D for Cardholder-Activated Terminal requirements.

**NOTE: Rules on this subject appear in the “Asia/Pacific Region” (pertaining to Malaysia), “Canada Region,” “Europe Region,” and “United States Region” sections at the end of this chapter.**

## 4.12 PIN-based Debit Transactions—United States Region Only

---

**NOTE:** A Rule on this subject appears in the “United States Region” section at the end of this chapter.

## 4.13 PIN-less Single Message Transactions—United States Region Only

---

**NOTE:** A Rule on this subject appears in the “United States Region” section at the end of this chapter.

## 4.14 Merchant-approved Maestro POS Transactions

---

This Rule applies to all Merchant-approved Maestro POS Transactions whether processed via the Mastercard® Single Message System or the Mastercard® Dual Message System. Refer to Chapter 3 of the *MI/Chip Requirements* for more detailed information on processing Merchant-approved Maestro POS Transactions that are Chip Transactions.

An Acquirer may elect to accept Merchant-approved Maestro POS Transactions from a Merchant that accepts Maestro Cards. A Merchant-approved Maestro POS Transaction may occur only when the POS Terminal cannot receive an online authorization for a Transaction because of technical difficulties between the Acquirer and the Interchange System or the Interchange System and the Issuer, or other temporary technical problems. Each Acquirer must forward all stored Transactions by means of electronic store-and-forward as soon as the technical problem has been resolved.

The Issuer must treat all Merchant-approved Maestro POS Transactions received by means of the Mastercard® Single Message System as financial request messages. If the Issuer is unavailable to authorize or decline a Merchant-approved Maestro POS Transaction at the time of presentment, the Interchange System indicates this, and returns the Transaction to the Acquirer. These returned Transactions may be submitted by the Acquirer to the Interchange System every 30 minutes, until a response is received from, or on behalf of the Issuer.

Merchant-approved Maestro POS Transactions settle only upon authorization by the Issuer. The Acquirer bears all responsibility for a Merchant-approved Maestro POS Transaction that is declined by the Issuer.

If a Merchant-approved POS Transaction is declined by the Issuer for insufficient funds, or because the Transaction exceeds withdrawal limits, the Acquirer may resubmit the Transaction once every 24 hours for a period ending 13 calendar days after the Transaction date. If the Issuer accepts the Transaction on submission or resubmission, the Issuer's liability is the same as for an online Transaction.



An Issuer is not required to assist an Acquirer in any attempt to collect on a systemically rejected Merchant-approved POS Transaction. The Issuer must make reasonable efforts to collect the Transaction amount, but in doing so, assumes no liability.

**NOTE: A variation to this rule appears in the “Europe Region” section at the end of this chapter.**

## 4.15 Mastercard Manual Cash Disbursement Transactions

---

A cash disbursement may be provided to a Mastercard Cardholder by a Customer at its offices and through its authorized agents. For purposes of this Rule, an authorized agent is a financial institution authorized to provide cash disbursement services on behalf of a Customer pursuant to written agreement with the Customer.

The Customer and each of its authorized cash disbursement agents must comply with the requirements set forth in “Mastercard Manual Cash Disbursement Acceptance Procedures” in Chapter 3.

A cash disbursement to a Maestro or Cirrus Cardholder is performed at a Bank Branch Terminal. Refer to Chapter 7 for Bank Branch Terminal requirements.

**NOTE: An addition to this Rule appears in the “United States Region” section at the end of this chapter.**

### 4.15.1 Non-discrimination Regarding Cash Disbursement Services

Each Customer 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.

### 4.15.2 Maximum Cash Disbursement Amounts

A Customer and each of its authorized cash disbursement agents may limit the amount of cash provided to any one Cardholder in one day at any individual office. Such limit may not be less than USD 5,000 per Cardholder in one day and uniformly must be applied 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 Customer may establish a maximum cash disbursement amount of less than USD 5,000 per person in one day at each such office, provided that the maximum cash disbursement amount:

1. Is not less than USD 1,000;

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 Customer can, if requested by Mastercard, demonstrate that a higher maximum would create a hardship.

**NOTE: Variations to this Rule appear in the “Europe Region” and “United States Region” sections at the end of this chapter.**

#### **4.15.3 Discount or Service Charges**

The Customer and each of its authorized cash disbursement agents must disburse all cash disbursements at par without any discount and without any service or other charge to the Cardholder, except as may be imposed to comply with applicable law. Any charge imposed to comply with applicable law must be charged to and paid by the Cardholder separately and must not be included in the total amount of the cash disbursement.

**NOTE: A modification to this Rule appears in the “United States Region” section at the end of this chapter.**

#### **4.15.4 Mastercard Acceptance Mark Must Be Displayed**

A Customer and each of its authorized cash disbursement agents must display the Mastercard Acceptance Mark as required by the Standards at each location where the Customer or any such agent provides cash disbursements to Mastercard Cardholders.

### **4.16 Encashment of Mastercard Travelers Cheques**

---

Each Mastercard Customer must encash Mastercard® Travelers Cheques issued in any currency when presented for payment at any of its locations, provided:

1. Such encashment is permitted by law; and
2. The Customer has the ability (including a foreign exchange capability, with respect to a currency other than U.S. currency Mastercard Travelers Cheques presented for encashment) to encash such cheques as a result of the business it normally conducts at a location. If the encashing Customer encashes any other brand of travelers cheques at a location, the Customer may impose terms and conditions for the encashment of Mastercard Travelers Cheques that it uses to encash other brands of travelers cheques.

### **4.17 ATM Transactions**

---

The following Rules relate to ATM Transaction processing.

#### 4.17.1 “Chained” Transactions

An Acquirer that deploys ATM Terminals that do not retain the Card internally until all Transactions requested by the Cardholder are completed must require the Cardholder to re-enter the PIN for every additional financial Transaction performed. This requirement applies to card swipe readers, card dip readers, and similar devices where a card is not held within the device, and is removed prior to Transaction completion.

#### 4.17.2 ATM Transaction Branding

If a Customer that does not have a Mastercard License acquires an ATM transaction initiated by a Mastercard Card that does not display the Maestro and/or Cirrus Marks and sends it through the Mastercard® ATM Network, that transaction is deemed to be an ATM Transaction and all Rules regarding ATM Transactions will apply.

### 4.18 ATM Access Fees

---

An ATM Access Fee may be charged by an Acquirer only in connection with a cash withdrawal Transaction or a Shared Deposit Transaction that is initiated at the Acquirer’s ATM Terminal with a Card. The ATM Access Fee is added to the amount of the Transaction transmitted to the Issuer.

For purposes of this Rule, a Transaction is any Transaction routed through the Mastercard® ATM Network. Nothing contained in this Rule affects the right of an Issuer to determine what fees, if any, to charge its Cardholders.

#### 4.18.1 ATM Access Fees—Domestic Transactions

A Cardholder may not be assessed or be required to pay an ATM Access Fee or other fee types imposed, or advised of, at an ATM, in connection with a Domestic Transaction.

**NOTE: Variations to this Rule appear in the “Asia/Pacific Region” (pertaining to Australia), “Canada Region,” “Europe Region,” “Latin America and the Caribbean Region,” and “United States Region” sections at the end of this chapter.**

#### 4.18.2 ATM Access Fees—Cross-border Transactions

Unless prohibited by local law or regulations, an Acquirer, upon complying with the ATM Access Fee notification requirements, may assess an ATM Access Fee on a Cross-border Transaction, so long as the Acquirer applies the ATM Access Fee in a consistent and nondiscriminatory manner.

#### 4.18.3 ATM Access Fee Requirements

An Acquirer that applies or plans to apply an ATM Access Fee to Domestic Transactions, Cross-border Transactions, or both must comply with all of the following requirements.

## **Transaction Field Specifications for ATM Access Fees**

At the time of each Transaction on which an ATM Access Fee is imposed, the Acquirer of such Transaction must transmit, in the field specified by the applicable technical specifications manual or other applicable technical specifications manual then in effect, the amount of the ATM Access Fee separately from the amount of the cash disbursed in connection with such 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 Terminal.

### **Notification of ATM Access Fee**

An Acquirer that wishes to charge an ATM Access Fee must notify its Sponsoring Principal, in writing, of its intent to do so prior to the planned first imposition of such ATM Access Fee by the Acquirer.

The Principal must update the Location Administration Tool (LAT) regarding its or its Affiliates' imposition of ATM Access Fees.

### **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.

### **Sponsor Approval of Proposed Signage, Screen Display, and Receipt**

An Affiliate that plans to charge an ATM Access Fee to a Transaction must submit proposed ATM Terminal signage, screen display, and receipt "copy" that meets the requirements of the Rules to its Sponsor in writing for approval prior to use, unless such Acquirer employs the model form provided in Appendix F.

The Sponsor has the right to determine the acceptability of any new or changes to previously approved signage, screen display, and receipt copy. In cases of conflict between the Acquirer and its Sponsor, Mastercard has the sole right to determine the acceptability of any and all signage, screen display, and receipt copy.

### **ATM Terminal Signage**

An Acquirer that plans to charge an ATM Access Fee may optionally display signage that is clearly visible to Cardholders on or near all Terminals at which ATM Access Fees apply.

The minimum requirement for ATM Access Fee signage text is wording that clearly states:

1. The identity of the ATM owner and of the Principal;
2. That the Transaction will be subject to an ATM Access Fee that will be deducted from the Cardholder's Account in addition to any Issuer fees;

3. The amount of, calculation method of, or Corporation-approved generic signage regarding the ATM Access Fee;
4. That the ATM Access Fee is assessed by the Acquirer instead of the Issuer;
5. That the ATM Access Fee is assessed on Cross-border Transactions only or Domestic Transactions only, if applicable.

The minimum requirements for ATM Terminal signage (physical characteristics) are as follows:

1. The signage must bear the heading "Fee Notice";
2. The size of the signage must be a minimum of four inches in height by four inches in width;
3. The text must be clearly visible to all; a minimum of 14-point type is recommended;
4. The heading must be clearly visible to all; a minimum of 18-point type is recommended.

Refer to Appendix F for a model of ATM Terminal signage relating to ATM Access Fee application.

### **ATM Terminal 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 ATM Terminals 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.

If an Acquirer displays the Mastercard-approved generic ATM Access Fee signage, the Acquirer must include the amount or calculation method of the ATM Access Fee as part of the ATM Terminal screen display.

Refer to Appendix F for a model of an ATM Terminal screen display relating to ATM Access Fee application.

### **ATM Transaction Receipts**

Any 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.

Refer to Appendix F for a model of ATM Transaction receipt text relating to ATM Access Fee application.

---

## 4.19 Merchandise Transactions at ATM Terminals

---

An ATM Terminal may dispense any merchandise, service, or other thing of value within a Mastercard-approved merchandise category, other than any merchandise, service, or other thing of value which:

1. Is illegal or would tend to offend the public morality or sensibility, disparage Mastercard, or otherwise compromise the good will or name of Mastercard;
2. Mastercard has notified Acquirers must not be dispensed by an ATM Terminal; or
3. Could be used to obtain products or services at a location other than an ATM Terminal which, if dispensed at an ATM Terminal, would be prohibited pursuant to this Rule.

Promptly upon written direction from Mastercard, an Acquirer must cease dispensing at all its ATM Terminals any merchandise, service, or other thing of value which Mastercard has directed is not permitted.

### 4.19.1 Approved Merchandise Categories

Approved merchandise categories are as follows.

Merchandise Category	Explanation
Event Tickets	Admission tickets to scheduled events that upon presentation of such tickets will admit the bearer to such scheduled events in lieu of other forms of admission tickets.
Transportation Tickets and Passes	Tickets or passes to board and ride scheduled transportation conveyances in lieu of other forms of transportation tickets.
Telecommunications Cards and Services	Prepaid telephone cards that entitle the holder to a specified amount of prepaid time or prepaid wireless telephone time that is credited to a subscriber's prepaid telephone account.
Retail Mall Gift Certificates	Gift certificates to be sold at ATM Terminals located in retail shopping malls and redeemable for merchandise at stores located in the mall where dispensed. Customers must receive prior written approval from the Corporation for each specific mall implementation.
Charitable Donation Vouchers	Pre-valued donation vouchers that are dispensed as receipts for donations resulting from an authorized Transaction at a participating ATM. Customers must receive prior written approval from the Corporation for each specific charitable entity.

**NOTE: An addition to this Rule appears in the “Europe Region” and the “United States Region” sections at the end of this chapter.**

#### 4.19.2 Screen Display Requirement for Merchandise Categories

The Acquirer must disclose to the Cardholder via the video monitor screen prior to the initiation of any Merchandise Transaction the following:

1. Full identification of the price and quantity of the Merchandise;
2. Any additional shipping or handling charges (for mailed purchases only);
3. Policy on refunds or returns; and
4. Provision for recourse concerning Cardholder complaints or questions.

#### 4.20 Shared Deposits—United States Region Only

---

**NOTE: Rules on this subject appear in the “United States Region” section at the end of this chapter.**

### Variations and Additions by Region

---

The remainder of this chapter provides modifications to the Standards set out in this chapter. The modifications are organized by region or country and by applicable subject title.

#### Asia/Pacific Region

---

The following modifications to the Rules apply in the Asia/Pacific Region or in a particular Region country or countries. Refer to Appendix A for the Asia/Pacific Region geographic listing.

#### 4.10 Purchase with Cash Back Transactions

In **India**, the Rule on this subject is modified as follows:

A Merchant located in India that has received prior approval from its Acquirer may offer a purchase with cash back Transaction with or without an accompanying purchase to a Cardholder presenting a Debit Mastercard or Maestro Card issued in India.

The maximum daily cash back amount per Card must be in accordance with applicable law including circulars published by the Reserve Bank of India.

#### 4.11 Transactions at Unattended POS Terminals

##### 4.11.1 Automated Fuel Dispenser Transactions

In **Malaysia**, the following Rule applies:

A Malaysia Acquirer must present Mastercard automated fuel dispenser Transactions (MCC 5542) to Malaysia Issuers within two business days of the Transaction date.

Within one business day of the presentment date of an automated fuel dispenser Transaction (MCC 5542), a Malaysia Issuer must post the Transaction to the Cardholder's account and release any hold amount exceeding the Transaction amount from the Cardholder's Account.

## **4.18 ATM Access Fees**

### **4.18.1 ATM Access Fees—Domestic Transactions**

The Rule on this subject, as it applies to Domestic Transactions occurring in Australia, is replaced with the following:

Subject to complying with the ATM Access Fee notification requirements, an Acquirer in Australia may assess an ATM Access Fee on a Debit Mastercard, Maestro, or Cirrus Transaction initiated with a Card that was issued in Australia provided the Acquirer applies the ATM Access Fee in a consistent and nondiscriminatory manner.

For the purpose of this Rule, "ATM Access Fee" means a fee charged by an Acquirer in Australia in connection with a financial or non-financial transaction initiated at that Acquirer's ATM Terminal with a Card issued in Australia, which fee is added to the amount of the Transaction transmitted to the Issuer.

## **Canada Region**

---

The following modifications to the Rules apply in the Canada Region. Refer to Appendix A for the Canada Region geographic listing.

### **4.10 Purchase with Cash Back Transactions**

In the Canada Region, the Rule on this subject is modified as follows.

A Customer must technically support the purchase with cash back Transaction for Debit Mastercard and prepaid Mastercard Cards.

A Merchant located in the Canada Region may, at its option, support purchase with cash back Transactions as set forth in this chapter, with the following variations:

1. The Merchant may offer purchase with cash back to Debit Mastercard and prepaid Mastercard Cardholders.
2. Purchase with cash back is available only for chip/PIN Transactions.
3. The maximum cash back amount of the purchase with cash back Transaction is CAD 100. Acquirers or Merchants may establish a lower maximum cash back amount, provided that:
  - a. Any such maximum amount is applied uniformly; and
  - b. Any maximum amount is not lower than the maximum amount established for any other payment means on which purchase with cash back is offered at the Merchant location.



## **4.11 Transactions at Unattended POS Terminals**

### **4.11.1 Automated Fuel Dispenser Transactions**

In the Canada Region, if an Issuer approves an online authorization request for an automated fuel dispenser (MCC 5542) Transaction, then within 60 minutes of the time that the authorization request message is sent, the Acquirer must send an authorization advice message advising the Issuer of the Transaction amount.

If, after approving the authorization request, the Issuer places a hold on Cardholder funds in excess of CAD 1, then, within 60 minutes of receiving the Acquirer's authorization advice message, the Issuer must release any hold amount that exceeds the Transaction amount.

## **4.18 ATM Access Fees**

### **4.18.1 ATM Access Fees—Domestic Transactions**

In the Canada Region, the Rule on this subject is replaced with the following:

Subject to complying with the ATM Access Fee notification requirements of the Rules, an Acquirer in the Canada Region may assess an ATM Access Fee on a Transaction initiated with a Card that was issued in the Canada Region provided the Acquirer applies the ATM Access Fee in a consistent and nondiscriminatory manner.

## **Europe Region**

---

The following modifications to the Rules apply in the Europe Region or in a particular Region country or countries. Refer to Appendix A for the Europe Region, Non-Single European Payments Area (Non-SEPA) and Single European Payments Area (SEPA) geographic listing.

### **4.1 Chip Transactions at Hybrid Terminals**

In the EEA, the Rule on this subject is modified as follows.

EMV chip data must be provided in the field specified by the registered switch of the Customer's choice for authorization and clearing messages.

### **4.2 Offline Transactions Performed on Board Planes, Trains, and Ships**

In the EEA, the Rule on this subject is modified as follows.

Decline of the authorization by the EMV chip must be indicated in the field and with the value specified by the registered switch of the Customer's choice.

### **4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions**

In the Europe Region, magnetic stripe and Contact Chip Maestro POS Transactions may be completed without CVM in the acceptance environments listed in this Rule, up to the maximum Transaction amount set out below.

Acceptance Environment	Maximum Transaction Amount
Tollways (MCC 4784)	EUR 100 (or local currency equivalent)
Parking Lots and Garages (MCC 7523)	EUR 50 (or local currency equivalent)
Transit Vending Machines (MCCs 4111, 4112 and 4131)	EUR 25 (or local currency equivalent)

Maestro Contactless Transactions may also be completed in these environments in accordance with the Standards applicable to Maestro Contactless Transactions.

The following Rules apply to Magnetic Stripe and Contact Chip Maestro POS Transactions:

1. The Merchant must obtain authorization online from the Issuer or offline from the chip. Magnetic stripe Transactions may also be authorized according to the Merchant-approved Transaction Rules, at POS Terminals that are not located in the EEA. At POS Terminals located in the EEA, effective 14 September 2019, magnetic stripe Transactions must not be completed.
2. The Acquirer bears the liability for fraud on magnetic stripe and Contact Chip Maestro POS Transactions completed without CVM.
3. The Transactions must be identified with one of the above-listed MCCs.
4. Transactions at vending machines and transit vending machines must be identified as unattended Transactions.
5. A POS Terminal at which no-CVM Maestro POS Transactions are performed may have a PIN pad.
6. An Issuer of Chip Cards must be able to authorize no-CVM Maestro POS Transactions even when the chip data in the authorization message indicates "Cardholder verification was not successful."
7. In the tollways environment, the Merchant may at its option maintain a negative file in the POS Terminal, provided this is done in a PCI-compliant manner.
8. An Issuer in the Netherlands is not required to technically support no-CVM Maestro POS Transactions at transit vending machines. Transit vending machines that support no-CVM Maestro POS Transactions must not be deployed in the Netherlands.

#### 4.4 Contactless Transactions at POS Terminals

In the Europe Region, the Rule on this subject is modified as follows.

Merchants that operate tollways (MCC 4784) and parking lots and garages (MCC 7523) may configure their POS Terminals to perform Maestro Contactless Transactions that exceed the applicable CVM limit without a CVM.

An Issuer must not systematically decline such Maestro Contactless Transactions when completed without a CVM.

The Acquirer is liable for a fraudulent Maestro Contactless Transaction that exceeds the CVM Limit and is completed without a CVM.

If a Maestro Card that also bears a domestic debit brand mark is used in a Contactless Transaction and the domestic debit brand does not support contactless payment functionality, the Transaction must be identified in all Transaction messages as a Maestro Contactless Transaction and all Rules regarding such Transactions apply to the Transaction. If processed by means of the Interchange System, the Maestro Contactless Transaction is identified by the following values, which indicate that an EMV Mode Contactless Transaction has occurred:

1. In authorization:
  - a. DE 22 (POS entry mode), subfield 1 (POS Terminal PAN Entry Mode) must contain the value of 7, and
  - b. DE 61 (POS Data), subfield 11 (POS Card Data Terminal Input Capability) must contain the value of 3.
2. In clearing:
  - a. DE 22 (POS entry mode), subfield 1 (Terminal Data: Card Data Input Capability) must contain the value of M, and
  - b. DE 22 (POS data), subfield 7 (Card Data: Input Mode) must contain the value of M.

If the Transaction is processed via a means other than the Interchange System (including bilateral and on-us processing), the Acquirer must ensure that corresponding data elements contain values that enable Issuers to clearly identify the transaction as a Maestro Contactless Transaction.

## **4.5 Contactless Transit Aggregated Transactions**

### **4.5.1 Mastercard Contactless Transit Aggregated Transactions**

In the EEA, the Rule on this subject is modified as follows.

A clearing message must be identified as specified by the registered switch of the Customer's choice.

### **4.5.2 Maestro Contactless Transit Aggregated Transactions**

In the Europe Region, the Rule on this subject is replaced with the following.

A Maestro Contactless transit aggregated Transaction occurs when the Acquirer generates an Authorization Request/0100 message for an estimated amount in connection with the use of one Maestro Account at one transit Merchant. Maestro Contactless transit aggregated Transactions must be processed as follows.

1. The Merchant sends an Authorization Request/0100 message with a value of 06 in DE 48, subelement 64, subfield 1 (Transit Transaction Type Indicator) for an estimated amount not to exceed the applicable Contactless transit Transaction ceiling limit amount.
2. The Merchant must obtain Issuer approval of the Transaction.

3. The Cardholder may make subsequent taps for additional rides; these taps will not be sent to the Issuer for authorization. The combined amount of the taps must be equal to or less than the Contactless transit aggregated Transaction limit amount.
4. When the limit is reached or within three calendar days, the Merchant totals the value of all taps and generates a Reversal Request/0400 or Authorization Advice/0120 message to reverse any unused funds.

The Merchant must inform the Cardholder that the amount held from the available funds in the Account may be greater than the cost of a single fare, and the Merchant must inform the Cardholder of the amount of time that the Merchant takes to reverse all unused funds. This information may be provided on the Merchant's Website, included in call center scripts, and/or displayed within the transit Merchant's system. The Merchant must also provide specific tap information to the Cardholder upon request.

For Contactless transit aggregated Transaction identification requirements, refer to Appendix C.

In the EEA, the Rule on this subject is modified as follows.

Maestro Contactless transit aggregated Transactions must be identified as specified by the registered switch of the Customer's choice.

Authorization, reversal and advice messages must be identified as specified by the registered switch of the Customer's choice.

#### **4.10 Purchase with Cash Back Transactions**

In the Europe Region, the Rule on this subject is modified as follows.

A Merchant located in the Europe Region may, at its option, support purchase with cash back Transactions on all types of Mastercard Cards. A Merchant must offer purchase with cash back Transactions on all Europe Region-issued Debit Mastercard and Maestro Cards if the Merchant offers this transaction type on any other debit brand.

An Acquirer in Romania must technically support purchase with cash back Mastercard and Maestro Transactions in its host system and on the attended POS Terminals of its Merchants.

An Acquirer in Ukraine that supports purchase with cash back Transactions must technically support purchase-only approval in its host and at all participating POS Terminals.

The following requirements apply to purchase with cash back Transactions on Mastercard Cards:

1. Purchase with cash back on Mastercard Cards is not available for paper-based, key-entered, or magnetic stripe Transactions. It is available for all other types of Mastercard Transactions.
2. If a Merchant provides purchase with cash back only upon presentation of particular Cards, then the Merchant must not promote the service at the POI location or prompt the Cardholder to use purchase with cash back.
3. For Mastercard Cards, the maximum cash back amount of the purchase with cash back Transaction is GBP 100 in the United Kingdom and EUR 100 or the local currency

equivalent in other Europe Region countries, with the exception of Germany, where the maximum is EUR 200, Russia, where the maximum is RUB 5,000, and Ukraine, where the maximum is UAH 500. An Acquirer or Merchant may establish a lower maximum cash back amount, provided that:

- a. Any such maximum amount is applied uniformly; and
- b. Any maximum amount is not lower than the maximum amount established for any other payment means on which purchase with cash back is offered at the Merchant location.

The following Rules apply to Intracountry Transactions under all brands in the country mentioned.

1. For Intracountry Transactions in **Poland**, the maximum cash back amount is PLN 500. An Issuer in Poland must not apply a cash back limit lower than PLN 500. An Acquirer in Poland must support purchase with cash back and must not apply a cash back limit lower than PLN 500. A Merchant in Poland that offers purchase with cash back must not apply a cash back limit lower than PLN 500.
2. Intracountry Transactions in **Russia** must be authorized with online PIN for the full amount, including both the purchase and cash-back amounts. An Issuer in Russia must not apply a cash back limit lower than RUB 5,000. A Merchant located in Russia that provides purchase with cash back service must be duly signed up by its Acquirer as a bank payment agent in accordance with the local legislation.
3. For Intracountry Maestro and Debit Mastercard Transactions in **Italy**, the maximum cash back amount is EUR 100, regardless of the CVM used (for example, PIN, CDCVM, signature).
4. Intracountry Transactions in **Ukraine** must be authorized with online PIN for the full amount, including both the purchase and cash-back amounts. The maximum cash back amount is UAH 500. An Issuer in Ukraine must not apply a cash back limit lower than UAH 500. Purchase with cash back Transactions must be processed in UAH only; POI currency conversion must not be offered.
5. Intracountry Transactions in **Switzerland** must be authorized with online PIN or Consumer Device Cardholder Verification Method (CDCVM) for the full amount, including both the purchase and cash back amounts. The purchase amount, cash back amount, and Transaction amount must all be in the same currency. The cash back amount must not be higher than CHF 300 or lower than CHF 10. An Issuer must decline the Transaction if the cash back amount exceeds CHF 300. The purchase amount of a purchase with cash back Transaction must not be lower than CHF 20.
6. Intracountry Transactions in **Germany** must be authorized with online PIN or offline PIN for Contact Chip Transactions and online PIN or CDCVM for Contactless Transactions.

The following requirements apply to Issuers:

1. An Issuer must technically support purchase with cash back Transactions on Debit Mastercard and Maestro Cards. The Issuer must make individual authorization decisions and must not automatically decline authorization of purchase with cash back Transactions on Debit Mastercard and Maestro Cards.

In addition, an Issuer must support purchase with cash back Transactions on Mastercard Cards issued under a BIN or BIN range assigned for the following countries:

Country	Mandate applies to Mastercard Cards issued or reissued on or after	With the exception of the following types of Cards
Germany	1 January 2017	Prepaid Mastercard Cards
Romania	1 September 2017	No exceptions
Russia	1 January 2020	No exceptions
Ukraine	1 January 2020	No exceptions

Issuers in Russia must technically support purchase with cash back functionality in their host systems.

Issuers in Ukraine must technically support purchase with cash back functionality in their host systems. Effective 1 January 2020, newly issued and reissued Cards and MDES Tokens must have the purchase with cash back flag. Effective 1 January 2022, all Cards and MDES tokens in circulation in Ukraine must have the purchase with cash back flag.

2. An Issuer that intends to support purchase with cash back Transactions for its Mastercard Cardholders must properly personalize the chip on its Mastercard Cards.
3. An Issuer that supports partial approval authorizations for magnetic stripe Transactions may use partial approval to authorize only the purchase amount. Partial approval must not be used to authorize only the cash back amount.

In the EEA, the Rule on this subject is modified as follows.

A purchase with cash back Transaction must be identified in authorization and clearing messages as specified by the registered switch of the Customer's choice. The Transaction amount and cash back amount must be identified in the fields and with the values specified by the registered switch of the Customer's choice.

## 4.11 Transactions at Unattended POS Terminals

In the EEA, the Rule on this subject is modified as follows.

Effective 14 September 2019, a CAT Level 2 Terminal supporting contact Transactions, that does not operate in a transport or parking environment (MCCs 4111, 4112, 4131, 4784, 4789, and 7523) must:

- Be upgraded to have dual capability by the addition of an offline PIN-capable PIN pad, or
- Be upgraded to become a CAT Level 1 Terminal by the addition of an online PIN-capable PIN pad, or
- Have contact chip functionality removed, resulting in contactless-only acceptance, or
- Be removed from deployment.

Effective 14 September 2019, a CAT Level 3 Terminal supporting contact Transactions, that does not operate in a transport or parking environment (MCCs 4784 and 7523) must:

- Be upgraded with the addition of an offline PIN-capable PIN pad, or
- Have contact chip functionality removed, resulting in contactless-only acceptance, or
- Be removed from deployment.

Effective 14 September 2019, a CAT Level 4 Terminal supporting contact Transactions must:

- Be upgraded with the addition of an offline PIN-capable PIN pad, or
- Have contact chip functionality removed, resulting in contactless-only acceptance, or
- Be removed from deployment.

CAT Transactions must be identified in authorization and clearing messages as specified by the registered switch of the Customer's choice.

References in Appendix D to Acquirer MIP X-Code processing are replaced by references to corresponding authorization services of the registered switch of the Issuer's choice.

#### **4.11.1 Automated Fuel Dispenser Transactions**

In the Europe Region, the Acquirer of a Merchant having an unattended POS Terminal at a petrol station (MCC 5542) must process POS Transactions as follows.

1. The Acquirer must submit a preauthorization message containing the maximum amount determined by the Acquirer or Merchant.
2. The Issuer's authorization response may be for the full amount of the preauthorization or for a lesser amount determined by the Issuer. Approval of a lesser amount is referred to as partial amount preauthorization. The Transaction is guaranteed up to the amount authorized by the Issuer.
3. The Acquirer must inform the Issuer of the final Transaction amount via an advice message, which must be sent to the Issuer within 20 minutes of the authorization response message.
4. The Issuer must send an advice acknowledgement upon receipt of the advice message. Issuers must be able to receive advice messages and return advice acknowledgements in the preauthorization environment.
5. The Issuer must post the Transaction to the Cardholder's Account on the basis of the advice message, rather than the preauthorization response.

Support for partial amount preauthorization (as defined in item 2 above) is mandatory for Issuers and Acquirers of Maestro Cards if the Customer supports partial amount preauthorization for any other debit brand. Support of partial amount preauthorization is also required for all Mastercard Account ranges if the Customer supports partial amount preauthorization for Maestro or any other debit brand.

The First Presentment/1240 message must contain the final Transaction amount in DE 4.

In the EEA, the Rule on this subject is modified as follows.

The final Transaction amount must be provided in clearing messages, in the field and with the value specified by the registered switch of the Customer's choice.

## 4.14 Merchant-approved Maestro POS Transactions

In the EEA, the Rule on this subject is modified as follows.

References to the Interchange System are replaced with references to the registered switch of the Customer's choice.

In Belgium, the Rule on this subject is modified as follows.

For Domestic Transactions in Belgium, the Acquirer may resubmit the Transaction once every 24 hours for a period ending 30 calendar days after the Transaction date, if a Merchant-approved Maestro POS Transaction is declined by the Issuer for insufficient funds, or because the Transaction exceeds withdrawal limits.

## 4.15 Mastercard Manual Cash Disbursement Transactions

### 4.15.2 Maximum Cash Disbursement Amounts

In the Europe Region, the Rule on this subject is modified as follows.

The maximum cash disbursement amounts of USD 5,000 and USD 1,000 therein stated are replaced by EUR 5,000 and EUR 1,000, respectively.

## 4.18 ATM Access Fees

### 4.18.1 ATM Access Fees—Domestic Transactions

In the Europe Region, the Rule on this subject, as it applies to Domestic Transactions in the countries listed below, is replaced with the following:

Subject to complying with the ATM Access Fee notification requirements, an Acquirer may assess an ATM Access Fee on a Domestic Transaction, provided the Acquirer applies the ATM Access Fee in a consistent and nondiscriminatory manner. The ATM Access Fee may vary according to the Card category (credit, debit, prepaid, commercial), on condition that corresponding cards of other brands accepted at that ATM Terminal attract an equal or higher ATM Access Fee. The ATM Access Fee must be properly populated in Transaction messages.

“ATM Access Fee” means a fee charged by an Acquirer in connection with a financial ATM Transaction and added to the Transaction amount that is transmitted to the Issuer. An Acquirer must not assess an ATM Access Fee on a non-financial (anything other than cash withdrawal) Transaction.

Austria (Maestro and Cirrus Transactions only)

Germany

Greece

Iceland

Spain

United Kingdom (Debit Card Transactions only)



The Acquirer does not receive a Service fee in connection with an intra-European or inter-European Transaction on which an ATM Access Fee has been charged.

## 4.19 Merchandise Transactions at ATM Terminals

### 4.19.1 Approved Merchandise Categories

In the Europe Region, the Rule on this subject is modified as follows.

Merchandise Category	Explanation
Mobile Phone Top Up	The purchase of a specified amount of prepaid wireless telephone time, to be credited to the mobile SIM card associated with the subscriber's prepaid telephone account. The Transaction is identified with MCC 4814.
Bill Payment	Payment via the ATM of utility, telephone or other bills. The Transaction may be identified with MCC 4900 or MCC 6050.

## Latin America and the Caribbean Region

The following modifications to the Rules apply in the Latin America and the Caribbean Region. Refer to Appendix A for the Latin America and the Caribbean Region geographic listing.

### 4.4 Contactless Transactions at POS Terminals

In the Latin America and the Caribbean Region, the Rule on this subject, as it applies in **Brazil**, is modified as follows.

If the Cardholder selects the "debit" option when using a Mastercard Card issued in Brazil to initiate a Contactless Transaction at a Merchant located in Brazil, Mastercard® Single Message System processing requirements and the chargeback procedures in Chapter 4 of the *Chargeback Guide* will apply. The resulting Transaction is referred to as a Maestro Magnetic Stripe Mode Contactless Transaction.

### 4.5 Contactless Transit Aggregated Transactions

#### 4.5.2 Maestro Contactless Transit Aggregated Transactions

In the Latin America and the Caribbean Region, the Rule on this subject is modified as follows.

In **Mexico**, when the limit is reached or within two calendar days, the Merchant totals the value of all taps and generates an Acquirer Reversal Advice/0420 message to reverse any unused funds.

---

Specific Maestro Contactless transit aggregated Transaction ceiling limits apply in the Bolivarian Republic of Venezuela, Colombia, and Mexico.

#### 4.10 Purchase with Cash Back Transactions

In **Argentina**, the Rule on this subject is modified as follows with respect to Domestic Transactions:

For purchase with cash back Transactions **with** or **without** an accompanying purchase, a Merchant may accept Maestro Cards, Debit Mastercard, and Prepaid Mastercard Cards.

The following requirements apply to purchase with cash back Transactions:

1. The Acquirer must obtain online authorization approval for the entire Transaction amount; partial approval is not permitted.
2. A surcharge must not be applied to the Transaction by the Merchant or the Acquirer.
3. Installment billing of the Transaction must not be offered to the Cardholder.
4. All Transactions must be authenticated either by signature or PIN, according to the technology enabled on the Card.
5. When cash is provided **with** an accompanying purchase, the total Transaction amount in DE 4 (Amount, Transaction) must be greater than the cash back amount in DE 54 (Additional Amounts), subfield 5 (Amount).
6. When cash is provided **without** an accompanying purchase, the total Transaction amount in DE 4 (Amount, Transaction) must be equal to the cash back amount in DE 54 (Additional Amounts), subfield 5 (Amount).
7. Acquirers must not offer purchase with cash back Transactions with or without an accompanying purchase to Cards issued outside the country.
8. Purchase with cash back Transactions with or without an accompanying purchase are not available for Mastercard® credit card products.

In **Brazil**, the Rule on this subject is modified as follows with respect to Domestic Transactions.

A Merchant may offer the purchase with cash back service on the following Card types:

- For purchase with cash back Transactions with an accompanying purchase, a Merchant may accept Maestro Cards, Mastercard débito, Debit Mastercard and prepaid Mastercard Cards enabled for Mastercard Single Message System processing.
- For purchase with cash back Transactions without an accompanying purchase, a Merchant may accept Maestro Cards, Mastercard débito, Debit Mastercard and prepaid Mastercard Cards enabled for either Mastercard Dual Message System or Mastercard Single Message System processing.
- Issuers and Acquirers must not support Purchase with Cash Back Transactions for the following Card types:
  - MBF Mastercard® Alimentação (Food)
  - MBM Mastercard® Refeição (Meal)
  - MLE Mastercard® Pedágio Prepaid Card
  - MLF Mastercard® Agro (available only in Brazil)

The following requirements apply to purchase with cash back Transactions:

1. The Acquirer must obtain online authorization approval for the entire Transaction amount. Partial approval is not permitted.
2. A surcharge must not be applied to the Transaction by the Merchant or the Acquirer.
3. Installment billing of the Transaction must not be offered to the Cardholder.
4. All Transactions must be PIN-verified.
5. When cash is provided **with** an accompanying purchase, the total Transaction amount in DE 4 (Amount, Transaction) must be greater than the cash back amount in DE 54 (Additional Amounts), subfield 5 (Amount).
6. When cash is provided **without** an accompanying purchase, the total Transaction amount in DE 4 (Amount, Transaction) must be equal to the cash back amount in DE 54 (Additional Amounts), subfield 5 (Amount).

In **Uruguay**, the Rule on this subject is modified as follows with respect to Domestic Transactions:

For purchase with cash back Transactions **with** an accompanying purchase, a Merchant may accept Maestro Cards, Debit Mastercard, and Prepaid Mastercard Cards.

The following requirements apply to purchase with cash back Transactions:

1. The Acquirer must obtain online authorization approval for the entire Transaction amount; partial approval is not permitted.
2. A surcharge must not be applied to the Transaction by the Merchant or the Acquirer.
3. Installment billing of the Transaction must not be offered to the Cardholder.
4. All Transactions must be authenticated either by signature or PIN, according to the technology enabled on the Card.
5. For Mastercard purchase with cash back Transactions authenticated by signature or PIN, a maximum cash back amount of USD 60 or local currency equivalent is established.
6. When cash is provided with an accompanying purchase, the total Transaction amount in DE 4 (Amount, Transaction) must be greater than the cash back amount in DE 54 (Additional Amounts), subfield 5 (Amount).
7. Acquirers must not offer purchase with cash back Transactions to Cards issued outside the country.
8. Purchase with cash back Transactions are not available for Mastercard® credit card products.

## 4.18 ATM Access Fees

### 4.18.1 ATM Access Fees—Domestic Transactions

In the Latin America and the Caribbean Region, the Rule on this subject, as it applies to Domestic Transactions occurring in the countries listed below, is replaced with the following:

Subject to complying with the ATM Access Fee notification requirements, the Acquirer may assess an ATM Access Fee on a Domestic Transaction provided the Acquirer applies the ATM Access Fee in a consistent and nondiscriminatory manner.

For the purposes of this Rule, “ATM Access Fee” means a fee charged by an Acquirer in connection with any financial Transaction initiated at that Acquirer’s ATM with a Card and added to the amount of the Transaction transmitted to the Issuer.

Argentina	Brazil
Chile	Colombia
Ecuador	Mexico
Panama	Peru
Puerto Rico	Venezuela

## Middle East/Africa Region

The following modifications to the Rules apply in the Middle East/Africa Region. Refer to Appendix A for the Middle East/Africa Region geographic listing.

### 4.10 Purchase with Cash Back Transactions

In **Kenya**, the Rule on this subject is modified as follows:

A Merchant located in Kenya that has received prior approval from its Acquirer may offer a purchase with cash back Transaction with or without an accompanying purchase to any Cardholder presenting a Mastercard Card, Prepaid Mastercard Card, Debit Mastercard Card, or Maestro Card issued in Kenya.

For purchase with cash back Transactions, a maximum cash back amount must be established that does not exceed KES 100,000.

PIN verification must be obtained for each purchase with cash back Transaction without an accompanying purchase.

In **South Africa**, the Rule on this subject is modified as follows:

A Merchant located in South Africa that has received prior approval from its Acquirer may offer a purchase with cash back Transaction with or without an accompanying purchase to any Cardholder presenting a Mastercard, Debit Mastercard, or Maestro Card issued in South Africa.

PIN verification must be obtained for each purchase with cash back Transaction without an accompanying purchase.

## United States Region

---

The following modifications to the Rules apply in the United States (U.S.) Region. Refer to Appendix A for the U.S. Region geographic listing.

### 4.1 Chip Transactions at Hybrid Terminals

The Rule on this subject is modified as follows:

- “PIN-capable Hybrid POS Terminal” means a Hybrid POS Terminal capable of performing both online and offline PIN verification when a PIN-preferring Chip Card is presented, and which, if attended, also accepts signature.
- “PIN-preferring Chip Card” means a Chip Card that has been personalized so that a PIN CVM option (online PIN or offline PIN) appears in the Card’s CVM list with a higher priority than the signature option, indicating that PIN is preferred to signature at any POS Terminal that supports the same PIN CVM option.

Technical fallback occurs when a Chip Card is presented at a Hybrid Terminal but due to the failure of Chip Transaction processing, the Transaction is completed using the magnetic stripe or manual key entry of the PAN. The ratio of technical fallback Transactions to all Transactions completed at Hybrid Terminals at a particular Merchant location or at an ATM Terminal for a calendar month must not exceed five percent of all Chip Card Transactions at that Merchant location or ATM Terminal. An Acquirer with a Merchant that has exceeded the Standard set forth in the preceding sentence may be subject to noncompliance assessments.

### 4.10 Purchase with Cash Back Transactions

In the U.S. Region, the Rule on this subject is modified as follows.

1. A Merchant may charge a fee on the cash back portion of a Transaction. The fee charged by the Merchant must be:
  - a. The same or less than the fee charged for a cash back transaction for all other payment networks.
  - b. Disclosed to the Cardholder before completion of the Transaction.
  - c. Detailed in DE 28 (Amount, Transaction Fee) of the Authorization Request/0100 message or Financial Transaction Request/0200.
  - d. Detailed in DE 54 (Amounts, Additional) of the First Presentment/1240 message.
  - e. Included in the total Transaction amount transmitted in DE 4 (Amount, Transaction) of authorization and clearing messages.
2. A purchase with cash back Transaction must not be conducted as a PIN-less Single Message Transaction.

### 4.11 Transactions at Unattended POS Terminals

#### 4.11.1 Automated Fuel Dispenser Transactions

In the U.S. Region, if an Issuer approves an online authorization request for an automated fuel dispenser (MCC 5542) Transaction, then within 60 minutes of the time that the authorization request message is sent, the Acquirer must send an authorization advice message advising the Issuer of the Transaction amount.

If after approving the authorization request, the Issuer places a hold on Cardholder funds in excess of USD 1, then within 60 minutes of receiving the Acquirer's authorization advice message, the Issuer must release any hold amount that exceeds the Transaction amount specified.

An automated fuel dispenser Merchant identified by the Corporation to be an Excessive Chargeback Merchant (ECM) must use the Mastercard Address Verification Service (AVS) to verify the Cardholder's ZIP code before completing a Cardholder-Activated Terminal (CAT) Level 2 Transaction. For information about ECM criteria, refer to section 8.3, "Excessive Chargeback Program," of the *Security Rules and Procedures*. For information about ECM requirements to use AVS, refer to United States Region section, Rule 5.10.4 of the *Mastercard Rules* manual.

#### 4.12 PIN-based Debit Transactions

In the U.S. Region, a Customer may choose to acquire Transactions effected with Debit Mastercard Cards where PIN is used as the Cardholder verification method (CVM).

#### 4.13 PIN-less Single Message Transactions

In the U.S. Region, a PIN-less Single Message Transaction is a Transaction where the Cardholder is not required to be verified by PIN or other CVM if all of the following conditions exist:

- The Card is issued in the U.S. Region; and
- The Card has an IIN/BIN that begins with a four; and
- The Transaction is initiated by means of a POS Terminal located in the U.S. Region; and
- The Transaction amount is equal to or less than USD 50; and
- The Corporation assigned indicator in DE 48, subelement 81 in Financial Request/0200 message is present, indicating that the Transaction qualifies as PIN-less Single Message; and
- The Transaction is a magnetic stripe or Magnetic Stripe Mode Contactless Transaction; and
- The Transaction type cannot be performed at an unattended POS Terminal.

A Customer must process Maestro POS Transactions that are magnetic stripe or Magnetic Stripe Mode Contactless Transactions as PIN-less Single Message Transactions, as provided below:

1. No CVM is required.
2. An Acquirer must be able to route a PIN-less Single Message Transaction to the Issuer for approval.

3. An Acquirer must only route a PIN-less Single Message Transaction when the final purchase Transaction amount is certain at the time of authorization. Therefore, the Acquirer must evaluate each specific MCC for PIN-less Single Message Transactions.
4. An Issuer must authorize the PIN-less Single Message Transaction when the data in the authorization message includes the Mastercard-assigned PIN-less indicator in DE 48, at a substantially equivalent rate compared to other similar programs. An Issuer may not charge back a PIN-less Single Message Transaction for reason of fraud.

## **4.15 Mastercard Manual Cash Disbursement Transactions**

In the U.S. Region, the Rule on this subject is modified as follows:

Subject to compliance with the Standards, each Customer within the United States Region must provide cash disbursement services to all Cardholders at all of the Customer's offices where teller services are provided.

### **4.15.2 Maximum Cash Disbursement Amounts**

In the U.S. Region, the Rule on this subject is replaced with the following:

A Customer and each of its authorized cash disbursement agents may limit the amount of cash provided to any one Cardholder in one day at any individual office. Any such limit must be uniformly applied to all Cardholders of the same Card type. With respect to prepaid Cards, the limit must not be less than USD 5,000 per Cardholder in one day. With respect to all other Card types, the limit must not be less than USD 1,000 per Cardholder in one day.

### **4.15.3 Discount or Service Charges**

In the U.S. Region, the Rule on this subject is replaced with the following:

With respect to the acceptance of prepaid Cards, the Customer and each of its authorized cash disbursement agents must disburse all cash disbursements at par without any discount and without any service or other charge to the Cardholder, except as may be imposed to comply with applicable law. Any charge imposed to comply with applicable law must be charged to and paid by the Cardholder separately and must not be included in the total amount of the cash disbursement.

With respect to the acceptance of any type of Mastercard Card other than a prepaid Card, a Customer or its authorized cash disbursement agent may charge a fee for performance of the cash disbursement service (herein, a "Manual Cash Disbursement Access Fee"). Any Manual Cash Disbursement Access Fee charged must be:

1. Not greater than the fee established for any other payment network.
2. Disclosed to the Cardholder before a Transaction authorization request is submitted. At the time of disclosure, the Cardholder must be afforded the opportunity to opt out of completing the Transaction.
3. Disclosed on the Transaction receipt.
4. Detailed in DE 28 (Amount, Transaction Fee) of the Authorization Request/0100 or Financial Transaction Request/0200 message.
5. Detailed in DE 54 (Amounts, Additional) of the First Presentment/1240 message.

6. Included in the total Transaction amount transmitted in DE 4 (Amount, Transaction) of authorization and clearing messages.

## **4.18 ATM Access Fees**

### **4.18.1 ATM Access Fees—Domestic Transactions**

In the U.S. Region, the Rule on this subject is replaced with the following:

In all states and territories of the United States and in the District of Columbia, upon complying with the ATM Access Fee notification requirements of the Rules, an Acquirer may assess an ATM Access Fee on a Domestic Transaction.

## **4.19 Merchandise Transactions at ATM Terminals**

### **4.19.1 Approved Merchandise Categories**

In the U.S. Region, the Rule on this subject is modified to add postage stamps issued by the U.S. Postal Service as an approved merchandise category.

## **4.20 Shared Deposits**

In the U.S. Region, an Acquirer may choose to participate in the Shared Deposit service; provided, if the Acquirer deploys ATM Terminals that participate in any other shared deposit service, those ATM Terminals must participate in the Shared Deposit service.

An Acquirer may make only its ATM Terminals available for participation in the Shared Deposit service. An Acquirer that, as an Issuer, elects to take part in the Shared Deposit service must designate its BINs/IINs and ATM Terminals that participate in any other shared deposit service for participation in the Shared Deposit service.

### **4.20.1 Non-discrimination Regarding Shared Deposits**

An Acquirer may impose a dollar limit on Shared Deposits accepted at an ATM Terminal provided that the limit imposed on Cardholders is the same or more favorable than the limits imposed on cardholders of other networks. This Rule does not limit the application of other non-discrimination provisions contained in the Standards.

### **4.20.2 Terminal Signs and Notices**

An Acquirer must display a notice regarding funds availability in accordance with section 229.18(c) of Regulation CC, 12 C.F.R. § 229.18(c) on each ATM Terminal that participates in the Shared Deposit service.

### **4.20.3 Maximum Shared Deposit Amount**

The maximum Shared Deposit Transaction amount must be limited to USD 99,999.99.

### **4.20.4 Deposit Verification**

An Acquirer must process its Shared Deposits as follows.



1. The Acquirer must complete an examination of each Shared Deposit no later than one business day after the date of the Transaction;
2. Such examination must be conducted under dual control standards either by two employees of the Acquirer or by one or more employees of the Acquirer with a surveillance camera monitoring the examination;
3. The examination must consist of the following:
  1. The deposit must be verified to ensure that the dollar amount of the deposit keyed by the Cardholder at the ATM Terminal matches the deposit contents; the deposit envelope is not empty; and the deposit envelope does not contain only non-negotiable items;
  2. The Acquirer must identify any irregularities that would make an item in the deposit envelope non-negotiable, such as:
    - The deposited currency is counterfeit;
    - The deposited currency, check or money order is in a denomination other than U.S. Region currency;
    - The item is drawn on or payable by an institution located outside the U.S. Region;
    - The item has a passbook attached;
    - The item is a photocopy;
    - The item is a certificate of deposit or banker's acceptance;
    - The item is a non-negotiable writing;
    - The item is a returned or cancelled check or draft;
    - A date is not present on the item;
    - The item is postdated;
    - The item is dated more than six months prior to the date of the deposit;
    - The payee field has not been completed;
    - Either the written or numeric amount does not appear on the item;
    - The written amount does not match the numeric amount on the item;
    - The amount on the item appears altered;
    - The item includes restrictive wording;
    - The item is missing an endorsement;
    - The item, which requires a signature, is unsigned
  3. The Acquirer must submit an adjustment within one business day of the deposit verification date if a discrepancy exists between the deposit amount and the amount keyed into the ATM Terminal.

#### **4.20.5 ATM Terminal Clearing and Deposit Processing**

An Acquirer that accepts Shared Deposits must clear its ATM Terminals at least once each business day.

By the end of the business day following the day on which an ATM Terminal was cleared, the Acquirer must forward for collection all Shared Deposits cleared from that Terminal in the same manner it would forward its own Cardholders' deposits.

#### **4.20.6 Shared Deposits in Excess of USD 10,000**

If an Acquirer receives a Shared Deposit or series of related Shared Deposits made to a single Account on one business day containing currency in excess of USD 10,000, the Acquirer must notify the Issuer of this fact by telephone, facsimile, or any other means permitted by the Corporation within two business days of the date of deposit. The Acquirer must record the occurrence as well as the act of reporting the occurrence and must include the name of the Issuer's employee that received notification.

The notification must include the following:

1. Cardholder number;
2. Amount of currency;
3. Amount of currency in bills of denomination of USD 10,000 or higher;
4. ATM Terminal location;
5. Date and time of deposit.

If the Acquirer fails to provide notification of such a cash deposits and the Issuer is assessed penalties or fines as a result of the Acquirer's failure, the Acquirer must indemnify the Issuer for such penalties and fines.

#### **4.20.7 Notice of Return**

If an item sent by an Acquirer to the payor bank of the item for presentment is returned to the Acquirer for any reason or the Acquirer receives notice of nonpayment of the item for any reason from the payor bank, the Acquirer must notify the Issuer of the receipt of such return or notice, and must initiate return of the returned item to the Issuer no later than one business day following the receipt of the returned item or the notice of nonpayment, whichever is received first. Such notice to the Issuer must include the reason for nonpayment as set forth on the returned item or notice of nonpayment received.

#### **4.20.8 Liability for Shared Deposits**

The maximum damages that an Acquirer may face for its failure to comply with these Shared Deposit Rules is the amount of loss incurred by the Issuer with respect to a particular Shared Deposit, not to exceed the amount of the Shared Deposit. In addition, an Acquirer will not be liable to an Issuer for any amount of the Shared Deposit that the Issuer could have recovered from the Cardholder. An Issuer must claim that:

1. Its Cardholder would not accept the adjustment of an improper Shared Deposit;
2. It could not debit the Cardholder when the Issuer received notice of the improper deposit; and
3. It could have debited the Cardholder if the Acquirer had complied with these Shared Deposit Rules.

In all events, the Issuer must first attempt to collect from its Cardholder.

## Chapter 5 Card-Not-Present Transactions

*The following Standards apply with regard to Transactions that occur in a Card-not-present environment, including electronic commerce (e-commerce), mail order/telephone order (MO/TO), and recurring payment Transactions. Where applicable, variations or additions by region and/or country are provided at the end of this chapter in the section titled, "Variations and Additions by Region."*

5.1 Electronic Commerce Transactions.....	149
5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements.....	149
5.1.2 E-commerce Transactions—Issuer Requirements.....	151
5.1.3 Use of Static AAV for Card-not-present Transactions.....	152
5.2 Mail Order and Telephone Order (MO/TO) Transactions.....	152
5.3 Credential-on-File Transactions.....	153
5.4 Recurring Payment Transactions.....	153
5.4.1 Recurring Payment Transactions for High-Risk Negative Option Billing Merchants.....	155
5.5 Installment Billing for Domestic Transactions—Participating Countries Only.....	156
5.5.1 Applicability of Rules.....	157
5.5.2 Definitions.....	157
5.5.3 Transaction Processing Procedures.....	158
5.6 Transit Transactions Performed for Debt Recovery.....	159
5.7 Use of Automatic Billing Updater.....	159
5.8 Authentication Requirements—Europe Region Only.....	160
5.9 Merchant-initiated Transactions—EEA Only.....	160
Variations and Additions by Region.....	160
Asia/Pacific Region.....	160
5.1 Electronic Commerce Transactions.....	160
5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements.....	161
5.1.2 E-commerce Transactions—Issuer Requirements.....	161
5.2 Mail Order and Telephone Order (MO/TO) Transactions.....	162
5.3 Credential-on-File Transactions.....	163
5.7 Use of Automatic Billing Updater.....	163
Canada Region.....	163
5.7 Use of Automatic Billing Updater.....	163
Europe Region.....	163
5.1 Electronic Commerce Transactions.....	163
5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements.....	163
5.1.2 E-commerce Transactions—Issuer Requirements.....	164

5.1.3 Use of Static AAV for Card-not-present Transactions.....	165
5.2 Mail Order and Telephone Order (MO/TO) Maestro Transactions.....	166
5.2.1 Definitions.....	166
5.2.2 Intracountry Maestro MO/TO Transactions—Cardholder Authority.....	167
5.2.3 Intracountry Maestro MO/TO Transactions—Transactions Per Cardholder Authority...	167
5.2.4 Intracountry Maestro MO/TO Transactions—CVC 2/AVS Checks.....	167
5.3 Credential-on-File Transactions.....	168
5.4 Recurring Payment Transactions.....	168
5.5 Installment Billing for Domestic Transactions—Participating Countries Only.....	169
5.5.3 Transaction Processing Procedures.....	180
5.6 Transit Transactions Performed for Debt Recovery.....	181
5.7 Use of Automatic Billing Updater.....	181
5.7.1 Issuer Requirements.....	181
5.7.2 Acquirer Requirements.....	182
5.8 Authentication Requirements.....	184
5.8.1 Acquirer Requirements.....	184
5.8.2 Issuer Requirements.....	187
5.9 Merchant-initiated Transactions – EEA Only.....	187
Latin America and the Caribbean Region.....	188
5.1 Electronic Commerce Transactions.....	188
5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements.....	188
5.1.2 E-commerce Transactions—Issuer Requirements.....	189
5.7 Use of Automatic Billing Updater.....	189
Middle East/Africa Region.....	189
5.1 Electronic Commerce Transactions.....	189
5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements.....	189
5.1.2 E-commerce Transactions—Issuer Requirements.....	189
5.7 Use of Automatic Billing Updater.....	189
United States Region.....	190
5.7 Use of Automatic Billing Updater.....	190

## 5.1 Electronic Commerce Transactions

---

An electronic commerce (“e-commerce”) Transaction must be authorized by the Issuer, in accordance with the authorization requirements described in Chapter 2. An e-commerce Transaction must not be effected using contactless payment, Mastercard Consumer-Presented QR payment, or as a purchase with cash back Transaction.

**NOTE: Additions to this Rule appear in the “Asia/Pacific Region” and “Europe Region” sections at the end of this chapter.**

### 5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements

Each Acquirer and Merchant conducting any e-commerce Transactions must comply with the following requirements:

1. The Merchant must display the appropriate Acceptance Marks on its website where payment methods are listed, in accordance with the Standards set forth in Chapters 4 and 5 of the *Mastercard Rules*.
2. The Merchant must provide a mailing address and a contact telephone number or email address for customer queries. This information may 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.
3. 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.
4. For each Merchant supporting Mastercard SecureCode or Identity Check, the Acquirer must provide the Merchant with a Merchant ID, and ensure that the Merchant correctly populates all UCAF fields with required data elements. Refer to the *Mastercard SecureCode—Acquirer Implementation Guide* for more information.
5. 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 posting and packing, etc.
6. 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.
7. 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.
8. 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.

9. The information provided on any email acknowledgment of the Cardholder's order must comply with the Transaction receipt requirements described in Chapter 3.
10. For a physical product or a sample of the physical product provided to a Cardholder by a high-risk negative option billing Merchant for a trial period, the trial period begins on the date that the Cardholder receives the product.  
For purposes of this Rule 5.1.1, a trial period means a preset length of time during which the Cardholder may evaluate the characteristics of the 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.
11. If the Merchant is a high-risk negative option billing Merchant, then the Merchant must provide a direct link to an online cancellation procedure for recurring payment Transactions on the website on which the Cardholder initiated an agreement with the Merchant to bill the Cardholder on a recurring basis for one or more physical products provided by the Merchant through the Merchant's website.

In addition, with respect to **Maestro e-commerce Transactions**:

1. The Acquirer and Merchant must be capable of accepting PANs between 13 and 19 digits in length and sending the full unaltered PAN and the expiration date (in MMY format) to the Interchange System. Transactions must not be declined by the Merchant or Acquirer as a result of edits or validations performed on the BIN/IIN or expiration date;
2. The Merchant must support Mastercard SecureCode or Identity Check;
  - a. For the EMV 3D Secure 2.0 specification, a Merchant must support both browser and in-app Transactions;
  - b. For the 3D Secure 1.0 specification, a Merchant must support browser Transactions and may support in-app Transactions;
3. The Acquirer and Merchant must support the passing of authentication data in the Universal Cardholder Authentication Field (UCAF);
4. The Acquirer must support the 3D Secure Merchant Plug-in, and be capable of handling Transactions within a 3D Secure environment;
5. The Merchant must provide a set of "help" functions to help Cardholders that have not yet been enabled by their Issuers for transacting via the Internet; and
6. On an ongoing basis, the Acquirer must educate its Merchants to ensure that each Merchant has an understanding of the special risks and responsibilities associated with accepting Transactions in an e-commerce environment.

**NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," "Latin America and the Caribbean Region," and "Middle East/Africa Region" sections at the end of this chapter.**

## 5.1.2 E-commerce Transactions—Issuer Requirements

An Issuer must approve or decline each e-commerce Transaction authorization request. Call referrals are not permitted.

A Region that previously implemented an intraregional Merchant-only liability shift for e-commerce Transactions may agree to require Issuers in that Region to implement Mastercard® SecureCode™ or Identity Check or both.

An Issuer that uses Mastercard SecureCode or Identity Check to verify its Cardholders must:

- Use the Mastercard Secure Payment Application (SPA) algorithm to generate the Accountholder Authentication Value (AAV);
- Verify the validity of the AAV when present in DE 48, subelement 43 of the authorization request message, or participate in the Mastercard SecureCode AAV Verification Service (refer to the Asia/Pacific Region section at the end of this chapter for a modification to this effective date); and
- Provide and keep updated information for display on the website [mastercard.com/securecode](https://www.mastercard.com/securecode).

Refer to the *Mastercard SecureCode—Issuer Implementation Guide* for further information. Mastercard SecureCode and Identity Check liability shifts applicable to e-commerce Transactions conducted with a **Mastercard Card** are described in the *Chargeback Guide*.

Refer to the *Chargeback Guide* for information about using message reason code 4841 (Cancelled Recurring Transactions and Digital Goods Purchases Under USD 25) to charge back a Transaction under USD 25 involving the purchase of Digital Goods.

The following applies with respect to a **Maestro Card** Program:

1. The Issuer is encouraged but not required to permit a Maestro Cardholder to engage in e-commerce Transactions. An Issuer that permits its Maestro Cardholders to perform e-commerce Transactions must be capable of recognizing and processing these Transactions when presented by an Acquirer.
2. The Issuer should provide a registration and set-up process for Cardholders wishing to engage in e-commerce Transactions.
3. The Issuer must provide a Cardholder wishing to engage in e-commerce Transactions with a PAN of between 13 and 19 digits in length and an expiration date in MMY format. The PAN must start with a Maestro BIN/IIN, which may be a BIN that is currently used by the Issuer. The Issuer may optionally use a PAN that is different from the PAN displayed on the Card (a “pseudo PAN”). If a pseudo PAN is used, it must be static and have an expiration date that does not exceed five years from the PAN issuance date.
4. The Issuer must implement security techniques between the Cardholder interface device and the Issuer server to guard against unauthorized Transactions.
5. The Issuer is responsible for deciding which CVMs are acceptable for the completion of e-commerce Transactions, and may choose to request that a Cardholder use a chip/hardware authentication device.

6. An Issuer should educate Cardholders of the risks of releasing Card details and PINs into open networks and entering PINs into public terminals without using the approved methods.
7. An Issuer may directly implement Mastercard *SecureCode* or Identity Check and register its Cardholders and each Cardholder's authentication information, or delegate a specific implementation and registration function to a designated Service Provider, in accordance with the set-up requirements provided to the Corporation by the Issuer. The Issuer must ensure that Cardholders are properly identified if issuing certificates.
8. The Issuer must perform an appropriate risk assessment on any Transaction for which the UCAF field (data element 48, subelement 43) contains a Corporation-assigned static AAV.
9. The Issuer is responsible for fraud in connection with any e-commerce Transaction that the Issuer has approved, unless it can be proved that the Merchant and/or Acquirer participated in the fraud or the Merchant Website does not support the passing of UCAF data. However, the Issuer will have a chargeback right for fraudulent Transactions containing the Corporation-assigned static AAV in the UCAF field.

**NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," "Latin America and the Caribbean Region," and "Middle East/Africa Region" sections at the end of this chapter.**

### 5.1.3 Use of Static AAV for Card-not-present Transactions

**NOTE: A Rule on this topic appears in the "Europe Region" section of this chapter.**

## 5.2 Mail Order and Telephone Order (MO/TO) Transactions

---

The following requirements apply to mail order and telephone ("phone") order (MO/TO) Transactions effected with a Mastercard Account, and where supported, a Maestro Account, including phone order Transactions conducted with Integrated Voice Response (IVR) technology. MO/TO Transactions are supported for Maestro in some of the Europe Region countries and India only.

1. MO/TO Transactions must not be effected using contactless payment, Mastercard Consumer-Presented QR payment, or as purchase with cash back Transactions. Manual key entry of the PAN is the normal method of performing a MO/TO Transaction. Online authorization is required.
2. The Issuer must approve or decline each authorization request. A call referral is an invalid response to a MO/TO Transaction authorization request and must be treated by the Acquirer and the Merchant as a decline.
3. There is no Cardholder verification procedure for MO/TO Transactions; however, an Acquirer and Merchant may choose to support Mastercard *SecureCode* for Mastercard phone order Transactions conducted with Integrated Voice Response (IVR) technology.



4. The Merchant must not request an authorization, in a single message environment, or submit a Transaction to the Acquirer for presentment, in a dual message environment, until the products and services are available for delivery.

**NOTE: Additions to this Rule appear in the “Europe Region” section and, pertaining to India, in the “Asia/Pacific” sections at the end of this chapter.**

## 5.3 Credential-on-File Transactions

---

A Credential-on-file Transaction occurs when a Cardholder expressly authorizes a Merchant to store the Cardholder’s Mastercard or Maestro 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 Mastercard or Maestro Account data in one or more Transaction(s).

For authorization, a Credential-on-file Transaction must contain the Credential-on-file indicator, which is a value of 10 (Credential on File) in DE 22 (Point-of-Service Entry Mode), subfield 1 (POS Terminal PAN Entry).

For clearing, a Credential-on-file Transaction must contain the Credential-on-file indicator, which is a value of 7 (Credential on File) in DE 22 (Point-of-Service Entry Mode), subfield 7 (Card Data Input Mode).

The Acquirer should ensure that the Merchant retains the Cardholder’s written agreement to the terms of a Credential-on-file Transaction arrangement.

**NOTE: Modifications to this Rule appear in the “Asia/Pacific Region” and “Europe Region” sections at the end of this chapter.**

## 5.4 Recurring Payment Transactions

---

A recurring payment Transaction is a Transaction made pursuant to an agreement between a Cardholder and a Merchant, whereby the Cardholder authorizes the Merchant to store and use the Cardholder’s Mastercard Account or (where supported) Maestro Account data periodically and on an ongoing basis, with no specified end date. Use 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.

By way of example and not limitation, the following are Merchant categories that frequently process recurring payment Transactions:

- MCC 4814 (Telecommunication Services including but not limited to prepaid phone services and recurring phone services)
- MCC 4816 (Computer Network/Information Services)

- MCC 4899 (Cable, Satellite, and Other Pay Television and Radio Services)
- MCC 4900 (Utilities—Electric, Gas, Heating Oil, Sanitary, Water)
- MCC 5192 (Books, Periodicals, and Newspapers)
- MCC 5968 (Direct Marketing—Continuity/Subscription Merchants)
- MCC 6300 (Insurance Sales, Underwriting, and Premiums)

The Acquirer must identify the first Transaction of a recurring payment series with the following values.

Data Element	Subfield	Value
61 (Point-of-Service [POS] Data)	1 (POS Terminal Attendance)	One of the following: <ul style="list-style-type: none"> <li>• 0 (Attended Terminal)</li> <li>• 1 (Unattended Terminal [Cardholder-activated Terminal {CAT}, home PC, mobile phone, personal digital assistant {PDA}])</li> <li>• 2 (No Terminal used [voice/audio response unit {ARU} authorization; server])</li> </ul>
61 (Point-of-Service [POS] Data)	4 (POS Cardholder Presence)	One of the following: <ul style="list-style-type: none"> <li>• 0 (Cardholder present)</li> <li>• 1 (Cardholder not present, unspecified)</li> <li>• 2 (Mail/facsimile order)</li> <li>• 3 (Phone/ARU order)</li> <li>• 5 (Electronic order [home PC, Internet, mobile phone, PDA])</li> </ul>
61 (Point-of-Service [POS] Data)	5 (POS Card Presence)	One of the following: <ul style="list-style-type: none"> <li>• 0 (Card present)</li> <li>• 1 (Card not present)</li> </ul>

An Acquirer must identify each subsequent recurring payment Transaction with the following values.

Data Element	Subfield	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	<ul style="list-style-type: none"> <li>• 10 (Credential on File)</li> </ul>

Data Element	Subfield	Value
61 (Point-of-Service [POS] Data)	1 (POS Terminal Attendance)	One of the following: <ul style="list-style-type: none"> <li>1 (Unattended Terminal [Cardholder-activated Terminal {CAT}, home PC, mobile phone, personal digital assistant {PDA}])</li> <li>2 (No Terminal used [voice/ audio response unit {ARU} authorization; server])</li> </ul>
61 (Point-of-Service [POS] Data)	4 (POS Cardholder Presence)	4 (Standing order/recurring Transactions)
61 (Point-of-Service [POS] Data)	5 (POS Card Presence)	1 (Card not present)
61 (Point-of-Service [POS] Data)	10 (Cardholder-activated Terminal Level)	0 (Not a CAT Transaction)
61 (Point-of-Service [POS] Data)	11 (POS Card Data Terminal Input Capability Indicator)	6 (Key entry only)

The recurring payment indicator must not appear in installment billing Transactions.

An Issuer should provide a Merchant advice code in DE 48, subelement 84 of the authorization response message when declining a recurring payment Transaction authorization request. The Acquirer and the Merchant should be able to receive and act on the Merchant advice code when present.

The Acquirer should ensure that the Merchant retains the Cardholder's written agreement to the terms of a recurring payment Transaction arrangement. The Merchant must not deliver products or perform services pursuant to a recurring payment Transaction arrangement after receiving notification of its cancellation by the Cardholder or Issuer or that the Account on file is not to be honored.

**NOTE: Additions to this Rule appear in the "Europe Region" section at the end of this chapter.**

### 5.4.1 Recurring Payment Transactions for High-Risk Negative Option Billing Merchants

The following Standards apply to recurring payment Transactions associated with a high-risk negative option billing Merchant:

1. The Acquirer must process all subsequent recurring payment Transactions using the same Merchant ID in DE 42 (Card Acceptor ID Code) and Merchant name in DE 43, subfield 1 (Card Acceptor Name) as the Acquirer used for the initial payment Transaction.
2. After the trial period for a physical product has expired, the high-risk negative option billing Merchant must provide the following information to the Cardholder and receive the

Cardholder's explicit consent in relation to this information before the Merchant may submit an authorization request for the initial recurring payment Transaction:

- The Transaction amount
- The payment date of the Transaction

**NOTE: After the Cardholder has provided consent, the Merchant may not change this date; however, a later payment date may be offered by the Merchant prior to consent, if the authorization request results in a declined response from the Issuer due to insufficient funds in the Cardholder's Account.**

- The Merchant name as it will appear on the Cardholder's statement
- Instructions for terminating the recurring payment Transaction cycle (for example, canceling the subscription service) at the Cardholder's discretion

For purposes of this Rule 5.4.1, a trial period means a preset length of time during which the Cardholder may evaluate the characteristics of the 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.
3. Each time that the Merchant receives an approved authorization request, the Merchant must provide the Cardholder with a Transaction information document (TID) through an e-mail message or other electronic communication method (such as an SMS "text message") including instructions for terminating the recurring payment Transaction cycle (such as canceling the subscription service). If the Merchant provides the Cardholder with a TID after a declined authorization request, the TID must state the reason for the decline response.
  4. The Merchant must provide the Cardholder with written confirmation in either hard copy or electronic format when either or both of the following events occur:
    - The Cardholder's trial period expires
    - The recurring payment Transaction cycle has been terminated by either the Merchant or the Cardholder

For more information about high-risk negative option billing Merchants, refer to section 9.4.10 of the *Security Rules and Procedures* manual.

---

## 5.5 Installment Billing for Domestic Transactions—Participating Countries Only

---

Installment billing consists of payments by an Issuer to an Acquirer on behalf of a Cardholder who authorizes a Merchant to bill the Cardholder's Account on a continued, periodic basis (typically based on the Transaction date, and on a monthly basis) until the total amount due for the goods or services purchased from the Merchant is paid. The amount of each payment is a fixed amount determined by the total number of installments specified and the total amount of goods or services purchased.

Installment billing differs from recurring payments in that there is a specified end date. For example, a Cardholder contracted to pay BRL 500 on a monthly basis for one year for membership in a health club. This would not qualify as a recurring payment arrangement because there is a beginning and ending time specified for the membership.

**NOTE: Modifications to this Rule appear in the “Europe Region” section at the end of this chapter.**

### 5.5.1 Applicability of Rules

The Rules in this “Installment Billing” section and in message reason code 4850—Installment Billing Disputes apply only to Acquirer-financed and Merchant-financed installment billing. In Acquirer-financed and Merchant-financed installment billing, the Acquirer processes an authorization request containing installment information for the full Transaction amount. Upon Issuer approval, the Acquirer submits multiple clearing records for the installment payments, in accordance with the terms agreed by the Cardholder at the POI.

The first installment billing may occur in a Card-present or Card-not-present environment; all subsequent installment billings are processed as Card-not-present Transactions.

Mastercard also supports Issuer-financed installment billing, which differs in that upon authorization approval, the Acquirer submits a single clearing record for the full Transaction amount. The Issuer then bills the Cardholder for the installments in accordance with the terms agreed by the Cardholder at the POI.

### 5.5.2 Definitions

Solely for the purposes of the installment billing Rules set forth herein and in “Message Reason Code 4850—Installment Billing Dispute” in the “Domestic Chargebacks” section of the *Chargeback Guide*, the following terms have the meanings set forth below:

#### **Installment billing**

An arrangement agreed between a Merchant and a Cardholder at the POI whereby a fixed number of periodic payments will be processed to complete a total payment for goods or services purchased.

#### **Installment**

One of a fixed number of periodic payments processed by a Merchant and submitted by its Acquirer as a separate clearing record in accordance with an installment billing arrangement between the Merchant and the Cardholder.

#### **Installment acceleration**

Acceleration of the processing of remaining installments for a Transaction. When installment acceleration is requested by the Issuer, the Acquirer must immediately process all remaining installments for the Transaction.

### 5.5.3 Transaction Processing Procedures

The Authorization Request/0100 message of a Transaction to be billed in installments must contain the following information, and must not contain the recurring payment indicator:

- The appropriate installment billing indicator code in DE 48, subelement 95 (Promotion Code), and
- The installment plan type and the number of installments requested by the Cardholder at the time of purchase in DE 112 (Additional Data, National Use). The Authorization Request/0100 message must be submitted for the total value of the Transaction. The Acquirer must ensure that the Authorization Request Response/0100 message contains the same number of installments indicated in DE 112 of the Authorization Request/0100 message.

The Transaction receipt must include the number of installments agreed between the Cardholder and the Merchant at the time of the Transaction.

Each installment payment is cleared and settled separately upon the processing of each installment. The Acquirer may process each installment payment clearing record upon receipt from the Merchant as the installment becomes due. The Acquirer must ensure that each installment payment clearing record contains information identifying the original approved authorization, as follows:

- The values contained in DE 63 (Network Data) and DE 15 (Settlement Date) from the authorization request response message must be placed in DE 63, subfield 2 (Trace ID) of each clearing record, and
- The value contained in DE 38 (Approval Code) from the authorization request response message must be placed in DE 38 of each clearing record.

For Transactions completed with electronically recorded Card information (whether Card-read or key-entered), the first installment must be presented within seven calendar days of the Transaction date. For Transactions completed with manually recorded Card information (whether imprinted or handwritten), the first installment must be processed within 30 days of the Transaction date.

Unless otherwise agreed between the Cardholder and the Merchant, the period between installments must be 30 calendar days. Acceleration of the processing of installments is permitted when authorized by the Issuer.

The Issuer is responsible for ensuring that each installment is processed accurately and for identifying each installment number on the Cardholder's billing statement (for example, installment one of six).

**NOTE: A modification to this Rule appears in the "Europe Region" section at the end of this chapter.**

## 5.6 Transit Transactions Performed for Debt Recovery

---

An Issuer of Maestro Cards that allows its Cardholders to perform Maestro Contactless transit aggregated Transactions must be able to accept and must make an individual authorization decision for each transit debt recovery Transaction identified as a Card-not-present Transaction (for example, as a PAN key-entered, e-commerce, or mail order or telephone order (MO/TO) Transaction) when the Authorization Request/0100 or Financial Transaction Request/0200 message is properly identified with:

- A value of 07 (Debt Recovery) in DE 48 (Additional Data), subelement 64 (Transit Program), subfield 1 (Transit Transaction Type Indicator); and
- An amount in DE 4 (Amount, Transaction) that is less than or equal to the applicable Maestro Contactless transit aggregated Transaction ceiling limit.

**NOTE: A modification to this Rule appears in the “Europe Region” section at the end of this chapter.**

## 5.7 Use of Automatic Billing Updater

---

The Automatic Billing Updater (ABU) is used by a Customer to communicate changes to Account information to Merchants that participate in Account-on-file and recurring payment Transactions. For information about ABU, refer to the *Mastercard Automatic Billing Updater Reference Guide*, available on Publications through Mastercard Connect.

When applicable, an Issuer of Mastercard Cards and each Acquirer that accepts Mastercard Cards must participate in ABU and be able to send, receive, and process Automatic Billing Updater (ABU) data.

To participate in ABU, an Issuer must take all of the following actions:

- Complete the Automatic Billing Updater Customer Enrollment Form available on Mastercard Connect™. Regarding a newly assigned ICA or BIN, an Issuer has six months from the date of the assignment to comply with this requirement.
- Provide to ABU a one-time upload plus six months of historic ICA and BIN data changes, up to a maximum of 50 months' data, and all newly issued and reissued activated Accounts.
- Submit to ABU all of the types of Account changes defined in the Mastercard Automatic Billing Updater Reference Guide, excluding any such Account changes to Cards issued under exempt Mastercard Card Programs.

The following Card Programs and Accounts are exempt from ABU participation requirements:

- A non-reloadable prepaid Card Program, provided that the Issuer does not allow the prepaid Cards to be used to enter into recurring payment arrangements;
- Remote Transaction Accounts issued for a single use or other predefined purpose; and

- A Commercial Card Program, except that ABU participation requirements apply to Cards issued for use by a small business (for a list of small business Card Programs, see [www.Mastercardbusiness.com](http://www.Mastercardbusiness.com) and select “Cards” under “Small Business”).

**NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Canada Region," "Europe Region," "Latin America and the Caribbean Region," "Middle East/Africa Region," and "United States Region" sections at the end of this chapter.**

---

## 5.8 Authentication Requirements—Europe Region Only

---

**NOTE: Rules on this subject appear in the “Europe Region” section at the end of this chapter.**

---

## 5.9 Merchant-initiated Transactions—EEA Only

---

**NOTE: Rules on this subject appear in the “Europe Region” section at the end of this chapter.**

---

## Variations and Additions by Region

---

The remainder of this chapter provides modifications to the Standards set out in this chapter. The modifications are organized by region or country and by applicable subject title.

---

### Asia/Pacific Region

---

The following modifications to the Rules apply in the Asia/Pacific Region or in a particular Region country or countries. Refer to Appendix A for the Asia/Pacific Region geographic listing.

#### 5.1 Electronic Commerce Transactions

In the Asia/Pacific Region, the Rule on this subject is modified as follows. A Customer that participates as an Issuer in another international cardholder authentication program must certify that it has enabled its Cardholders and its e-commerce Merchants for Mastercard SecureCode or Identity Check or both.

In **India**, the Rule on this subject, as it applies to Mastercard Intracountry e-commerce Transactions, is modified as follows:

1. Electronic commerce Transactions occurring at a Merchant located in India with a Mastercard Card issued in India must be authenticated. An authenticated Transaction occurs when:
  - a. The Merchant is Universal Cardholder Authentication Field (UCAF)-enabled;



- b. The Issuer provided the UCAF data for that Transaction;
  - c. All other authorization and clearing requirements applicable to the Transaction were satisfied; and
  - d. The Authorization Request Response/0110 message reflected the Issuer's approval of the Transaction.
- 2. Each Issuer and e-commerce Transaction Acquirer must participate in the Activation During Shopping (ADS) method of Cardholder enrollment in Mastercard *SecureCode*. Cardholders must complete enrollment on the first attempt, and the Issuer must not permit a Cardholder to opt-out of the *SecureCode* enrollment process.
  - 3. Each Issuer and e-commerce Transaction Acquirer participating in the Mastercard Assurance Service must register with the Corporation. Each e-commerce Transaction enabled using the Mastercard Assurance Service must contain a value of 6 (UCAF Control Byte) in DE 48, subelement 43, position 1, and a value of MAS in DE 124 of the Authorization Request/0100 message. For additional information, please contact [south\\_asia\\_ops@mastercard.com](mailto:south_asia_ops@mastercard.com).

A refund for a Maestro Intracountry e-commerce Transaction must be processed as a Payment Transaction.

#### **5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements**

Effective 1 October 2019, an Acquirer must technically support in authorization and clearing the data fields and values described in Appendix C (Transaction Identification Requirements) for e-commerce Transactions and Digital Secure Remote Payment Transactions containing UCAF data.

In India, Bangladesh, and Malaysia, the Rule on this subject is modified as follows.

Effective 18 October 2019, each Acquirer and each Merchant must request Cardholder authentication using EMV 3DS and comply with the requirements set forth in the Identity Check authentication program.

#### **5.1.2 E-commerce Transactions—Issuer Requirements**

Effective 1 October 2019, an Issuer must technically support in authorization and clearing the data fields and values described in Appendix C (Transaction Identification Requirements) for e-commerce Transactions and Digital Secure Remote Payment Transactions containing UCAF data.

The requirement either to verify the validity of the AAV when present in DE 48, subelement 43 of the authorization request message or to participate in the Mastercard *SecureCode* AAV Verification Service does not apply to an Issuer in China.

In India, Singapore, Bangladesh, and Malaysia, the Rule on this subject is modified as follows.

Effective 18 October 2019, an Issuer must support EMV 3DS and respond to a Cardholder authentication request using a solution that is compliant with the Identity Check authentication program requirements.

## 5.2 Mail Order and Telephone Order (MO/TO) Transactions

In **India**, the Rule on this subject, as it pertains to Intracountry mail order and phone order (including Integrated Voice Response or IVR) Transactions (“MO/TO” Transactions), is modified as follows.

1. Mail order and phone order Transactions effected at a Merchant located in India with a Mastercard Card issued in India must be authenticated. An authenticated Transaction occurs when:
  - a. The Merchant is Universal Cardholder Authentication Field (UCAF)-enabled;
  - b. The Issuer provided the UCAF data for that Transaction;
  - c. All other authorization and clearing requirements applicable to the Transaction were satisfied; and
  - d. The Authorization Request Response/0110 message reflected the Issuer’s approval of the Transaction.
2. Each IVR Transaction enabled using Mastercard *SecureCode* must contain a value of 2 (*SecureCode* phone order) in DE 61 (point-of-service [POS] Data), subfield 7 (POS Transaction Status) of the Authorization Request/0100 message.
3. Each Issuer and MO/TO Transaction Acquirer participating in the Mastercard Assurance Service must register with the Corporation. Each mail order and phone order (including IVR) Transaction enabled using the Mastercard Assurance Service must contain a value of 6 (UCAF Control Byte) in DE 48, subelement 43, position 1, and a value of MAS in DE 124 of the Authorization Request/0100 message. For additional information, please contact [south\\_asia\\_ops@mastercard.com](mailto:south_asia_ops@mastercard.com).
4. An Issuer may not use message reason codes 4837, 4849 or 4863 to charge back a mail order or phone order (including IVR) Transaction that occurs at a Merchant located in India, if:
  - a. The Merchant is UCAF-enabled;
  - b. The Issuer provided the UCAF for that Transaction;
  - c. All other phone order authorization and clearing requirements were satisfied, including the presence of:
    - i. A value of 2 (*SecureCode* phone order) in DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) of the Authorization Request/0100 message for IVR Transactions enabled with Mastercard *SecureCode*; or
    - ii. A value of 6 (UCAF Control Byte) in DE 48, subelement 43, position 1, and a value of MAS in DE 124 of the Authorization Request/0100 message for mail order, phone order, or IVR Transactions enabled with the Mastercard Assurance Service.
  - d. The Authorization Request Response/0110 message reflected the Issuer’s approval of the Transaction.
5. Each Issuer and IVR Transaction Acquirer must participate in the Activation During Shopping (ADS) method of cardholder enrollment in Mastercard *SecureCode*. Cardholders must complete enrollment on the first attempt, and the Issuer must not permit a Cardholder to opt-out of the *SecureCode* enrollment process.

6. Each Issuer and mail order and phone order (including IVR) Transaction Acquirer that wishes to participate in the Mastercard Assurance Service must register with the Corporation.

### 5.3 Credential-on-File Transactions

In Japan, the Rule on this subject is modified as follows.

For Acquirers in Japan, for authorization, a Credential-on-file Transaction may contain the Credential-on-file indicator, which is a value of 10 (Credential on File) in DE 22 (Point-of-Service Entry Mode), subfield 1 (POS Terminal PAN Entry).

For Acquirers in Japan, for clearing, a Credential-on-file Transaction may contain the Credential-on-file indicator, which is a value of 7 (Credential on File) in DE 22 (Point-of-Service Entry Mode), subfield 7 (Card Data Input Mode).

### 5.7 Use of Automatic Billing Updater

An Issuer in the Asia/Pacific Region must comply with the ABU requirements set forth in this chapter by 1 November 2018.

An Acquirer in the Asia/Pacific Region may comply with the ABU requirements set forth in this chapter.

## Canada Region

---

The following modifications to the Rules apply in the Canada Region. Refer to Appendix A for the Canada Region geographic listing.

### 5.7 Use of Automatic Billing Updater

Each Issuer and Acquirer in the Canada Region must comply with the ABU requirements set forth in this chapter.

## Europe Region

---

The following modifications to the Rules apply in the Europe Region or in a particular Region country or countries. Refer to Appendix A for the Europe Region, Non-Single European Payments Area (Non-SEPA) and Single European Payments Area (SEPA) geographic listing.

### 5.1 Electronic Commerce Transactions

#### 5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements

In the Europe Region, the Rule on this subject is modified as follows.

An Acquirer must technically support the authorization and clearing of the data fields and values described in Appendix C, Transaction Identification Requirements, for e-commerce Transactions and Digital Secure Remote Payment Transactions containing UCAF data, if the

Transactions are processed via the Interchange System. If the Transactions are processed via an alternative switch, the Acquirer must populate the corresponding data fields in authorization and clearing messages with the values specified by the alternative switch.

For Maestro e-commerce Transactions, the Acquirer and Merchant must be capable of sending the full unaltered PAN to the registered switch of the Acquirer's choice.

The following Rules apply to Intra-EEA Transactions and to Intracountry Transactions in the EEA.

## **PSD2 Strong Customer Authentication (SCA) Requirements**

### **Authentication Amount**

Effective 14 September 2019, the authentication amount for a Remote Electronic Transaction must be an amount that the Cardholder would reasonably expect and the authentication must use the same currency as the authorization.

As a best practice, the total Transaction amount of all authorizations that relate to a Remote Electronic Transaction should not exceed the authentication amount for the Transaction by more than 20 percent (20%). If the Transaction amount is not known in advance, the authentication amount must be an amount that the Cardholder would reasonably expect (e.g., within a tolerance of 20 percent [20%]). In this case, if the authorization amount exceeds the authenticated amount by more than 20 percent (20%), it is recommended that the Merchant treat the incremental amount compared to the authenticated amount as a separate Transaction. Transactions subject to PSD2 RTS will require separate SCA unless an exemption applies or unless they are handled as Merchant-initiated Transactions. If the Transaction amount exceeds the Cardholder's reasonable expectations, the refund right for authorized transactions under Articles 76-77 PSD2 may apply.

This Rule does not apply to recurring payment Transactions.

### **Attempt to Authenticate Following Soft Decline**

Effective 1 July 2020, in response to a decline of a Remote Electronic Transaction in which the Issuer indicates that SCA is required, a Merchant must attempt EMV 3DS authentication with the 3DS Requestor Challenge Indicator set to 04 (Challenge requested: Mandate). Until such time as all Issuers support the response code that indicates that SCA is required, a Merchant is advised always to send an authentication request following an authorization that is declined for non-financial and non-technical reasons.

It is recommended that the Merchant retry with a 3DS 1.0.2 authentication if the EMV 3DS authentication response has Transaction Status A (Attempts) and the Merchant is enrolled in 3DS 1.0.2. Transaction Status A will be used by Smart Authentication Stand-in when an EMV 3DS authentication request cannot be approved or when a Card is not enrolled for EMV 3DS, in which case retrying with a 3DS 1.0.2 authentication is likely to be approved, leading to higher authorization approval rates.

## **5.1.2 E-commerce Transactions—Issuer Requirements**

In the Europe Region, the Rule on this subject is modified as follows.

1. An Issuer must allow its Cardholders to engage in Maestro e-commerce Transactions on any Maestro Card except a prepaid Card.
2. An Issuer in Italy or San Marino must allow its Cardholders to engage in e-commerce Transactions using a Debit Card bearing the Debit Mastercard brand or the Maestro brand.
3. An Issuer in Albania, Austria, Bosnia, Bulgaria, Croatia, Czech Republic, Hungary, Israel, Kosovo, Macedonia, Montenegro, Poland, Romania, Serbia, Slovakia, or Slovenia must not participate in the Activation During Shopping (ADS) method of Cardholder enrollment in Mastercard SecureCode in a manner that would require the Cardholder to manually input any personal data, including a user name and/or password. An Issuer may require a Cardholder to confirm acceptance of SecureCode terms and conditions and/or acknowledgment of service activation by clicking a button. This Cardholder confirmation must be limited to a single click and a single SecureCode screen in the whole process.
4. An Issuer must technically support the authorization and clearing of the data fields and values described in Appendix C, Transaction Identification Requirements, for e-commerce Transactions and Digital Secure Remote Payment Transactions containing UCAF data, if the Transactions are processed via the Interchange System. If the Transactions are processed via an alternative switch, the Issuer must technically support the corresponding data fields and values specified by the alternative switch.

In the EEA, the Rule on this subject is modified as follows.

The UCAF field must be identified as specified by the registered switch of the Customer's choice.

The following Rule applies for Intra-EEA Transactions and Intracountry Transactions in the EEA.

### **PSD2 SCA Requirements – EEA Only**

Effective 14 September 2020, an Issuer in the EEA must decline authorization of a Remote Electronic Transaction using the "soft-decline" response code defined by the registered switch of its choice, if SCA is required and is missing. In response to a CNP authorization request, an Issuer must not use the "soft decline" response code for any reason other than requesting SCA. An Issuer must not use this response code if an authorization request is flagged as "fully authenticated".

### **5.1.3 Use of Static AAV for Card-not-present Transactions**

In the Europe Region, an Issuer must technically support Card-not-present Transactions that contain a value of 3, 4, or 5 in DE 48 (Additional Data—Private Use), subelement 43 (Static AAV), position 1 of Authorization Request/0100 messages. The Issuer must make individual authorization decisions and must not automatically decline authorization of Card-not-present Transactions containing these values.

In the EEA, the Rule on this subject is modified as follows.

The static AAV must be provided in authorization messages in the field and with the values specified by the registered switch of the Customer's choice.

## 5.2 Mail Order and Telephone Order (MO/TO) Maestro Transactions

In the Europe Region, the Rule on this subject is modified as follows.

### 5.2.1 Definitions

Solely within the Europe Region, the following terms have the meanings set forth below:

#### Address Verification Service (AVS)

A process whereby the Issuer checks the address given for a Card-not-present Transaction. For more information on AVS participation and message requirements, refer to Chapter 5 of the *Customer Interface Specification* manual and Chapter 9 of the *Authorization Manual*.

#### Cardholder Authority

A Cardholder's instructions requesting a Merchant to perform a CNP Transaction.

#### CVC 2/AVS Check

Automated verification by the Issuer of the Card Validation Code (CVC) 2 and address details provided for a CNP Transaction.

#### Mail Order Transaction

A CNP Transaction for which the Cardholder provides a written Cardholder Authority.

#### Phone Order Transaction, Telephone Order Transaction

A CNP Transaction for which the Cardholder provides a Cardholder Authority through the telephone system.

An Acquirer in the **United Kingdom, Ireland, or France** that acquires intracountry MO/TO transactions under other debit brands must also acquire MO/TO Transactions under the Maestro brand. For the rules applicable to Intracountry Maestro POS Transactions in the United Kingdom, refer to the *UK Domestic Rules*.

Merchants located in Europe Region countries designated by the Corporation may at their option offer MO/TO Transactions on Maestro Cards issued in the same country. Merchants in the United Kingdom, Ireland, Turkey, and France may offer this option.

The Rules for Maestro MO/TO Transactions are the same as those for Maestro face-to-face POS Transactions except that:

1. A MO/TO Transaction must have its own unique Cardholder Authority.
2. Merchants must collect and transmit CVC 2 for all MO/TO Transactions. AVS checking is optional.
3. Merchants must not present the Transaction until the products or services are ready to be dispatched.
4. If the Merchant does not give the Cardholder the Transaction receipt or the products and/or services upon completion of the Transaction, then they must be either delivered to the Cardholder by a method chosen at the Merchant's discretion or collected by the Cardholder.

### **5.2.2 Intracountry Maestro MO/TO Transactions—Cardholder Authority**

For a Maestro Mail Order Transaction, a document signed by the Cardholder or a document which the Acquirer considers to be acceptable in lieu of a signed document (for example, an authority sent by facsimile transmission).

For a Maestro Telephone Order Transaction:

1. Either instructions given over the telephone by the Cardholder to the Merchant, either to the Merchant's staff or to equipment operated by the Merchant (for example, an interactive voice system), or instructions given over the telephone by means of a text message from the Cardholder to the Merchant, via equipment operated by the Merchant; and
2. The date on which the Cardholder gave her/his authority.

### **5.2.3 Intracountry Maestro MO/TO Transactions—Transactions Per Cardholder Authority**

A Cardholder Authority must contain:

1. The Card's PAN, expiry date, and CVC 2;
2. The Cardholder's name and home address (including postcode);
3. The Transaction amount (including postage and packaging);
4. If products or services are to be delivered, the delivery address, and if the goods/services are to be delivered to or collected by a third party, the third party's name.

### **5.2.4 Intracountry Maestro MO/TO Transactions—CVC 2/AVS Checks**

The following applies where the Merchant carries out AVS checking and for CVC 2 checks:

1. The Cardholder authority must include the CVC 2 shown on the Cardholder's Card.
2. When entering the Transaction, the Merchant must key in the CVC 2 and numeric data in the Cardholder's address and postcode.
3. Online authorization must be sought for the Transaction.
4. The Acquirer must attempt to send the authorization request to the Issuer accompanied by the data referred to in paragraph 2 above.

When the Issuer's authorization response is an approval, the Issuer must accompany its response with an indication as to whether:

- The address, postcode, and CVC 2 data provided matches information held in its own records;
- The address, postcode, and CVC 2 data does not match information held in its own records;
- The address and postcode data provided have not been checked; or
- The address, postcode, and CVC 2 data has not been supplied.

When the Acquirer sends a response to the authorization request to the Merchant's POS Terminal, the message must include the Issuer's CVC 2 and AVS responses.



The Merchant must not re-use the CVC 2 or retain the CVC 2 in any manner for any purpose. The CVC 2 on a Cardholder authority for a Mail Order Transaction must be rendered unreadable prior to storage.

### 5.3 Credential-on-File Transactions

In the EEA, the Rule on this subject is modified as follows.

Credential-on-file Transactions must be identified in authorization and clearing messages as specified by the registered switch of the Customer's choice.

### 5.4 Recurring Payment Transactions

In the Europe Region, the Rule on this subject is modified as follows.

A Merchant may submit Maestro recurring payment Transactions using a risk-based authentication approach in accordance with program requirements. For the Mastercard Utility Payment Program (MUPP) or the Maestro Low Risk Merchant Program, for example, the Acquirer must ensure that the Merchant receives a Mastercard-assigned Merchant ID and static AAV.

An Issuer must:

1. Permit its Cardholders to perform recurring payment Transactions on all Maestro Cards except prepaid Maestro Cards. For prepaid Maestro Cards, it is strongly recommended that an Issuer allow its Cardholders to perform recurring payment Transactions; and
2. Recognize all properly identified recurring payment Transactions, including the identification of the first payment as either a face-to-face recurring payment Transaction or as an e-commerce recurring payment Transaction, depending on the environment in which the recurring payment arrangement is initiated.

In **France, Germany, Hungary, Ireland, Poland, Romania, Ukraine, and the United Kingdom**, the Rule on this subject, as it applies to Domestic recurring payment Transactions, is modified as follows:

1. It is recommended that an Acquirer ensure that a Merchant only includes the Card expiration date in the first Transaction of a recurring payment arrangement involving a particular Mastercard or Maestro Account number. Mastercard further recommends that the Card's expiration date not be included in any subsequent recurring payment Transaction authorization requests involving the same PAN. An Issuer must not decline a non-face-to-face recurring payment Transaction from a Merchant solely on the basis of missing Card expiration date information.
2. If a recurring payment Transaction authorization request is declined by the Issuer, the Acquirer must ensure that the Merchant resubmits the Transaction no more than once per day for a maximum of 31 consecutive days until the Transaction is approved by the Issuer.

For recurring payment Transactions relating to a bill invoiced to the Cardholder, it is recommended that in the First Presentment/1240 message, the Merchant name in DE 43 subfield 1 be followed by a space, the word "BILL" or the local language equivalent, a space, and the bill reference number.



In the EEA, the Rule on this subject is modified as follows.

Recurring payment Transactions must be identified in authorization messages as specified by the registered switch of the Customer's choice. If provided, the Merchant advice code must be provided in the field and with the value specified by the registered switch of the Customer's choice.

#### **PSD2 SCA Requirements - EEA Only**

The following Rules apply to Intra-EEA Transactions and to Intracountry Transactions in the EEA.

Effective 14 September 2020, SCA is required on the initial authorization in a recurring payment arrangement, unless the initial authorization takes place as Card-present or MO/TO.

The initial authorization (either authorization request or account status inquiry) in a recurring payment arrangement must be identified as a recurring payment using the appropriate values in the fields specified by the registered switch of the Customer's choice.

Effective 14 September 2020, an Acquirer must provide the unique Trace ID from the initial recurring payment authorization response in the appropriate field of a subsequent recurring payment authorization request, as specified by the registered switch of its choice.

If the initial authorization took place as Card-present or MO/TO, or occurred before 14 September 2020, then the Trace ID may be populated with a default value as specified by the registered switch of the Acquirer's choice.

Alternatively, if the initial authorization occurred before 14 September 2020, the Acquirer may provide the Trace ID of any other authorization belonging to that same recurring payment arrangement, provided that this authorization took place before 14 September 2020.

The Trace ID will be considered the reference to the mandate that the Cardholder provided to and authenticated with the Merchant.

Effective 14 September 2020, the Issuer must be able to use the Trace ID provided in the authorization message of a subsequent recurring payment to retrieve and confirm the original recurring payment mandate.

### **5.5 Installment Billing for Domestic Transactions—Participating Countries Only**

In the Europe Region countries where the Mastercard installment billing service is supported, the Rule on this subject is modified as follows.

In participating countries in the Europe Region, installment billing is not limited to Domestic Transactions only.

Within a single country, only one option may be supported, either Issuer-financed installment billing or Acquirer-financed installment billing, unless otherwise noted. The Rules in this section apply to both options unless otherwise specified.

Merchant-financed installment billing is in place in Greece. Refer to the Domestic Rules folder on Mastercard Connect™ for further information.

Issuer-financed installment billing is in place in the following countries:

- Czech Republic
- Hungary
- Poland (effective 1 March 2020)
- Romania
- Slovakia
- Slovenia
- Ukraine
- United Kingdom

The installment billing service is available in both face-to-face and non-face-to-face environments and for Mastercard, Debit Mastercard, and Maestro Card payments, except in the Czech Republic, Hungary, Poland, and Ukraine, where support of installment billing on Maestro is not required.

### **Issuer-financed Installment Billing**

A participating Issuer must clearly inform its Cardholders of the terms and conditions applicable to installment billing, the Card products that are eligible for installment billing, installment transaction fees, and outstanding amounts in connection with installment transactions performed by a Cardholder.

In the **Czech Republic, Hungary, Poland, Slovakia, Slovenia, Ukraine**, and the **United Kingdom**, an Issuer that wishes to participate in the installment billing service must register for “Mastercard POS Enabled Installments” via Mastercard Connect. The Issuer must be able to support the enhanced authorization request and response messages aimed at receiving and sending sufficient information on payment options and installment parameters to the POI. A participating Issuer must be able to split and post the billing of the Transaction amount to the Cardholder’s Account according to the option selected at the POI.

### **Acceptance Mark**

The Acquirer must ensure that a Merchant in the **Czech Republic, Georgia, Hungary, Poland, Romania, Slovakia, Slovenia**, or **Ukraine** that participates in the Mastercard installment billing service displays the special MC Installments mark at the POI.

### **Merchant Support—Czech Republic, Hungary, Poland, and Ukraine**

The Acquirer of a Merchant identified with an MCC not contained in the Merchant Exclusions section must ensure that the Mastercard installment billing service is supported at all POS Terminals and Card-not-present acceptance locations of the Merchant in the specific country, as applicable. At Cardholder-activated Terminals, support for the Mastercard installment billing service is a recommendation and not a requirement.

### **Merchant Support—Romania Only**

The Acquirer of a Merchant in Romania identified with an MCC in the following list must ensure that the Mastercard installment billing service is supported at all newly deployed POS Terminals and new Card-not-present acceptance locations of the Merchant, as applicable.

The Acquirer of a Merchant in Romania identified with an MCC in the following list must ensure that the Mastercard installment billing service is supported at all POS Terminals and Card-not-present acceptance locations of the Merchant, as applicable.

<b>MCC and Description</b>	<b>MCC and Description</b>
0742 Veterinary Services	5732 Electronic Sales
0780 Horticultural and Landscaping Services	5733 Music Stores—Musical Instruments, Pianos, Sheet Music
1711 Air Conditioning, Heating, and Plumbing Contractors	5734 Computer Software Stores
1731 Electrical Contractors	5921 Package Stores, Beer, Wine, Liquor
1750 Carpentry Contractors	5932 Antique Shops—Sales, Repairs, and Restoration Services
1771 Concrete Work Contractors	5940 Bicycle Shops—Sales and Service
3297 Tarom Romanian Air Transport	5941 Sporting Goods Stores
4511 Air Carriers, Airlines—not elsewhere classified	5944 Clock, Jewelry, Watch, and Silverware Store
4722 Travel Agencies and Tour Operators	5945 Game, Toy, and Hobby Shops
4812 Telecommunication Equipment Including Telephone Sales	5946 Camera and Photographic Supply Stores
4816 Computer Network/Information Services	5948 Leather Goods and Luggage Stores
5013 Motor Vehicle Supplies and New Parts	5965 Direct Marketing—Combination Catalog and Retail Merchants
5021 Office and Commercial Furniture	5969 Direct Marketing—Other Direct Marketers—not elsewhere classified
5039 Construction Materials—not elsewhere classified	5971 Art Dealers and Galleries
5044 Office, Photographic, Photocopy, and Microfilm Equipment	5975 Hearing Aids—Sales, Service, Supply Stores
5045 Computers, Computer Peripheral Equipment, Software	5976 Orthopedic Goods—Artificial Limb Stores
5047 Dental/Laboratory/Medical/Ophthalmic Hospital Equipment and Supplies	5977 Cosmetic Stores

<b>MCC and Description</b>	<b>MCC and Description</b>
5065 Electrical Parts and Equipment	5983 Fuel Dealers—Coal, Fuel Oil, Liquified Petroleum, Wood
5072 Hardware Equipment and Supplies	5999 Miscellaneous and Specialty Retail Stores
5074 Plumbing and Heating Equipment	6300 Insurance Sales, Underwriting, and Premiums
5094 Precious Stones and Metals, Watches and Jewelry	7032 Recreational and Sporting Camps
5111 Stationery, Office Supplies, Printing and Writing Paper	7298 Health and Beauty Spas
5137 Men's, Women's, and Children's Uniforms and Commercial Clothing	7372 Computer Programming, Data Processing, and Integrated Systems Design Services
5139 Commercial Footwear	7379 Computer Maintenance, Repair, and Services—not elsewhere classified
5198 Paints, Varnishes, and Supplies	7395 Photo Developing, Photofinishing Laboratories
5200 Home Supply Warehouse Stores	7531 Automotive Body Repair Shops
5211 Building Materials, Lumber Stores	7534 Tire Retreading and Repair Shops
5231 Glass, Paint, Wallpaper Stores	7538 Automotive Service Shops
5251 Hardware Stores	7622 Electronic Repair Shops
5511 Automobile and Truck Dealers—Sales, Service, Repairs, Parts, and Leasing	7699 Miscellaneous Repair Shops and Related Services
5521 Automobile And Truck Dealers—(Used Only) —Sales	7991 Tourist Attractions and Exhibits
5532 Automotive Tire Stores	7997 Clubs—Country Clubs, Membership (Athletic, Recreation, Sports), Private Golf Courses
5533 Automotive Parts, Accessories Stores	7999 Recreation Services—not elsewhere classified
5571 Motorcycle Shops and Dealers	8011 Doctors—not elsewhere classified
5599 Miscellaneous Automotive, Aircraft, and Farm Equipment Dealers—not elsewhere classified	8021 Dentists, Orthodontists
5611 Men's and Boy's Clothing And Accessories Stores	8042 Optometrists, Ophthalmologists

MCC and Description	MCC and Description
5621 Women's Ready To Wear Stores	8043 Opticians, Optical Goods, and Eyeglasses
5631 Women's Accessory And Specialty Stores	8049 Chiropodists, Podiatrists
5641 Children's and Infant's Wear Stores	8050 Nursing and Personal Care Facilities
5651 Family Clothing Stores	8062 Hospitals
5655 Sports Apparel, Riding Apparel Stores	8071 Dental and Medical Laboratories
5661 Shoe Stores	8099 Health Practitioners, Medical Services—not elsewhere classified
5681 Furriers and Fur Shops	8211 Schools, Elementary and Secondary
5691 Men's and Women's Clothing Stores	8220 Colleges, Universities, Professional Schools, and Junior Colleges
5699 Accessory and Apparel Stores—Miscellaneous	8249 Schools, Trade and Vocational
5712 Equipment, Furniture, and Home Furnishings Stores (except Appliances)	8299 Schools and Educational Services—not elsewhere classified
5713 Floor Covering Stores	8351 Child Care Services
5714 Drapery, Upholstery, and Window Coverings Stores	9222 Fines
5719 Miscellaneous House Furnishing Specialty Shops	9311 Tax Payments
5722 Household Appliance Stores	

### Merchant Support—Slovakia and Slovenia Only

The Acquirer of a Merchant in Slovakia or Slovenia identified with an MCC not contained in the Merchant Exclusions section must ensure that the Mastercard installment billing service is supported at all POS Terminals and Card-not-present acceptance locations of the Merchant, as applicable. At Cardholder-activated Terminals (CATs), support for the Mastercard installment billing service is a recommendation and not a requirement.

### Exclusions

The Mastercard installment billing service is permitted only for purchases of goods and services. It must not be offered on purchase with cash back Transactions.

Installments must not be offered if the clearing amount might not match the authorization amount, for example in the case of a preauthorization or an incremental authorization, or if

the Transaction type does not require Cardholder involvement, such as a Merchant-initiated Transaction or a recurring payment Transaction.

An Acquirer must not deploy installments-capable POS applications in an acceptance location identified with one of the following MCCs:

- 4829 (Money Transfer—Merchant)
- 6010 (Manual Cash Disbursements—Customer Financial Institution)
- 6050 (Quasi-Cash—Customer Financial Institution)
- 6051 (Quasi-Cash—Merchant)
- 6532 (Payment Transaction—Customer Financial Institution)
- 6533 (Payment Transaction—Merchant)
- 6536 (MoneySend Intracountry)
- 6537 (MoneySend Intercountry)
- 6538 (MoneySend Funding)
- 6540 (POI Funding Transaction)
- 7995 (Gambling Transactions)

In the **United Kingdom**, the following additional MCCs are also excluded:

- 6011 (Automated Cash Disbursements—Customer Financial Institution)
- 8999 (Professional Services—not elsewhere classified)
- 9311 (Tax Payments)

In the **Czech Republic** and **Hungary**, the following additional MCCs are also excluded:

- 6011 (Automated Cash Disbursements—Customer Financial Institution)
- 9406 (Government-owned Lottery)

In addition, in **Hungary**, support for installment billing at Merchants identified with any of the following MCCs is neither excluded nor mandatory:

MCC	Description
3000-3350	Airlines, Air Carriers
4111	Transportation-Suburban and Local Commuter Passenger, including Ferries
4112	Passenger Railways
4121	Limousines and Taxicabs
4225	Public Warehousing
4789	Transportation Services-Not Elsewhere Classified
5310	Discount Stores
5422	Freezer, Locker Meat Provisioners
5441	Candy, Nut, Confectionery Stores

<b>MCC</b>	<b>Description</b>
5451	Dairy Products Stores
5462	Bakeries
5499	Miscellaneous Food Stores
5811	Caterers
5812	Eating Places, Restaurants
5813	Bars, Cocktail Lounges, Discotheques, Nightclubs and Taverns
5814	Fast Food Restaurants
5935	Salvage and Wrecking Yards
5942	Book Stores
5947	Gift Card, Novelty and Souvenir Shops
5963	Door-to-Door Sales
5964	Direct Marketing-Catalog Merchants
5992	Florists
5993	Cigar Stores and Stands
5994	News Dealers and Newsstands
6012	Merchandise and Services-Customer Financial Institution
6211	Securities-Brokers/Dealers
7210	Cleaning, Garment, and Laundry Services
7211	Laundry Services-Family and Commercial
7216	Dry Cleaners
7273	Dating and Escort Services
7342	Exterminating and Disinfecting Services
7523	Automobile Parking Lots and Garages
7542	Car Washes
7829	Motion Picture and Video Tape Production and Distribution
7832	Motion Picture Theaters
7998	Aquariums, Dolphinariums, Zoos and Seaquariums
8041	Chiropractors

MCC	Description
8241	Schools, Correspondence

In **Poland**, the following additional MCCs are also excluded:

MCC	Description
5541	Service Stations with or without Ancillary Service
5542	Fuel Dispenser, Automated
5812	Eating Places, Restaurants
5813	Bars, Cocktail Lounges, Discotheques, Nightclubs and Taverns
5814	Fast Food Restaurants
5933	Pawn Shops
5960	Direct Marketing-Insurance Services
5962	Direct Marketing-Travel Related Arrangement Services
5964	Direct Marketing-Catalog Merchants
5965	Direct Marketing-Combination Catalog and Retail Merchants
5966	Direct Marketing-Outbound Telemarketing Merchants
5967	Direct Marketing-Inbound Telemarketing Merchants
5968	Direct Marketing-Continuity/Subscription Merchants
5969	Direct Marketing-Other Direct Marketers-Not Elsewhere Classified
6011	Automated Cash Disbursements-Customer Financial Institution
6012	Merchandise Services-Customer Financial Institutions
6211	Securities-Brokers/Dealers
7523	Automobile Parking Lots and Garages
9405	Intra-Government Purchases-Government Only



MCC	Description
9406	Government-Owned Lottery (including totalizator sportowy in Poland)

In **Ukraine**, the following additional MCCs are also excluded:

MCC	Description
5811	Caterers
5812	Eating Places, Restaurants
5813	Bars, Cocktail Lounges, Discotheques, Nightclubs and Taverns
5814	Fast Food Restaurants
6011	Automated Cash Disbursements-Customer Financial Institution
6012	Merchandise and Services – Customer Financial Institution
6211	Securities-Brokers/Dealers
9311	Tax Payments
9399	Government Services-Not Elsewhere Classified
9402	Postal Services-Government Only
9405	Intra-Government Purchases-Government Only
9406	Government-Owned Lottery (Non-U.S.)

### Transaction Amount

In **Hungary**, an Acquirer must enable the installment billing option only for Transaction amounts above HUF 20,000.

In **Poland**, an Acquirer must enable the installment billing option only for Transaction amounts above PLN 400. An Issuer must not set a different minimum amount.

In **Ukraine**, an Acquirer must enable the installment billing option only for Transaction amounts above UAH 3,000. An Issuer may set a minimum above this amount.

In the **United Kingdom**, the minimum purchase amount above which installment billing may be offered is GBP 150. An Issuer may set a minimum above this amount.

In the **Czech Republic**, the minimum purchase amount above which installment billing may be offered is CZK 1500. An Issuer may set a minimum above this amount.

In **Slovakia** and **Slovenia**, the minimum purchase amount above which installment billing may be offered is EUR 50. An Issuer may set a minimum above this amount.

### Information Requirements

The Cardholder must be informed clearly of the installment terms before agreeing to the installment billing arrangement. The required information includes the number, frequency, and amount of the installments and any associated fees. The information may be provided via screen messages on the POS terminal, or in another manner, provided that it is clear to the Cardholder.

The POS terminal or electronic commerce payment page of a participating Merchant must display both payment options—full payment and installment billing. If no selection is made then “full payment” is the default option. In the installments section of the menu, the cardholder may have the option to choose the number and/or frequency of installments (for example, between two and 24 installments).

Model POS Terminal and e-commerce displays are provided in Appendix F of this manual.

In **Poland**, the Cardholder will be provided repayment options of 3, 6, or 12 months.

In **Ukraine**, the Issuer must present to the Cardholder a maximum of three repayment options, for example, 3, 6, and 9 months, or 6, 9, and 12 months.

In **Hungary**, the authorization request must not contain the installments indicator if the currency is not HUF.

The authorization request response message must contain the following information, at a minimum:

- Total amount due
- Installment amount
- Interest rate
- Installment fee or annual percentage rate (APR)

In **Slovenia**, the authorization request response message must contain the following information, at a minimum:

- Total amount due
- Interest rate
- Installment fee
- Call center number

In **Poland**, the authorization request response message must contain three occurrences of the following installment payment data, for each of 3, 6, and 12 months payments options:

- Number of installments
- Interest rate
- Installment fee
- Annual percentage rate
- First installment amount

- Subsequent installment amount
- Total amount due

### Transaction Receipt Contents

Transaction receipt contents must be in the local language, if the Card is issued in the Merchant's country, and in English if the Card is issued in a different country.

The Transaction receipt or e-mail confirmation page must contain the additional information listed below if the Cardholder has chosen installment billing and the authorization request has been approved:

- Transaction type (Installment).
- If applicable, installment fee charged to the Cardholder for the transaction Total amount charged to the cardholder (price of the product or service plus if applicable, installment Transaction fee).
- Payment plan (information summarizing the number of installments and the amount of each installment. If the amount of the first installment is different from the subsequent installment amounts, this must be clearly stated on the Transaction receipt or electronic commerce payment page).

In **Poland**, the above information may be provided by the Issuer. In this case, the Transaction receipt or e-mail confirmation page must contain a statement advising the Cardholder to contact the Issuer for more information.

In **Hungary**, the Transaction receipt or e-mail confirmation page must additionally contain a legend inviting the Cardholder to contact the Issuer for more information and a contact telephone number.

In the **Czech Republic** and **Slovakia**, the Transaction receipt or e-mail confirmation page must additionally contain a legend inviting the Cardholder to contact the Issuer for more information.

In **Slovenia**, the Transaction receipt or e-mail confirmation page must additionally contain the interest rate and a contact telephone number.

In **Ukraine**, the Transaction receipt or e-mail confirmation page must additionally contain the address of the Issuer's website.

### Support for Transaction Identification

Each Issuer and Acquirer must technically support the proper coding for installment Transaction authorization and clearing messages, as must each participating Merchant.

In **Slovakia** and **Slovenia**, this requirement applies to all Acquirers, to all Merchants apart from excluded Merchants and to participating Issuers.

In the **Czech Republic**, **Hungary**, **Poland**, **Ukraine**, and the **United Kingdom**, this requirement applies to all Acquirers and to participating Issuers and Merchants.

If an Acquirer's Transaction volume in the country is below a threshold determined by the local country management, support by that Acquirer for the Mastercard installment billing service is recommended rather than required.

The requirement to technically support the proper coding of installment Transactions does not apply to any Acquirer that acquires only Merchants at which support for installment billing is excluded.

In participating countries **in the EEA**, the Rule on this subject is modified as follows.

Installment billing Transactions must be identified in authorization and clearing messages as specified by the registered switch of the Customer's choice. If provided, the Merchant advice code must be provided in the field and with the value specified by the registered switch of the Customer's choice.

### **Chargeback Rules**

For Issuer-financed installment billing, chargeback message reason code 4850 does not apply.

### **Authorization Processing**

Offline processing is not allowed for installment Transactions. Installment Transactions are not eligible for Stand-in or X-Code authorization processing. All installment authorization requests must be approved or declined only by the Issuer.

In the **EEA**, the Rule on this subject is modified as follows.

The decline reason codes in the table contained in this Rule are replaced by the corresponding reason codes specified by the registered switch of the Issuer's choice.

The Issuer must use the following decline response codes when appropriate, and the relevant description must be reflected on the screen of the POS Terminal or the webpage for the declined Transaction.

<b>DE 39 (Response Code)</b>	<b>Description</b>	<b>Reason</b>
13	Invalid amount	Installment Transaction amount less than GEL 45 (in Georgia)
57	Transaction not permitted to Cardholder	Invalid number of installments, issuer does not offer Installment Transactions at all, or not for this specific Cardholder
58	Transaction not permitted to Merchant	Installment Transactions must not be initiated by this Merchant (see "Excluded Transactions")

### **5.5.3 Transaction Processing Procedures**

In the EEA, the Rule on this subject is modified as follows.

Installment billing Transactions must contain the required data in authorization and clearing messages in accordance with the specifications of the registered switch of the Customer's choice.

## 5.6 Transit Transactions Performed for Debt Recovery

In the EEA, the Rule on this subject is modified as follows.

Transit Transactions performed for debt recovery must be identified in authorization messages as specified by the registered switch of the Customer's choice.

## 5.7 Use of Automatic Billing Updater

### 5.7.1 Issuer Requirements

By the following effective date	ABU must be used for Mastercard and Maestro Cards issued under a BIN or BIN range assigned for	With the exception of the following types of cards
In effect	Ireland	Non-reloadable prepaid Mastercard Cards in the BIN range of 539366 to 539585.
In effect	United Kingdom	Both consumer and corporate prepaid Cards that the Issuer does not permit to be used to enter into recurring payment arrangements, and single-use-only Virtual Accounts.
In effect	Italy	Non-reloadable prepaid Cards, single-use-only Virtual Accounts, and those Debit Mastercard Cards or Maestro Cards that are not required to be enabled for e-commerce.
In effect	Albania, Andorra, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Gibraltar, Greece, Iceland, Kazakhstan, Kosovo, Kyrgyzstan, Latvia, Lithuania, Luxembourg, Macedonia, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovakia, Slovenia, Spain, Sweden, San Marino, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, and Vatican City	Non-reloadable prepaid Cards, prepaid Cards that the Issuer does not permit to be used to enter into recurring payment arrangements, and single-use-only Virtual Accounts.

By the following effective date	ABU must be used for Mastercard and Maestro Cards issued under a BIN or BIN range assigned for	With the exception of the following types of cards
In effect	Germany, Liechtenstein, and Switzerland	Non-reloadable prepaid Cards, prepaid Cards that the Issuer does not permit to be used to enter into recurring payment arrangements, and single-use-only Virtual Accounts. Maestro Cards issued under a BIN assigned for Germany, Liechtenstein, or Switzerland are also excluded.

An Issuer must be able to send, receive, and process ABU data and must accurately maintain its entire Card portfolio in ABU, subject to the above-listed exceptions.

With respect to newly assigned ICAs and BINs, an Issuer is allowed six months from the date of assignment to come into compliance with the ABU requirements.

All of the types of Account changes defined in the *Mastercard Automatic Billing Updater Reference Guide* must be submitted to ABU.

An Issuer must not provide ABU support for Cards issued under an ICA or BIN that has not been assigned to it.

An Issuer must participate in the Mastercard Automatic Billing Updater program by completing ABU Customer Form 806 available on Mastercard Connect™.

To support the account validation process, an Issuer must report new Accounts and provide a one-time upload plus 6 months of historic data changes up to a maximum of 40 months data to the Issuer Account Change Database.

An Issuer is permitted to use an alternative continuity service, provided that it has an equivalent level of functionality and supports all Merchants globally.

### 5.7.2 Acquirer Requirements

By the following effective date	An Acquirer must comply with the requirements set out in this section, with regard to Merchants located in the following countries	That process the following Transaction types
In effect	Albania, Andorra, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Gibraltar, Greece, Hungary, Iceland, Ireland, Italy, Kazakhstan, Kosovo, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxembourg, Macedonia, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Spain, Sweden, Switzerland, Tajikistan, Turkmenistan, Ukraine, United Kingdom, Uzbekistan, and Vatican City	Recurring payments and Card-on-file Transactions

An Acquirer must:

1. Be technically able to send, receive, and process ABU data, and must ensure that the acquiring host processing system used by the Acquirer incorporates ABU functionality.
2. Participate in the ABU program by completing ABU Customer Form 806 available on Mastercard Connect™.
3. Register each Merchant that participates in the ABU program.
4. Submit Account number queries to ABU on behalf of each registered Merchant before authorization. The Acquirer must then take appropriate action based on any response codes received from ABU.
5. Submit account inquiry updates on behalf of each enrolled Merchant no less than once every 180 days.

It is strongly recommended that an Acquirer query the ABU database for brand flips to/from another scheme on behalf of registered Merchants located in the **United Kingdom** or **Ireland**.

An Acquirer has the option to submit brand flips to/from another scheme to the ABU program on behalf of registered Merchants.

An Acquirer is permitted to use an alternative continuity service, provided that it has an equivalent level of functionality and supports all Issuers and Merchants globally.

An Acquirer in the **United Kingdom** must additionally participate in the Account validation service and take appropriate action to inform Merchants of the response code received from the ABU program to support Account validation as outlined in the *Mastercard ABU Reference Guide*.

## **EEA**

In the EEA, the Rule on this subject is modified to replace references to the Automatic Billing Updater with references to the corresponding tool of the registered switch of the Customer's choice.

## **5.8 Authentication Requirements**

The Rules in this section apply with regard to Remote Electronic Transactions and to the Merchants that carry out such Transactions.

**"PSD2 RTS"** means the 2nd Payment Services Directive (Directive [EU] 2015/2366 of 25 November 2015) Regulatory Technical Standards on Strong Customer Authentication ("SCA").

### **5.8.1 Acquirer Requirements**

#### ***SecureCode* and Identity Check**

The Rules in this section apply according to the following timeline.



---

Effective Date	Countries
1 April 2019	Andorra
	Belgium
	Denmark
	Estonia
	Finland
	France
	Germany
	Gibraltar
	Iceland
	Ireland
	Italy
	Latvia
	Liechtenstein
	Lithuania
	Luxembourg
	Monaco
	Netherlands
	Norway
	Portugal
	San Marino
	Spain
	Sweden
	Switzerland
	Vatican City
	United Kingdom

---

Effective Date	Countries
1 September 2019	Albania
	Austria
	Bosnia and Herzegovina
	Bulgaria
	Czech Republic
	Croatia
	Cyprus
	Hungary
	Greece
	Israel
	Kosovo
	Macedonia
	Malta
	Montenegro
	Poland
	Romania
	Serbia
	Slovakia
	Slovenia
31 December 2019	Moldova
	Turkey
	Ukraine

---

Effective Date	Countries
1 April 2020	Armenia
	Azerbaijan
	Belarus
	Georgia
	Kazakhstan
	Kyrgyzstan
	Russian Federation
	Tajikistan
	Turkmenistan
	Uzbekistan

---

An Acquirer must ensure that its online Merchants support Cardholder authentication using EMV 3-D Secure version 2 (EMV 3DS) and comply with the Mastercard Identity Check Program, including display of the Identity Check brand.

A Merchant that already supports *SecureCode* must continue to support the current 3DS 1.0.2 format to ensure interoperability with Issuers that do not yet support EMV 3DS (for example, those outside of Europe).

In the EEA, Andorra, Monaco, San Marino, Switzerland, and Vatican City, an Acquirer and its online Merchants may implement alternative technical authentication solutions that are compliant with the Mastercard Identity Check Key Performance Indicators, which are published in the *Mastercard Identity Check Program Guide*.

### 5.8.2 Issuer Requirements

Issuer authentication requirements are contained in Rule 6.1 (Card Issuance—General Requirements) of Chapter 12 (Europe Region) of the *Mastercard Rules* manual.

## 5.9 Merchant-initiated Transactions – EEA Only

The following Rules apply for Intra-EEA Transactions and Intracountry Transactions in the EEA.

A Merchant-initiated Transaction (MIT) may represent a single payment or multiple payments (e.g., installment payments, travel bookings, purchases at marketplaces) or a recurring payment arrangement (e.g., utility bills, streaming services).

Effective 14 September 2020, to set up each individual MIT, SCA is required, in addition to an agreement between the Merchant and the Cardholder specifying the reason for the payment and the payment amount (or an estimate when the precise amount is not known).

An Acquirer is only allowed to process an MIT when:

- the Transaction is triggered by the Merchant, and the Cardholder is typically off-session (off-session means that the Cardholder is no longer interacting with the Merchant page or the Merchant app), or
- the Transaction is triggered by the Merchant, as the Transaction could not have been triggered by the Cardholder during checkout, because:
  - the final amount is not known during the checkout (e.g., online groceries shopping), or
  - an event triggered the Transaction after the checkout (e.g., miscellaneous rental or service charges), or
  - the Transaction is part of a recurring payment arrangement, or
  - the Transaction is segmented into different payments happening at different times (e.g., installments, travel bookings, marketplaces), or
  - the Transaction is a staged-wallet funding transaction.

The MIT exclusion must not be used to bypass the PSD2 SCA requirements for Transactions for which Card data has been registered on file with the Merchant and the Cardholder triggers the payment (Credential-on-File).

Effective 1 July 2020, an Acquirer must identify the MIT by populating the authorization message (either an authorization request or account status inquiry) with the appropriate value in the field specified by the registered switch of its choice. An Acquirer must use an account status inquiry when the MIT agreement has been established for a zero amount.

Effective 14 September 2020, setting up an MIT requires an authorization request or an account status inquiry, the Trace ID of which must be provided by the Acquirer in all subsequent related authorizations. Further processing of an MIT, including the Trace ID, must reflect the recurring payments and/or credential-on-file processing flags and rules.

If the initial authorization occurred before 14 September 2020 and its Trace ID is not available (for example, because it was not stored), then the Trace ID must be populated with a default value as specified by the registered switch of the Customer's choice.

Effective 14 September 2020, Issuers must be able to process the Trace ID, for example to validate if SCA took place to set up the MIT.

The requirement to reference the initial Authorization's Trace ID does not apply to reversals, which must continue to include the Trace ID of the authorization to be reversed.

## Latin America and the Caribbean Region

---

The following modifications to the Rules apply in the Latin America and the Caribbean Region. Refer to Appendix A for the Latin America and the Caribbean Region geographic listing.

### 5.1 Electronic Commerce Transactions

#### 5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements

In **Brazil**, the Rule on this subject is modified as follows:

Merchant websites must not display the Mastercard Acceptance Mark accompanied by the “débito” identifier.

### **5.1.2 E-commerce Transactions—Issuer Requirements**

In **Brazil**, the Rule on this subject is modified as follows:

An Issuer in Brazil must enable all Maestro Account ranges (including prepaid Accounts) to perform e-commerce Transactions. The use of Mastercard® *SecureCode*™ authentication is highly recommended.

## **5.7 Use of Automatic Billing Updater**

In the Latin America and the Caribbean Region, an Issuer using a third-party service for the purpose of communicating Account change information to Account-on-file and recurring payment Transaction Merchants is not required to participate in ABU, provided that such third-party service supports and is accessible to all Merchants regardless of Merchant location.

An Acquirer in the Latin America and the Caribbean Region must comply with the ABU requirements set forth in this chapter by 12 October 2018.

## **Middle East/Africa Region**

---

The following modifications to the Rules apply in the Middle East/Africa Region. Refer to Appendix A for the Middle East/Africa Region geographic listing.

## **5.1 Electronic Commerce Transactions**

### **5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements**

In Nigeria and South Africa, the Rule on this subject is modified as follows.

Effective 18 October 2019, each Acquirer and each Merchant must request Cardholder authentication using EMV 3DS and comply with the requirements set forth in the Identity Check authentication program.

### **5.1.2 E-commerce Transactions—Issuer Requirements**

In Nigeria and South Africa, the Rule on this subject is modified as follows.

Effective 18 October 2019, an Issuer must support EMV 3DS and respond to a Cardholder authentication request using a solution that is compliant with the Identity Check authentication program requirements.

## **5.7 Use of Automatic Billing Updater**

An Issuer in the Middle East/Africa Region must comply with the ABU requirements set forth in this chapter by 12 October 2018.

An Acquirer in the Middle East/Africa Region must comply with the ABU requirements set forth in this chapter by 12 October 2018.

## **United States Region**

---

The following modifications to the Rules apply in the United States (U.S.) Region. Refer to Appendix A for the U.S. Region geographic listing.

### **5.7 Use of Automatic Billing Updater**

An Issuer in the United States Region must comply with the ABU requirements set forth in this chapter.

An Issuer is not required to comply with the ABU requirements with respect to prepaid Card programs the Issuer may have.

## Chapter 6 Payment Transactions

*The following Standards apply with regard to Payment Transactions, including MoneySend Payment Transactions and Gaming Payment Transactions. Where applicable, variations or additions by region and/or country are provided at the end of this chapter in the section titled, "Variations and Additions by Region."*

6.1 Payment Transactions.....	192
6.1.1 Payment Transactions—Acquirer and Merchant Requirements.....	192
6.1.2 Payment Transactions—Issuer Requirements.....	193
6.2 Gaming Payment Transactions.....	194
6.3 MoneySend Payment Transactions.....	194
Variations and Additions by Region.....	194
Europe Region.....	194
6.1 Payment Transactions.....	195
6.1.1 Payment Transactions—Acquirer and Merchant Requirements.....	195
6.1.2 Payment Transactions—Issuer Requirements.....	195
6.2 Gaming Payment Transactions.....	195
6.3 MoneySend Payment Transactions.....	198
Middle East/Africa Region.....	198
6.2 Gaming Payment Transactions.....	198
United States Region.....	199
6.2 Gaming Payment Transactions.....	199

## 6.1 Payment Transactions

---

A Payment Transaction is a transfer of funds to an Account via the Corporation System.

Each Payment Transaction must comply with all requirements set forth herein, in Appendix C, and in the technical specifications for authorization messages.

If a Payment Transaction is conducted pursuant to a Customer-to-Customer, intracountry, or intercountry business service arrangement, the business service arrangement must be approved by the Corporation in writing, in advance of the effecting of a Payment Transaction. The Corporation reserves the right to audit or to monitor any Payment Transaction Program at any time.

**NOTE: Modifications to this Rule appear in the “Europe Region” section at the end of this chapter.**

### 6.1.1 Payment Transactions—Acquirer and Merchant Requirements

The following requirements apply to an Acquirer and any Merchant that conducts Payment Transactions:

1. An Acquirer must submit an authorization request to the receiving Issuer (either an Authorization Request/0100 or Financial Transaction Request/0200 message, as applicable) for each Payment Transaction.
2. Each Payment Transaction must be authorized, cleared and settled separately and distinctly. Two or more funds transfers or payments must not be aggregated into a single Payment Transaction, nor may one Payment Transaction be separated into two or more Payment Transactions.
3. A Payment Transaction must be effected on the date agreed to with the Cardholder whose Account is to be funded.
4. A Payment Transaction **must not** be effected:
  - a. To “authenticate” an Account or a Cardholder; for example, by effecting or attempting to effect a Payment Transaction for a nominal amount.
  - b. For any illegal purpose or any other purpose deemed by the Corporation to be impermissible.
  - c. For the purchase of goods or services, unless that Payment Transaction is expressly permitted by the Standards.
5. Funds for the Payment Transaction must be deemed collected and in the control of the Acquirer before the Payment Transaction is submitted to the Interchange System.
6. In a dual message environment, the Acquirer must submit a clearing message to the Interchange System within one calendar day of the Issuer’s approval of the authorization request. The Acquirer must ensure that the amount of the Payment Transaction in the clearing message matches the amount in the authorization request.
7. A reversal of a Payment Transaction (other than a MoneySend Payment 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 within one calendar day of the date the Payment Transaction was submitted to the Interchange System (as a Financial Transaction/0200 message or First Presentment/1240 message, as applicable) for posting to an Account. Reversible clerical errors include, by way of example and not limitation, the erroneous capture of Payment Transaction data, a duplicate Payment Transaction, or an error caused by the transposition of data.

8. A reversal of a MoneySend Payment Transaction must only be submitted for reasons of (a) timeout when the Acquirer's time-out limit has been exceeded for receiving the authorization request response message, or (b) incorrectly formatted response messages where the response received by the Acquirer is not properly formatted as defined for the request response messages in Dual Message System or Single Message System specifications. In such an event, the error must be reversed within sixty (60) seconds of when the original authorization message related to a MoneySend Payment Transaction was submitted to the Dual Message System or the Single Message System (as an Authorization Request/0100 message or a Financial Transaction/0200 message, as applicable) for posting to an Account, and must include Data Element (DE) 90 (subfields when available). Any other adjustment of a MoneySend Payment Transaction must be in accordance with the *MoneySend Program Guide*.
9. The Acquirer or Merchant that offers the Payment Transaction service must not request or require that a Cardholder disclose his or her PIN. If the Payment Transaction service is provided 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 Payment Transaction, the contents of that form must not lead the Cardholder to believe that he or she must provide his or her PIN. The Acquirer must ensure that the Merchant is following these procedures. The Corporation will also, from time to time, perform audits on these Merchants to ensure that they are compliant with this and all other requirements.

**NOTE: Modifications to this Rule appear in the "Europe Region" section at the end of this chapter.**

## 6.1.2 Payment Transactions—Issuer Requirements

The following requirements apply to an Issuer that receives Payment Transactions, **excluding** MoneySend Payment Transactions.

An Issuer that offers the Payment Transaction must make either the PAN or a pseudo PAN available to the Cardholder. If the Issuer provides the Cardholder with a pseudo PAN, the Issuer must be able to link the pseudo PAN to the Cardholder's actual PAN.

An Issuer must receive, process, and provide a valid authorization response to each Payment Transaction authorization request received.

Upon receiving a Payment Transaction, the Issuer, at its discretion, may:

1. Approve (and receive remuneration for costs incurred) or decline any requests by the Acquirer to correct a clerical error;
2. Establish a maximum Payment Transaction amount; or

3. Determine when to make the transferred funds available to the recipient—immediately or after a period of time defined by the Issuer.

A Payment Transaction must be effected in a way that does not conflict with Cardholder agreements or instructions.

**NOTE: An addition to this Rule appears in the “Europe Region” section at the end of this chapter.**

## 6.2 Gaming Payment Transactions

---

**NOTE: Rules on this subject appear in the “Europe Region”, “Middle East/Africa Region”, and “United States Region” sections at the end of this chapter.**

## 6.3 MoneySend Payment Transactions

---

Each Issuer and Acquirer and each MoneySend Payment Transaction must comply with all requirements set forth in the Standards applicable to MoneySend, including but not limited to those herein and in Appendix C, in the technical specifications for authorization messages, and in the *MoneySend Program Guide*.

An Issuer of a consumer Card Program or Eligible Commercial Card Program (excluding anonymous prepaid and gift Card Accounts) must be able to receive, process, authorize (meaning making an individual authorization decision with respect to each MoneySend Payment Transaction), and post MoneySend Payment Transactions in compliance with the Standards applicable to MoneySend. Refer to the *MoneySend Program Guide* for a list of Eligible Commercial Card Program types.

**NOTE: A modification to this Rule appears in the “Europe Region” section at the end of this chapter.**

## Variations and Additions by Region

---

The remainder of this chapter provides modifications to the Standards set out in this chapter. The modifications are organized by region or country and by applicable subject title.

### Europe Region

---

The following modifications to the Rules apply in the Europe Region or in a particular Region country or countries. Refer to Appendix A for the Europe Region, Non-Single European Payments Area (Non-SEPA) and Single European Payments Area (SEPA) geographic listing.

## 6.1 Payment Transactions

In the EEA, the Rule on this subject is modified as follows.

A Payment Transaction may be processed via any switch of the Customer's choice that is registered with the Corporation.

Each type of Payment Transaction must be identified in authorization and clearing messages as specified by the registered switch of the Customer's choice.

In Russia, the Rule on this subject is modified as follows.

Payment Transactions in Russia may be processed through a domestic switching service.

### 6.1.1 Payment Transactions—Acquirer and Merchant Requirements

In the Europe Region, the Rule on this subject is modified as follows.

With respect to an interregional Payment Transaction involving a Europe Region Acquirer and an Issuer located in another Region, if the Acquirer does not submit a clearing message to the Interchange System within seven days of the authorization request, the Corporation collects the Payment Transaction amount and any additional fees charged from the Acquirer by means of a Fee Collection/1740 message.

In the EEA, the Rule on this subject is modified as follows.

Funds for the Payment Transaction must be deemed collected and in the control of the Acquirer before the Payment Transaction is submitted to the registered switch of the Customer's choice.

The Acquirer must submit a clearing message to the registered switch of its choice within one calendar day of the Issuer's approval of the authorization request.

A clerical error must be reversed or adjusted within three calendar days of the date the Payment Transaction was submitted to the registered switch of the Acquirer's choice for posting to a Mastercard Account, or within one calendar day if submitted for posting to a Maestro or Cirrus Account.

### 6.1.2 Payment Transactions—Issuer Requirements

In **Italy**, the Rule on this subject is modified as follows:

1. An Issuer must support, process, and provide a valid authorization response to each Payment Transaction authorization request received, for all prepaid Mastercard, Debit Mastercard (including prepaid), and Mastercard charge Card Programs (revolving credit Card Programs are excluded); and
2. Except with respect to non-reloadable prepaid Cards, an Issuer must not automatically decline Payment Transactions.

## 6.2 Gaming Payment Transactions

In the Europe Region, in addition to the requirements for Payment Transactions, the following requirements apply to Gaming Payment Transactions:

1. The Gaming Payment Transaction may only be used to transfer winnings or unspent chips or other value usable for gambling to the same Card that the Cardholder used to place the bet or purchase value used or usable for gambling.
2. The Gaming Payment Transaction must be properly identified in authorization and clearing messages using MCC 7995, a Transaction type value of 28, and a Payment Transaction program type value of C04.
3. The Gaming Payment Transaction must not exceed EUR 50,000.
4. E-commerce Merchants that process Gaming Payment Transactions must be Mastercard® *SecureCode*™-enabled, and must seek Cardholder authentication during authorization of the Payment Transaction in which the bet is placed or the value to be used for gambling is purchased. The Maestro Low Risk Merchant Program is not available for such Merchants.
5. Mail order and telephone order (MO/TO) Merchants may process Gaming Payment Transactions.
6. Gaming Payment Transactions must not be processed to any type of Mastercard Corporate Card.
7. The following Anti-Money-Laundering (AML) requirements apply:
  - a. The Acquirer must consider its Merchants that submit Gaming Payment Transactions as higher risk under its anti-money laundering compliance program.
  - b. In addition to any requirement of applicable local law or regulation, the Acquirer must conduct enhanced customer due diligence reviews of any Merchant that submits Gaming Payment Transactions.
  - c. The Acquirer must ensure that each Merchant that submits Gaming Payment Transactions has appropriate controls in place to identify legitimate customers and to block suspicious activities, Cards, or Payment Transactions.
  - d. The Acquirer must have robust procedures and ongoing controls in place to monitor Transactions and Payment Transactions conducted by Merchants that submit Gaming Payment Transactions and to detect and report any potentially suspicious activity.
8. A Gaming Payment Transaction may be effected if not prohibited by applicable law or regulation and only for Cards issued in the following countries.

Country Code	Country	Country Code	Country
020	Andorra	428	Latvia
031	Azerbaijan	442	Luxembourg
040	Austria	470	Malta
056	Belgium	492	Monaco
070	Bosnia and Herzegovina	498	Moldova
100	Bulgaria	499	Montenegro
112	Belarus	528	Netherlands
196	Cyprus	578	Norway

Country Code	Country	Country Code	Country
203	Czech Republic	616	Poland
208	Denmark	642	Romania
233	Estonia	643	Russia
246	Finland	674	San Marino
250	France	688	Serbia
268	Georgia	703	Slovakia
280	Germany	705	Slovenia
292	Gibraltar	724	Spain
300	Greece	752	Sweden
348	Hungary	756	Switzerland
352	Iceland	792	Turkey
372	Ireland	804	Ukraine
380	Italy	826	United Kingdom

9. An Issuer in a country listed above must support the Gaming Payment Transaction in authorization and clearing messages.

An Issuer in Poland must only support Gaming Payment Transactions that originate from a Merchant that is properly licensed for gambling in Poland.

An Issuer in one of the following countries must support the Gaming Payment Transaction only for Domestic Transactions originating from a gambling Merchant that is properly licensed in the respective country.

- Bosnia and Herzegovina
- Montenegro
- Poland
- Russia
- Serbia

An Issuer in Finland must support the Gaming Payment Transaction on Debit and Prepaid Cards only, and not on Credit Cards.

An Issuer in Russia must make the transferred funds available to the Cardholder without delay after it has received the clearing message.

10. In Russia, the Acquirer must submit the clearing message within one business day of the Issuer's approval of the authorization request.
11. Gaming Payment Transactions will not be authorized in Mastercard Stand-In or Down Option Services. Authorization is entirely under the control of the Issuer. In the EEA,

reference to Mastercard Stand-In or Down Option Services is replaced by reference to the corresponding services of the registered switch of the Customer's choice.

## 6.3 MoneySend Payment Transactions

In the EEA, the Rule on this subject is modified as follows.

A MoneySend Payment Transaction may be processed via any switch of the Customer's choice that is registered with the Corporation.

## Middle East/Africa Region

---

The following modifications to the Rules apply in the Middle East/Africa Region. Refer to Appendix A for the Middle East/Africa Region geographic listing.

## 6.2 Gaming Payment Transactions

In the Middle East/Africa Region, in addition to the requirements for Payment Transactions, the following requirements apply to Gaming Payment Transactions:

1. The Gaming Payment Transaction may only be used to transfer winnings or unspent chips or other value usable for gambling to the same Card that the Cardholder used to place the bet or purchase value used or usable for gambling.
2. The Gaming Payment Transaction must be properly identified in authorization and clearing messages using MCC 7995, a Transaction type value of 28, and a Payment Transaction program type value of C04.
3. The Gaming Payment Transaction must not exceed USD 50,000 or the local currency equivalent.
4. E-commerce Merchants that process Gaming Payment Transactions must be Mastercard® *SecureCode*™-enabled, and must seek Cardholder authentication during authorization of the Payment Transaction in which the bet is placed or the value to be used for gambling is purchased.
5. Mail order and telephone order (MO/TO) Merchants may not process Gaming Payment Transactions.
6. Gaming Payment Transactions must not be processed to any type of Mastercard Corporate Card, Maestro Card, or prepaid Card. In Kenya, a Gaming Payment Transaction may be processed to a consumer prepaid Card (excluding anonymous prepaid Cards).
7. The following Anti-Money-Laundering (AML) requirements apply:
  - a. The Acquirer must consider its Merchants that submit Gaming Payment Transactions as higher risk under its anti-money laundering compliance program.
  - b. In addition to any requirement of applicable local law or regulation, the Acquirer must conduct enhanced customer due diligence reviews of any Merchant that submits Gaming Payment Transactions.
  - c. The Acquirer must ensure that each Merchant that submits Gaming Payment Transactions has appropriate controls in place to identify legitimate customers and to block suspicious activities, Cards, or Payment Transactions.

- d. The Acquirer must have robust procedures and ongoing controls in place to monitor Transactions and Payment Transactions conducted by Merchants that submit Gaming Payment Transactions and to detect and report any potentially suspicious activity.
8. A Gaming Payment Transaction may be effected if not prohibited by applicable law or regulation and only for Cards issued in the following countries.

Country Code	Country	Country Code	Country
024	Angola	480	Mauritius
072	Botswana	508	Mozambique
174	Comoros	516	Namibia
180	Democratic Republic of the Congo	566	Nigeria
262	Djibouti	646	Rwanda
232	Eritrea	690	Seychelles
230	Ethiopia	694	Sierra Leone
270	Gambia	706	Somalia
288	Ghana	728	South Sudan
404	Kenya	748	Swaziland
426	Lesotho	834	Tanzania
430	Liberia	800	Uganda
450	Madagascar	894	Zambia
454	Malawi	716	Zimbabwe

9. In Nigeria, an Issuer must support the Gaming Payment Transaction in authorization and clearing messages.
10. Gaming Payment Transactions will not be authorized by the Stand-In Processing Service. Authorization is entirely under the control of the Issuer.

## United States Region

The following modifications to the Rules apply in the United States (U.S.) Region. Refer to Appendix A for the U.S. Region geographic listing.

### 6.2 Gaming Payment Transactions

In the United States Region, in addition to the requirements for Payment Transactions, the following requirements apply to Gaming Payment Transactions:

1. The Gaming Payment Transaction may only be used to transfer winnings related to a lottery conducted and managed by a U.S. state government body to a Card that the Cardholder chooses.
2. The Gaming Payment Transaction must be properly identified in authorization and clearing messages using MCC 7800, a Transaction type value of 28, and a Payment Transaction program type value of C04.
3. The Gaming Payment Transaction must not exceed USD 10,000 or its currency equivalent.
4. The Gaming Payment Transaction must not be processed to any type of Mastercard Corporate Card.
5. The following Anti-Money-Laundering (AML) requirements apply:
  - a. The Acquirer must consider its Merchants that submit Gaming Payment Transactions as higher risk under its anti-money laundering compliance program.
  - b. In addition to any requirement of applicable local law or regulation, including but not limited to, sanctions screening checks against the Office of Foreign Assets Control (OFAC) requirements and United Nations watch lists, the Acquirer must conduct enhanced customer due diligence reviews of any Merchant that submits Gaming Payment Transactions.
  - c. The Acquirer must ensure that each Merchant that submits Gaming Payment Transactions has appropriate controls in place to identify legitimate customers and to block suspicious activities, Cards, or Payment Transactions.
  - d. The Acquirer must have robust procedures and ongoing controls in place to monitor Transactions and Payment Transactions conducted by Merchants that submit Gaming Payment Transactions and to detect and report any potentially suspicious activity.
6. The Gaming Payment Transaction may be effected if not prohibited by applicable law or regulation and only for Cards issued in the United States Region.
7. U.S. state government-owned lottery Merchants and/or any of their agents must perform a Gaming Payment Transaction using a lottery point of redemption system.
8. An Issuer in the United States Region must technically support the Gaming Payment Transaction in authorization and clearing messages.
9. The Gaming Payment Transaction will not be authorized via Mastercard Stand-In or Down Option Services. Authorization is entirely under the control of the Issuer.



## Chapter 7 Terminal Requirements

*The following Standards apply with regard to POS Terminals, ATM Terminals, and Bank Branch Terminals. Where applicable, variations or additions by region and/or country are provided at the end of this chapter in the section titled, “Variations and Additions by Region.”*

7.1 Terminal Eligibility.....	204
7.2 Terminal Requirements.....	204
7.2.1 Terminal Function Keys for PIN Entry.....	205
7.2.2 Terminal Responses.....	206
7.2.3 Terminal Transaction Log.....	206
7.3 Contactless Payment Functionality.....	206
7.3.1 Contactless Reader Requirements.....	207
7.4 POS Terminal Requirements.....	207
7.4.1 Contactless-enabled POS Terminals.....	208
7.4.2 Contactless-only POS Terminals.....	209
7.4.3 Mobile POS (MPOS) Terminals.....	210
7.4.4 Mastercard Consumer-Presented QR-enabled POS Terminals.....	211
7.4.5 Signature-based Maestro POS Terminals.....	211
7.4.6 POS Terminals Using Electronic Signature Capture Technology (ESCT).....	211
7.5 ATM Terminal and Bank Branch Terminal Requirements.....	212
7.5.1 ATM Terminals.....	213
7.5.2 Bank Branch Terminals.....	213
7.5.3 Contactless Payment Functionality.....	213
7.6 Hybrid Terminal Requirements.....	213
7.6.1 Hybrid POS Terminal Requirements.....	214
Hybrid POS Terminal and Chip-only MPOS Terminal Displays.....	215
7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements.....	215
7.7 Mastercard Consumer-Presented QR Functionality.....	216
Variations and Additions by Region.....	216
Asia/Pacific Region.....	216
7.3 Contactless Payment Functionality.....	216
7.4 POS Terminal Requirements.....	217
7.4.3 Mobile POS (MPOS) Terminals.....	218
7.5 ATM Terminal and Bank Branch Terminal Requirements.....	218
7.6 Hybrid Terminal Requirements.....	219
Canada Region.....	219
7.3 Contactless Payment Functionality.....	219

7.4 POS Terminal Requirements.....	219
7.4.1 Contactless-enabled POS Terminals.....	219
7.4.3 Mobile POS (MPOS) Terminals.....	219
7.4.4 Mastercard Consumer-Presented QR-enabled POS Terminals.....	219
7.5 ATM Terminal and Bank Branch Terminal Requirements.....	220
Europe Region.....	220
7.1 Terminal Eligibility.....	220
7.2 Terminal Requirements.....	220
7.3 Contactless Payment Functionality.....	220
7.3.1 Contactless Reader Requirements.....	221
7.4 POS Terminal Requirements.....	221
7.4.1 Contactless-enabled POS Terminals.....	221
7.4.3 Mobile POS (MPOS) Terminals.....	224
7.4.5 Signature-based Maestro POS Terminals.....	225
7.5 ATM Terminal and Bank Branch Terminal Requirements.....	225
7.5.2 Bank Branch Terminals.....	226
7.6 Hybrid Terminal Requirements.....	226
7.6.1 Hybrid POS Terminal Requirements.....	226
7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements.....	226
Latin America and the Caribbean Region.....	227
7.3 Contactless Payment Functionality.....	227
7.4 POS Terminal Requirements.....	227
7.4.1 Contactless-enabled POS Terminals.....	228
7.6 Hybrid Terminal Requirements.....	228
Middle East/Africa Region.....	228
7.3 Contactless Payment Functionality.....	228
7.3.1 Contactless Reader Requirements.....	228
7.6 Hybrid Terminal Requirements.....	229
7.6.1 Hybrid POS Terminal Requirements.....	229
United States Region.....	229
7.3 Contactless Payment Functionality.....	229
7.4 POS Terminal Requirements.....	229
7.4.1 Contactless-enabled POS Terminals.....	229
7.4.3 Mobile POS (MPOS) Terminals.....	230
7.4.4 Mastercard Consumer-Presented QR-enabled POS Terminals.....	230
7.5 ATM Terminal and Bank Branch Terminal Requirements.....	230
7.6 Hybrid Terminal Requirements.....	230
Additional U.S. Region and U.S. Territory Rules.....	231
7.6 Hybrid Terminal Requirements.....	231

7.6.1 Hybrid POS Terminal Requirements..... 231

Hybrid POS Terminal and Chip-only MPOS Terminal Displays.....231

## 7.1 Terminal Eligibility

---

The following types of terminals, when compliant with the applicable technical requirements and other Standards, are eligible to be Terminals:

1. Any ATM Terminal or Bank Branch Terminal that is owned, operated or controlled by a Customer;
2. Any ATM Terminal that is owned, operated or controlled by an entity that is ineligible to be a Customer, provided that such ATM Terminal 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 or Association; and
4. Any other type of terminal which the Corporation may authorize.

A terminal that dispenses scrip is ineligible to be a Terminal.

**NOTE: A modification to this Rule appears in the “Europe Region” section at the end of this chapter.**

## 7.2 Terminal Requirements

---

Each Terminal must:

1. Have an online connection to the Acquirer host system for the authorization of Transactions, except where offline-only processing is specifically permitted by the Standards. 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 in accordance with the PIN security Standards.
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/IINs, 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 sentinel, and Longitudinal Redundancy Check (LRC), to ensure that the Card conforms to the technical specifications set forth in Appendix A of the *Security Rules and Procedures* manual. 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 English as well as the local language, as selected by the Cardholder. Two or more languages may be displayed simultaneously. In the Europe Region, operating instructions in French and German must also be available whenever technically feasible, and Spanish and Italian are recommended; 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.

Refer to the *Security Rules and Procedures* for additional requirements related to Terminal security, PIN processing, and use of service codes. Refer to Rule 3.9 for requirements relating to Terminal-generated Transaction receipts, including truncation of the primary account number (PAN).

**NOTE: A modification to this Rule appears in the "Europe Region" section at the end of this chapter.**

## 7.2.1 Terminal Function Keys for PIN Entry

A PIN-capable Terminal must have a numeric keyboard to enable the entry of PINs, with an 'enter key' function to indicate the completion of entry of a variable length PIN.

In all Regions except the Canada and United States Regions, a Terminal's PIN entry device (PED) or encrypting PIN pad (EPP) must accept PINs having four to six numeric characters. In the Canada and United States Regions, each PED and EPP must support PINs of up to 12 alphanumeric characters. It is recommended that all PEDs and EPPs support the input of PINs in letter-number combinations as follows:

1	Q, Z	6	M, N, O
2	A, B, C	7	P, R, S
3	D, E, F	8	T, U, V
4	G, H, I	9	W, X, Y
5	J, K, L		

The support of the following PED function keys 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**. In the Europe Region, this key is mandatory. The key must allow the Cardholder to cancel a Transaction prior to the final step that results in the submission of an authorization request.

### 7.2.2 Terminal Responses

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.

### 7.2.3 Terminal Transaction Log

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 may 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. The only exception to this Rule is for Merchant-approved Maestro POS Transactions, which may be logged until either the Transaction is authorized or the end of the 13-day period during which the Merchant may make attempts to obtain an authorization pursuant to the Standards, whichever occurs first.

When an attempted Transaction is rejected, an indication or reason for the rejection must be included on the Terminal Transaction log.

## 7.3 Contactless Payment Functionality

---

For purposes of this Rule, a "contactless-enabled" Terminal is any POS Terminal (including any MPOS Terminal), ATM Terminal, or Bank Branch Terminal with a contactless reader that is activated and that accepts Cards and Access Devices based on contactless magnetic stripe technology ("Magnetic Stripe Mode") and also optionally contactless chip technology ("EMV Mode").

Effective 12 October 2018, all newly-deployed POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes Cardholder-Activated Terminals (CATs), excludes Mobile POS (MPOS) Terminals, and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

Effective 18 October 2019, all newly-deployed MPOS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

Effective 1 April 2023, all POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes CATs and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

Refer to Rules 7.4.1, 7.4.2, 7.5, and 7.6.3 for additional contactless-enabled Terminal requirements. Refer to Rules 4.4 through 4.7 regarding Contactless Transaction processing.

**NOTE: Modifications to this Rule appear in the “Asia/Pacific Region,” “Canada Region,” “Europe Region,” “Latin America and the Caribbean Region,” “Middle East/Africa Region,” and “United States Region” sections at the end of this chapter.**

### 7.3.1 Contactless Reader Requirements

The reader of a contactless-enabled Terminal must:

- Comply with Mastercard Contactless Reader Specification Version 3.0 (MCL 3.0) or EMV CL Book C-2; and
- For POS Terminals only (including MPOS Terminals), be configured to support Consumer Device CVM (CDCVM) and the processing of Contactless Transactions that exceed the applicable Cardholder verification method (CVM) limit amount up to the amount that the same POS Terminal supports on its contact interface.

These requirements take effect:

- **1 January 2016** for any contactless-enabled Terminal submitted to the Corporation for M-TIP testing as a new project; and
- **1 January 2019** for all contactless-enabled Terminals.

Support of CDCVM is required only for Transactions that exceed the CVM limit.

**NOTE: Modifications to this Rule appear in the “Europe Region” and “Middle East/Africa Region” sections at the end of this chapter.**

## 7.4 POS Terminal Requirements

---

Each POS Terminal must comply with Rule 7.2, except contactless-only POS Terminals as described below and Mastercard Consumer-Presented QR-only POS Terminals. Each Merchant is responsible for the maintenance arrangements of its POS Terminals, unless the Acquirer undertakes this function.

For unattended POS Terminal requirements, refer to Rule 4.11. An unattended POS Terminal that accepts Mastercard Cards must comply with the Cardholder-Activated Terminal (CAT) requirements set forth in Appendix D.

Effective 12 October 2018, all newly-deployed POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes Cardholder-Activated Terminals (CATs), excludes Mobile POS (MPOS) Terminals, and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

Effective 1 April 2023, all POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes CATs and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

**NOTE: Modifications to this Rule appear in the “Asia/Pacific Region,” “Canada Region,” “Europe Region,” “Latin America and the Caribbean Region,” and “United States Region” sections at the end of this chapter.**

## 7.4.1 Contactless-enabled POS Terminals

A contactless-enabled POS Terminal must comply with the following. (Refer to the next table if a requirement to support MCL version 3.0 and Consumer Device CVM [CDCVM] applies.)

If the contact interface of the POS Terminal...	Then for Transactions exceeding the CVM limit (“high-value Transactions”), the contactless interface of the POS Terminal...
Supports online PIN	<ul style="list-style-type: none"> <li>• Must support online PIN;</li> <li>• If Mastercard is accepted, must support signature; and</li> <li>• May support CDCVM.</li> </ul>
Does not support online PIN	<p>Must be configured in accordance with one of the following:</p> <ol style="list-style-type: none"> <li>1. A high-value Transaction can only occur when a Mobile Payment Device is used and CDCVM was successful. For this configuration, CDCVM is the only CVM supported.</li> <li>2. A high-value Transaction can occur with signature as the CVM when Mastercard is accepted, and may also be able to occur when a Mobile Payment Device is used and CDCVM was successful. For this configuration, signature must be supported, and CDCVM may also be supported.</li> </ol>

The following applies:

- To any contactless-enabled POS Terminal deployed in a country or Region where a requirement to support MCL version 3.0 and CDCVM is currently in effect;



- In all other locations, to any contactless-enabled POS Terminal submitted to the Corporation for M-TIP testing as a new project on or after 1 January 2016; and
- Effective 1 January 2019, to all contactless-enabled POS Terminals.

If the contact interface of the POS Terminal...	Then for Transactions exceeding the CVM limit ("high-value Transactions"), the contactless interface of the POS Terminal...
Supports online PIN	<ul style="list-style-type: none"> <li>• Must support both online PIN and CDCVM; and</li> <li>• If Mastercard is accepted, must support signature.</li> </ul>
Does not support online PIN	<p>Must be configured in accordance with one of the following:</p> <ol style="list-style-type: none"> <li>1. A high-value Transaction can only occur when a Mobile Payment Device is used and CDCVM was successful. For this configuration, CDCVM is the only CVM supported.</li> <li>2. A high-value Transaction can occur with signature as the CVM when Mastercard is accepted, and may also be able to occur when a Mobile Payment Device is used and CDCVM was successful. For this configuration, both signature and CDCVM must be supported.</li> </ol>

Mastercard Rule 5.11.3, "Minimum/Maximum Transaction Amount Prohibited" applies to both the contact and contactless payment functionalities of a Dual Interface POS Terminal (whether attended or unattended).

**NOTE: Modifications to this Rule appear in the "Canada Region," "Europe Region," "Latin America and the Caribbean Region," and "United States Region" sections at the end of this chapter.**

## 7.4.2 Contactless-only POS Terminals

A POS Terminal that utilizes only contactless payment functionality, as permitted in accordance with Rule 4.7, must comply with all of the requirements set forth in Rule 7.4 except those applicable to contact magnetic stripe or chip 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. If Cards and Access Devices with contactless chip payment functionality are accepted, support both online and offline authorization.

### 7.4.3 Mobile POS (MPOS) Terminals

Any Merchant and any Customer or cash disbursement agent conducting Manual Cash Disbursement Transactions may use a Mobile POS (MPOS) Terminal that complies with the POS Terminal Standards.

Any Merchant may 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).

Only a Merchant with less than USD 100,000 in annual Mastercard POS Transaction Volume may use an MPOS Terminal with any of the following characteristics, for Mastercard 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.

Effective 18 October 2019, all newly-deployed MPOS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement applies regardless of Merchant Transaction Volume.

Effective 1 April 2023, all POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

All authorization and clearing messages for Transactions occurring at an MPOS Terminal must contain the MPOS acceptance device indicator, as follows:

- A value of 9 in DE 61 (Point-of-Service Data), subfield 10 (Cardholder-Activated Terminal Level) of the Authorization Request/0100 or Financial Transaction Request/0200 message; and
- A value of CT9 in PDS 0023 (Terminal Type) of the First Presentment/1240 message.

PIN verification, if supported by an MPOS Terminal, must be conducted by means of a PIN entry device (PED) that complies with section 4.10 of the *Security Rules and Procedures* manual.

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).

A Chip-only MPOS Terminal must use the following values:

- A value of 9 in DE 61 (Point-of-Service Data), Subfield 11 (POS Card Data Terminal Input Capability Indicator) in the Authorization Request/0100 or Financial Transaction Request/0200 message, as described in the *Customer Interface Specification* and *Single Message System Specifications* manuals; and

- A value of E in DE 22 (Point of Service Data Code), Subfield 1 (Terminal Data: Card Data Input Capability) of the First Presentment/1240 message, as described in the *IPM Clearing Formats* manual.

The Acquirer must comply with the MPOS Terminal requirements set forth in the *M/Chip Requirements* manual, the EMV chip specifications, and section 4.10 of the *Security Rules and Procedures* manual.

**NOTE: A modification to this Rule appears in the “Asia/Pacific Region,” “Canada Region,” “Europe Region,” and “United States Region” sections at the end of this chapter.**

#### 7.4.4 Mastercard Consumer-Presented QR-enabled POS Terminals

A Mastercard Consumer-Presented QR Transaction must be authorized online by the Issuer.

Mastercard Consumer-Presented QR-enabled POS Terminals must comply with the following:

- Must support purchase and refund Transactions. The requirement to support refunds using Mastercard Consumer-Presented QR payment is only applicable to attended Terminals.
- Terminal CVM processing is not supported for Mastercard Consumer-Presented QR Transactions.
- A Mastercard Consumer-Presented QR-enabled POS Terminal must operate in accordance with the *M/Chip Requirements for Contact and Contactless* manual and other Terminal-related specifications as provided by Mastercard.

The Acquirer must comply with the Mastercard Consumer-Presented QR Transaction requirements set forth in the *M/Chip Requirements for Contact and Contactless* manual and the *EMV QR Code Specification for Payments Systems-Consumer-Presented Mode* specifications.

An Acquirer may sponsor a Merchant that deploys POS Terminals that utilize only Mastercard Consumer-Presented QR functionality with the condition that, should the Merchant accept other forms of payment (e.g., contactless) for competing brands, the Merchant will also accept those forms of payment for Mastercard.

#### 7.4.5 Signature-based Maestro POS Terminals

**NOTE: A Rule on this subject appears in the “Europe Region” section at the end of this chapter.**

#### 7.4.6 POS Terminals Using Electronic Signature Capture Technology (ESCT)

An Acquirer that deploys POS Terminals using Electronic Signature Capture Technology (ESCT) must ensure the following:

- Proper electronic data processing (EDP) controls and security are in place, so that digitized signatures are recreated on a Transaction-specific basis. The Acquirer may recreate the signature captured for a specific Transaction only in response to a retrieval request for the Transaction.

- Appropriate controls exist over employees with authorized access to digitized signatures maintained in the Acquirer or Merchant host computers. Only employees and agents with a “need to know” should be able to access the stored, electronically captured signatures.
- The digitized signatures are not accessed or used in a manner contrary to the Standards.

## 7.5 ATM Terminal and Bank Branch Terminal Requirements

---

In addition to complying with Rule 7.2, each ATM Terminal and Bank Branch Terminal must:

1. Offer cash withdrawals from an Account;
2. Offer balance inquiry functionality to Cardholders, if balance inquiry functionality is offered to cardholders of any other network accepted at that ATM Terminal or Bank Branch Terminal;
3. During Account selection, include the word “Savings” when offering a cash withdrawal or transfer from a savings account, and the word “Checking” or “Chequing” when offering a cash withdrawal or transfer from a checking account;
4. Not automatically generate an online reversal for the full or partial amount of any authorized cash withdrawal or disbursement when the ATM Terminal or Bank Branch Terminal indicates that such Transaction was not completed because the Cardholder failed to collect some or all of the cash dispensed;
5. Have an online connection to the Acquirer host system;
6. Encrypt the PIN at the point of entry and send the PIN to the Acquirer host system in encrypted form, in accordance with the PIN security Standards;
7. Process each Transaction in the currency dispensed by the Terminal during that Transaction. Terminals may process Transactions in other currencies only if done in accordance with “POI Currency Conversion” in Chapter 3, except that a withdrawal of foreign currency may be processed in the issuing currency of the Card if it is the same as the currency of the country where the Terminal is located. The amount of currency dispensed, Transaction amount, and conversion rate must be shown on the screen before the Cardholder completes the Transaction and must also be included on the Transaction receipt.

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.

An ATM Terminal or Bank Branch Terminal also:

1. May offer Merchandise Transactions from no account specified; and
2. May offer MoneySend Payment Transactions.

Refer to Chapter 4 of the *Security Rules and Procedures* manual for PIN entry device and PIN security requirements.

**NOTE: Additions and/or variations to this Rule appear in the “Asia/Pacific Region,” “Canada Region,” “Europe Region,” and “United States Region” sections at the end of this chapter.**

### 7.5.1 ATM Terminals

In addition to complying with Rule 7.5, an ATM Terminal must permit the Cardholder to obtain the equivalent of USD 100 in the currency in use at the ATM Terminal per Transaction, subject to authorization of the Transaction by the Issuer.

Refer to Chapter 4 for additional requirements.

### 7.5.2 Bank Branch Terminals

In addition to complying with Rule 7.5, a Bank Branch Terminal must:

1. Be approved in writing by the Corporation to have access to the Interchange System;
2. With respect to Maestro and Cirrus acceptance, accept all Maestro and Cirrus Cards. A bank branch offering the service must display the Maestro and Cirrus Acceptance Marks on the door or window, and at the counter where the service is provided. With respect to Mastercard acceptance, refer to Rule 4.15.4, Mastercard Acceptance Mark Must be Displayed;
3. Clearly describe by Transaction receipt, screen information, or both the action taken in response to a Cardholder's request. It is recommended that the bank branch address also be printed on the Transaction receipt;
4. With respect to Maestro and Cirrus acceptance, permit the Cardholder to obtain the equivalent of USD 200 in the currency in use at the Bank Branch Terminal per Transaction, subject to authorization of the Transaction by the Issuer. With respect to Mastercard acceptance, refer to Rule 4.15.2, Maximum Cash Disbursement Amounts. The currency may be dispensed in local currency or another currency, provided the Cardholder is informed of the currency that will be dispensed before the Transaction is performed. The Transaction receipt, if provided, must identify the currency dispensed.

**NOTE: Refer to Rule 4.15 for additional Mastercard Manual Cash Disbursement Transaction requirements. An addition to this Rule appears in the "Europe Region" section at the end of this chapter.**

### 7.5.3 Contactless Payment Functionality

Online PIN must be the only CVM supported for Contactless Transactions effected:

- At a Dual Interface ATM Terminal with a Mastercard, Maestro, or Cirrus Card or Access Device; or
- At a Bank Branch Terminal with a Maestro or Cirrus Card or Access Device.

## 7.6 Hybrid Terminal Requirements

---

In addition to complying with Rule 7.2, 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 EMV-compliant Payment Applications for each of the Corporation's brands accepted at that location when a Card containing any such Payment Application is presented, if the Hybrid Terminal reads and processes any other EMV-compliant payment application; and
4. Request a cryptogram for all chip-read Transactions; 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 Corporation to be a magnetic stripe-only Terminal, and must be identified in Transaction messages as such.

Chip Transactions must be processed in accordance with the *MI/Chip Requirements for Contact and Contactless* manual, the *Security Rules and Procedures* manual, and other applicable technical specifications. In particular, refer to:

- The *Security Rules and Procedures* manual for Hybrid Terminal security and PIN processing requirements;
- The *MI/Chip Requirements for Contact and Contactless* manual for technical fallback, Cardholder verification method (CVM) fallback, and Card authentication method (CAM) support requirements; and
- The *Chargeback Guide* for information about Intracountry Transaction and Intraregional Transaction chip liability shifts and the Global Chip Liability Shift Program for Interregional Transactions.

**NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," and "United States Region" sections at the end of this chapter.**

### 7.6.1 Hybrid POS Terminal Requirements

In addition to complying with Rule 7.6, a Hybrid POS Terminal must:

1. At a minimum, support online authorization.
2. If Maestro Cards are accepted, support both online and offline PIN as the CVM. On a country-by-country basis, Mastercard may permit Acquirers to, at a minimum, support offline PIN as the CVM as outlined in Rule 3.1.5.
3. Perform Terminal offline chip authorization limit and Card velocity checking. Transactions above the Terminal offline chip authorization limit programmed in the POS Terminal must be routed online to the Issuer, as indicated by the authorization request cryptogram (ARQC).
4. Support online mutual authentication (OMA) and script processing if connected to a debit acquiring network.
5. If offline Transactions are supported, identify all offline Transactions as such to the Issuer when submitted for clearing and settlement.

A Hybrid POS Terminal is identified in Transaction messages with the following values:

- A value of 3, 5, 8, or 9 in DE 61 (Point-of-Service Data), Subfield 11 (POS Card Data Terminal Input Capability Indicator) in the Authorization Request/0100 or Financial Transaction Request/0200 message, as described in the *Customer Interface Specification* and *Single Message System Specifications* manuals; and
- A value of 5, C, D, E, or M in DE 22 (Point of Service Data Code), Subfield 1 (Terminal Data: Card Data Input Capability) of the First Presentment/1240 message, as described in the *IPM Clearing Formats* manual.

A PIN-capable Hybrid POS Terminal is indicated when in addition, DE 22, Subfield 2 (Terminal Data: Cardholder Authentication Capability), of the First Presentment/1240 message contains a value of 1.

A chip-capable POS Terminal that does not satisfy all of the requirements to be a Hybrid POS Terminal is deemed by the Corporation to be a magnetic stripe-only POS Terminal and must be identified in Transaction messages as such.

**NOTE: Additions to this Rule appear in the “Europe Region” and “Middle East/Africa Region” sections at the end of this chapter.**

### 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.
3. Display to the Cardholder the Transaction amount and Transaction currency, if different from the Merchant’s or cash disbursement agent’s local currency.

**NOTE: A modification to this Rule appears in the “Additional U.S. Region and U.S. Territory Rules” section at the end of this chapter.**

## 7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements

In addition to complying with Rule 7.6, each Hybrid ATM Terminal 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. Offline authorization by means of the chip, for a technical or any other reason, is not permitted;
2. Support online PIN as the CVM for all ATM Transactions and for all Manual Cash Disbursement Transactions effected with a Maestro or Cirrus Card;
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 for all products they accept;

- c. Attempting to match all AIDs contained in the ATM Terminal or Bank Branch Terminal with those on any EMV-compliant Chip Card used;
- d. Displaying all matching application labels or preferred names to the Cardholder, except when the Standards permit a compatible product or application to take priority;
- e. Allowing the Cardholder to select the application to be used when multiple matching applications exist, except when the Standards permit a compatible product or application to take priority; and
- f. Providing the Cardholder the option of approving or canceling a Merchandise Transaction before the products are dispensed or the services are performed.

**NOTE: An addition to this Rule appears in the “Europe Region” section at the end of this chapter.**

## 7.7 Mastercard Consumer-Presented QR Functionality

---

A Terminal may be deployed with Mastercard Consumer-Presented QR payment functionality. For the purpose of this Rule, a “Mastercard Consumer-Presented QR-enabled” Terminal is any attended or unattended POS Terminal (including any MPOS Terminal) with a QR Code reader that is activated and can effect a Transaction through the presentment of a QR Code by the Cardholder and capture of the QR Code by the Merchant to initiate a Transaction.

## Variations and Additions by Region

---

The remainder of this chapter provides modifications to the Standards set out in this chapter. The modifications are organized by region or country and by applicable subject title.

### Asia/Pacific Region

---

The following modifications to the Rules apply in the Asia/Pacific Region or in a particular Region country or countries. Refer to Appendix A for the Asia/Pacific Region geographic listing.

#### 7.3 Contactless Payment Functionality

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

A contactless-enabled Terminal may support:

- Contactless magnetic stripe technology (“Magnetic Stripe Mode”) only;
- Both contactless magnetic stripe and contactless chip technology (“EMV Mode”); or
- EMV mode only.

Effective 1 April 2023, all POS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This



requirement includes CATs and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

In **Indonesia**, the Rule on this subject is modified as follows.

Effective 12 October 2018, all newly-deployed POS Terminals must be Dual Interface Hybrid Terminals that support EMV contact payment functionality. This requirement includes Cardholder-Activated Terminals (CATs), excludes Mobile POS (MPOS) Terminals, and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

Effective 18 October 2019, all newly-deployed MPOS Terminals must be Dual Interface Hybrid Terminals that support and enable EMV contact payment functionality.

Effective 12 October 2020, all newly-deployed POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes CATs, excludes MPOS Terminals, and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

Effective 12 October 2020, all newly-deployed MPOS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

In **Japan**, the Rule on this subject is modified as follows.

All newly-deployed POS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes CATs, excludes MPOS Terminals, and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

All newly-deployed MPOS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

In the **Republic of Korea**, the Rule on this subject is modified as follows.

Effective 12 October 2020, all newly-deployed POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes CATs, excludes MPOS Terminals, and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

Effective 18 October 2020, all newly-deployed MPOS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

## 7.4 POS Terminal Requirements

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

Effective 1 April 2023, all POS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes CATs and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

In **Indonesia**, the Rule on this subject is modified as follows.

Effective 12 October 2020, all newly-deployed POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes CATs, excludes MPOS Terminals, and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

In **Japan**, the Rule on this subject is modified as follows.

All newly-deployed POS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes CATs, excludes MPOS Terminals, and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

In the **Republic of Korea**, the Rule on this subject is modified as follows.

Effective 12 October 2020, all newly-deployed POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement includes CATs, excludes MPOS Terminals, and excludes contactless-only acceptance as described in Rule 4.7 of this manual.

### **7.4.3 Mobile POS (MPOS) Terminals**

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

Effective 1 April 2023, all MPOS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

In **Indonesia**, the Rule on this subject is modified as follows.

Effective 12 October 2020, all newly-deployed MPOS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement applies regardless of Merchant Transaction Volume.

In **Japan**, the Rule on this subject is modified as follows.

All newly-deployed MPOS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

In the **Republic of Korea**, the Rule on this subject is modified as follows.

Effective 12 October 2020, all newly-deployed MPOS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality. This requirement applies regardless of Merchant Transaction Volume.

## **7.5 ATM Terminal and Bank Branch Terminal Requirements**

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

An Acquirer must ensure that each of its ATM Terminals and Bank Branch Terminals offer:

1. Cash withdrawals from savings accounts and checking accounts;
2. Cash advances from a credit card; and
3. Balance inquiry for checking accounts, savings accounts, and credit cards.

## 7.6 Hybrid Terminal Requirements

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

All new Terminals deployed by Region Customers and capable of accepting Chip Cards (credit or debit) must be EMV-compliant.

## Canada Region

---

The following modifications to the Rules apply in the Canada Region. Refer to Appendix A for the Canada Region geographic listing.

### 7.3 Contactless Payment Functionality

In the Canada Region, the Rule on this subject is modified as follows.

All POS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

### 7.4 POS Terminal Requirements

In the Canada Region, the Rule on this subject is modified as follows.

All POS Terminals, including CATs, may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

#### 7.4.1 Contactless-enabled POS Terminals

In the Canada Region, the Rule on this subject is modified to add the following:

An Acquirer must ensure that any contactless-enabled POS Terminal that is newly deployed on or after 1 January 2016 transmits the device type indicator in DE 48, subelement 23 (Payment Initiation Channel), subfield 1 (Device Type) of authorization messages when present in the Card or Access Device used to effect a Transaction. The Acquirer must also include the device type indicator, when present, in PDS 0198 (Device Type Indicator) of First Presentment/1240 messages.

#### 7.4.3 Mobile POS (MPOS) Terminals

In the Canada Region, the Rule on this subject is modified as follows.

All POS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

#### 7.4.4 Mastercard Consumer-Presented QR-enabled POS Terminals

In the Canada Region, the Rule on this subject is modified to add the following:

An Acquirer must transmit the device type indicator in DE 48, subelement 23 (Payment Initiation Channel), subfield 1 (Device Type) of the Authorization Request/0100 message or Financial Transaction Request/0200 message when present in the Access Device used to effect

a Transaction. The Acquirer must also include the device type indicator, when present, in PDS 0198 (Device Type Indicator) of the First Presentment/1240 message.

## 7.5 ATM Terminal and Bank Branch Terminal Requirements

In the Canada Region, the Rule on this subject is modified as follows.

An Acquirer must ensure that each of its ATM Terminals and Bank Branch Terminals:

1. Offer cash withdrawal from a savings and checking (or chequing) accounts;
2. Offer cash advances from a credit card.
3. If offered via a Competing ATM Network, offer balance inquiry to a savings account, checking account, and/or credit card account, and transfers from checking to savings and from savings to checking accounts.
4. If cash withdrawals not requiring account selection are performed, convert the Transaction to a withdrawal from no account specified.

An ATM Terminal or Bank Branch Terminal may offer cash withdrawals from no account specified.

## Europe Region

---

The following modifications to the Rules apply in the Europe Region or in a particular Region country or countries. Refer to Appendix A for the Europe Region, Non-Single European Payments Area (Non-SEPA) and Single European Payments Area (SEPA) geographic listing.

### 7.1 Terminal Eligibility

In the EEA, the Rule on this subject is modified as follows.

Terminals may be connected to any switch of the Customer's choice that is registered with the Corporation.

### 7.2 Terminal Requirements

In the EEA, the Rule on this subject is modified as follows.

A Terminal must not perform tests or edits on Track 1 data for the purpose of disqualifying Cards from eligibility for processing by the registered switch of the Acquirer's choice.

### 7.3 Contactless Payment Functionality

In the Europe Region, the Rule on this subject is modified as follows.

A contactless-enabled Terminal may support:

- Contactless magnetic stripe technology ("Magnetic Stripe Mode") only;
- Both contactless magnetic stripe and contactless chip technology ("EMV Mode"); or
- EMV mode only.

Effective 13 October 2017, a newly deployed contactless-enabled Terminal must support EMV Mode Contactless Transactions.

Effective 1 January 2020, all contactless-enabled Terminals must support EMV Mode Contactless Transactions.

Effective 1 January 2020, all newly-deployed contactless-enabled Terminals must only support EMV Mode Contactless Transactions and must not support Magnetic Stripe Mode Contactless Transactions.

### **7.3.1 Contactless Reader Requirements**

All contactless-enabled Terminals, including MPOS Terminals, deployed in a Europe Region country must support Mastercard Contactless Reader Specification version 3.0 (MCL 3.0) or above.

In the EEA, the Rule on this subject is modified as follows.

A POS Terminal that is required to support Mastercard Contactless Reader Specification version 3.0 (MCL 3.0) or above pursuant to this Rule must support a level of contactless functionality equivalent to MCL 3.0 or above.

## **7.4 POS Terminal Requirements**

The following requirements apply in **Greece**:

1. A POS Terminal must be configured to require entry of the Transaction amount before the Card or Access Device is swiped, dipped, or tapped.
2. A POS Terminal deployed at a Merchant location where a gratuity may be added (such as a bar, restaurant, hotel, or taxi) must contain an automated prompt to the Cardholder to add the gratuity before the authorization request is submitted. This requirement applies for the addition of a gratuity to all types of Transactions.

The following requirements apply in **Hungary**:

An Acquirer that has deployed at least 250 POS Terminals in Hungary, or that has at least two percent (2%) of the domestic POS acquiring Volume, must technically support the selection of the different voucher types for government-defined employee benefit programs, such as accommodation, catering, and recreation voucher types, at Merchant locations offering the types of goods and/or services that may be purchased under the employee benefit program. The voucher types apply for prepaid Cards issued under a meal/food voucher product code, such as MRJ. The Volume percentage must be calculated by the Acquirer twice per year on the basis of the Hungarian National Bank half-yearly report.

### **7.4.1 Contactless-enabled POS Terminals**

In the Europe Region, the Rule on this subject is modified as follows.

#### **Contactless Enablement**

The Acquirer of a Merchant located in the Europe Region (excluding countries where a country-specific mandate is set out below) must ensure that:

- All new and all upgraded POS Terminals (including MPOS Terminals) deployed on or after 1 January 2016 are contactless-enabled; and
- Effective 1 January 2020, all existing POS Terminals (including MPOS Terminals) are contactless-enabled.

The Acquirer of a Merchant located in...	Must ensure that all <b>new and upgraded POS Terminals</b> (including MPOS Terminals) are contactless-enabled if deployed on or after:	Must ensure that all <b>existing POS Terminals</b> (including MPOS Terminals) are contactless-enabled as of:
Belarus	1 January 2017	1 January 2020
Bulgaria	1 July 2015	1 July 2018
Estonia	1 January 2017	1 January 2020
Germany	1 January 2015	1 January 2018
Hungary	1 July 2014	1 July 2017
Latvia	1 January 2017	1 January 2020
Lithuania	1 January 2017	1 January 2020
Montenegro	1 July 2015	1 July 2018
Romania	1 July 2015	1 July 2018
Serbia	1 July 2015	1 July 2018
Slovenia	1 January 2016	1 January 2019
Sweden	1 January 2017	1 January 2020
Turkey	1 July 2014	1 July 2017

The Acquirer of a Merchant located in **Czech Republic** or **Slovakia** with an annual Transaction Volume of more than USD 100,000 must ensure that:

- All new and all upgraded POS Terminals (including MPOS Terminals) deployed on or after 1 July 2014 are contactless-enabled; and
- As of 1 July 2017, all existing POS Terminals (including MPOS Terminals) are contactless-enabled.

The Acquirer of a Merchant located in **Poland** must ensure that:

- All new, upgraded, and replacement POS Terminals (including MPOS Terminals) deployed on or after 1 January 2018 are contactless-enabled; and
- As of 1 January 2018, all existing POS Terminals (including MPOS Terminals) are contactless-enabled.

The Acquirer of a Merchant located in **Italy** and identified with one of the following Card acceptor business codes (MCCs) must ensure that:

- All new, upgraded, and replacement POS Terminals deployed at the Merchant's locations on or after 1 January 2014 are contactless-enabled and support MCL 3.0 or later; and
- As of 1 January 2017, all existing POS Terminals at the Merchant's locations are contactless-enabled.

<b>MCC</b>	<b>Description</b>
5310	Discount Stores
5311	Department Stores
5411	Grocery Stores, Supermarkets
5499	Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores
5541	Service Stations (with or without Ancillary Services)
5651	Family Clothing Stores
5661	Shoe Stores
5691	Men's and Women's Clothing Stores
5699	Accessory and Apparel Stores—Miscellaneous
5719	Miscellaneous House Furnishing Specialty Shops
5722	Household Appliance Stores
5812	Eating Places, Restaurants
5813	Bars, Cocktail Lounges, Discotheques, Nightclubs, and Taverns—Drinking Places (Alcoholic Beverages)
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5942	Book Stores
5977	Cosmetic Stores
7230	Barber and Beauty Shops
7523	Automobile Parking Lots and Garages
7832	Motion Picture Theaters

### **MCL 3.0 and CDCVM Support**

The contactless reader of a POS Terminal that is deployed at a Merchant newly adopting contactless payment functionality on or after 1 January 2014 must support Mastercard Contactless Reader Specification version 3.0 (MCL 3.0) or later. A Merchant that has deployed any contactless-enabled POS Terminals before 1 January 2014 may support an earlier MCL version with respect to contactless-enabled POS Terminals that are deployed, upgraded, or replaced at its existing and new Merchant locations.

An attended or unattended POS Terminal that supports MCL 3.0 must support Consumer Device CVM (CDCVM) in addition to any other CVM specified in the Rules.

Refer to Rule 7.3.1 in this Europe Region section for additional MCL 3.0 support requirements.

### **Online PIN Support**

As of 1 January 2016, an Acquirer deploying new contactless-enabled POS Terminals in Finland, France, Ireland, and the United Kingdom must not support online PIN on the contactless interface. As of 1 March 2019, an Acquirer deploying new contactless-enabled POS Terminals in Israel must not support online PIN on the contactless interface. In these countries, Contactless Transactions cannot be completed above the CVM limit, except with an Access Device supporting CDCVM when used at a contactless-enabled POS Terminal supporting MCL 3.0 (or later).

An Acquirer deploying new contactless-enabled POS Terminals in all other Europe Region countries except Estonia, Latvia and Lithuania must support online PIN on the contactless interface. In such countries, all contactless-enabled Access Devices can be accepted above the CVM limit.

Effective 1 July 2019, all POS Terminals deployed in Iceland must support online PIN on the contactless interface.

Prior to 1 January 2020, an Acquirer in Estonia, Latvia, or Lithuania may deploy new contactless-enabled POS Terminals that either support or do not support online PIN on the contactless interface. Effective 1 January 2020, all new POS Terminals deployed in Estonia, Latvia, and Lithuania must support online PIN on the contactless interface.

### **7.4.3 Mobile POS (MPOS) Terminals**

In the Europe Region, the Rule on this subject is modified as follows.

A Merchant may use an MPOS Terminal that supports only Contact Chip Transactions and Contactless Transactions and does not support magnetic stripe Transactions.

The following Rule applies in the EEA:

An MPOS Terminal, including any Chip-only MPOS Terminal, must be identified in authorization and clearing messages as specified by the registered switch of the Customer's choice.



### 7.4.5 Signature-based Maestro POS Terminals

A “signature-based Maestro POS Terminal” is a POS Terminal with no online PIN capability and which therefore uses signature as the CVM for magnetic stripe-based Transactions and Chip Transactions effected with Cards that do not support offline PIN. The following requirements apply to signature-based Maestro POS Terminals:

1. If the signature is unsatisfactory, the Merchant must be able to indicate the cancellation of the Transaction to the POS Terminal, or perform a refund;
2. In case of temporary printer malfunction, the POS Terminal should be able to reprint the receipt, preferably including a duplicate statement, without repeating the Transaction process;
3. The POS Terminal must be designed to protect the Cardholder from deception with regard to:
  - a. The fact that no PIN is required;
  - b. The normal sequence of Transaction steps;
  - c. The information printed or displayed;
  - d. Additional data requested;
  - e. The authorization response;
  - f. The completion or cancellation of the Transaction.

### 7.5 ATM Terminal and Bank Branch Terminal Requirements

In the Europe Region, the Rule on this subject is modified as follows.

1. Each ATM Terminal and Bank Branch Terminal must be capable of dispensing, without limit per Transaction, the authorized amount requested by the Cardholder unless for technical and/or security considerations/constraints, the amount per Transaction is limited to at least the equivalent of EUR 200 in local currency.
2. For Domestic Transactions in **Ukraine**, each ATM Terminal must be capable of dispensing the authorized amount requested by the Cardholder, or at least UAH 1000 per Transaction. An Acquirer may limit the number of cash withdrawal Domestic Transactions per day, provided that the limit is not less than three Transactions per Card per day.
3. Transfers from one account to another and account selection are not currently supported in the Europe Region.
4. It is strongly recommended that an Acquirer in the Europe Region support and offer domestic, inter-European, and intra-European balance inquiry and PIN change and unblock functionality at all of its ATM Terminals. The Acquirer must ensure that the balance amount is not provided by the ATM Terminal before the Cardholder’s PIN has been entered. The recommendation to support PIN change and unblock functionality applies in relation to Chip Cards only.

An Acquirer must offer balance inquiry and/or PIN change/unblock functionality to Cardholders if it offers these services to the cardholders of any other network accepted at the ATM Terminal, ensuring equal treatment according to the Card category (for example, debit, credit).

5. Except when a Transaction was not completed because the Cardholder failed to collect some or all of the cash dispensed, the Acquirer must send a reversal or partial reversal within 60 seconds of receiving the authorization response at the Acquirer host system when a Transaction fails to complete.

### 7.5.2 Bank Branch Terminals

In the Europe Region, the Rule on this subject is modified as follows.

An Issuer is required to support and an Acquirer may optionally support Transactions effected with a Bank Branch Terminal.

## 7.6 Hybrid Terminal Requirements

In the Europe Region, the Rule on this subject is modified as follows.

1. At a Hybrid ATM Terminal, if the Card also supports EMV chip technology, the Transaction must be completed using the chip. Technical fallback to magnetic stripe is not permitted.
2. Technical fallback is permitted at Hybrid POS Terminals and Hybrid Bank Branch Terminals. When technical fallback occurs, PIN must be used as the CVM. An Acquirer may withdraw support for technical fallback at attended POS Terminals and Bank Branch Terminals when the Acquirer is content that technical fallback support is no longer required to ensure good customer service. Upon doing so, the Acquirer must ensure that the POS Terminal or Bank Branch Terminal continues to support magnetic stripe Card acceptance.
3. All Terminals deployed within SEPA must support both magnetic stripe and EMV chip technology.
4. All Terminals deployed in **Albania, Bosnia and Herzegovina, Kosovo, Macedonia, Moldova, Montenegro, or Serbia** must support both magnetic stripe and EMV chip technology.

### 7.6.1 Hybrid POS Terminal Requirements

In the Europe Region, the Rule on this subject is modified as follows.

1. CVM fallback from PIN to signature on a Chip Transaction conducted with a Maestro Card is not permitted.
2. All Hybrid POS Terminals deployed within **SEPA** must support the use of PIN as the CVM for intra-SEPA Chip Transactions conducted with Mastercard Cards.

All Hybrid POS Terminals deployed in **Albania, Bosnia and Herzegovina, Kosovo, Macedonia, Moldova, Montenegro, and Serbia** must support the use of PIN as the CVM for Chip Transactions conducted with a Mastercard Card.

In the EEA, the Rule on this subject is modified as follows.

A Hybrid POS Terminal and a PIN-capable Hybrid POS Terminal must be identified in authorization and clearing messages as specified by the registered switch of the Customer's choice.

### 7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements

In the Europe Region, the Rule on this subject is modified as follows.

Effective 22 January 2021, all newly deployed ATM Terminals in the **Czech Republic** and **Poland** must be contactless-enabled.

Effective 19 January 2024, all ATM Terminals in the **Czech Republic** and **Poland** must be contactless-enabled.

Where a Hybrid ATM Terminal or Hybrid Bank Branch Terminal supports more than one payment application residing on a Chip Card (for example, the Cirrus Payment Application and a stored value payment application), the Cardholder must be permitted to choose the preferred payment application.

## Latin America and the Caribbean Region

---

The following modifications to the Rules apply in the Latin America and the Caribbean Region. Refer to Appendix A for the Latin America and the Caribbean Region geographic listing.

### 7.3 Contactless Payment Functionality

In the Latin America and the Caribbean Region, the Rule on this subject is modified as follows.

A contactless-enabled Terminal may support:

- Contactless magnetic stripe technology (“Magnetic Stripe Mode”) only;
- Both contactless magnetic stripe and contactless chip technology (“EMV Mode”); or
- EMV mode only.

All newly-deployed integrated POS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

Effective 16 October 2020, all newly-deployed integrated POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

For the purposes of this Rule, an integrated POS Terminal refers to acceptance architectures where the Merchant’s POS solution is integrated with the Card-reading technology. They are typically deployed by large Merchant chains and stores. This definition may include automated fuel dispenser Terminals that have integrated payment functionality, although it does not include any devices that can be deployed as stand-alone payment Terminals.

### 7.4 POS Terminal Requirements

In the Latin America and the Caribbean Region, the Rule on this subject is modified as follows.

Effective 16 October 2020, all newly-deployed integrated POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

For the purposes of this Rule, an integrated POS Terminal refers to acceptance architectures where the Merchant’s POS solution is integrated with the Card-reading technology. They are

typically deployed by large Merchant chains and stores. This definition may include automated fuel dispenser Terminals that have integrated payment functionality, although it does not include any devices that can be deployed as stand-alone payment Terminals.

#### **7.4.1 Contactless-enabled POS Terminals**

In the Latin America and the Caribbean Region, the Rule on this subject is modified as follows. A contactless-enabled POS Terminal deployed in Brazil, Chile, or Colombia must minimally support online PIN and may also support Consumer Device CVM (CDCVM) as the CVM for a Maestro Contactless Transaction that exceeds the applicable contactless CVM limit.

In Brazil, the following requirements apply:

1. A contactless-enabled POS Terminal must support online PIN as the CVM for a Maestro Magnetic Stripe Mode Contactless Transaction that exceeds BRL 50; and
2. For Domestic Transactions, if the Cardholder selects the “debit” option when using a Mastercard Card or Access Device to initiate a Contactless Transaction, Mastercard® Single Message System processing requirements and the chargeback procedures in Chapter 4 of the *Chargeback Guide* will apply. The resulting Transaction is referred to as a Maestro Magnetic Stripe Mode Contactless Transaction.

#### **7.6 Hybrid Terminal Requirements**

In the Latin America and the Caribbean Region, the Rule on this subject is modified as follows.

All Terminals that are newly deployed within the Region must be EMV-compliant.

## **Middle East/Africa Region**

---

The following modifications to the Rules apply in the Middle East/Africa Region. Refer to Appendix A for the Middle East/Africa Region geographic listing.

### **7.3 Contactless Payment Functionality**

In the Middle East/Africa Region, the Rule on this subject is modified as follows.

A contactless-enabled Terminal may support:

- Contactless magnetic stripe technology (“Magnetic Stripe Mode”) only;
- Both contactless magnetic stripe and contactless chip technology (“EMV Mode”); or
- EMV mode only.

#### **7.3.1 Contactless Reader Requirements**

In the Middle East/Africa Region, the Rules on this subject take effect:

- 1 July 2015 for any contactless-enabled Terminal submitted to the Corporation for M-TIP testing as a new project; and
- 1 July 2017 for all contactless-enabled Terminals.

## 7.6 Hybrid Terminal Requirements

### 7.6.1 Hybrid POS Terminal Requirements

In the Middle East/Africa Region, the Rule on this subject is modified as follows.

All new or retrofitted Terminals deployed by Region Customers must be capable of upgrade to EMV compliance.

## United States Region

---

The following modifications to the Rules apply in the United States (U.S.) Region. Refer to Appendix A for the U.S. Region geographic listing.

## 7.3 Contactless Payment Functionality

In the United States Region, the Rule on this subject is modified as follows.

All POS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

Prior to 18 October 2019, a newly deployed contactless-enabled Terminal may support Magnetic Stripe Mode contactless payment functionality.

Effective 18 October 2019:

- A newly-deployed POS Terminal that supports contactless acceptance must support only EMV mode contactless. Magstripe mode contactless must not be supported.
- A POS Terminal that accepts Mastercard and Maestro as well as supports contactless acceptance for competing brands, must enable Mastercard and Maestro on the contactless interface.

Effective 1 April 2023, all POS Terminals that support contactless acceptance must support only EMV mode contactless. Magstripe mode contactless must not be supported.

## 7.4 POS Terminal Requirements

In the United States Region, the Rule on this subject is modified as follows.

All POS Terminals, including CATs, may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

### 7.4.1 Contactless-enabled POS Terminals

In the U.S. Region, the Acquirer of a Merchant that uses a contactless-enabled POS Terminal must comply with all of the following:

1. **MCL Version 3.0**—The contactless reader of a newly deployed contactless-enabled POS Terminal must support MCL version 3.0 or later.
2. **Device Type Indicator**—An Acquirer must ensure that any newly deployed contactless-enabled POS Terminal transmits the device type indicator in DE 48, subelement 23

(Payment Initiation Channel), subfield 1 (Device Type) of authorization messages when present in the Card or Access Device used to effect a Transaction. The Acquirer must also include the device type indicator, when present, in PDS 0198 (Device Type Indicator) of First Presentment/1240 messages.

3. **CVM Support**—A contactless-enabled POS Terminal deployed in the U.S. Region must minimally support online PIN as the CVM for a Maestro Contactless Transaction that exceeds the applicable contactless CVM limit. Any newly deployed or replacement contactless-enabled POS Terminal must also support Consumer Device CVM (CDCVM).

#### **7.4.3 Mobile POS (MPOS) Terminals**

In the United States Region, the Rule on this subject is modified as follows.

All POS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

#### **7.4.4 Mastercard Consumer-Presented QR-enabled POS Terminals**

In the U.S. Region, the Rule on this subject is modified to add the following:

An Acquirer must transmit the device type indicator in DE 48, subelement 23 (Payment Initiation Channel), subfield 1 (Device Type) of the Authorization Request/0100 message or the Financial Transaction Request/0200 message when present in the Access Device used to effect a Transaction. The Acquirer must also include the device type indicator, when present, in PDS 0198 (Device Type Indicator) of the First Presentment/1240 message.

### **7.5 ATM Terminal and Bank Branch Terminal Requirements**

In the U.S. Region, the Rule on this subject is modified as follows:

1. An ATM Terminal or Bank Branch Terminal must:
  - a. Offer cash withdrawals from savings and checking accounts and cash advances from credit cards;
  - b. Offer balance inquiry for checking accounts, savings accounts, and credit cards;
  - c. Offer transfers from checking to savings accounts and from savings to checking accounts;
  - d. Offer Shared Deposit to savings accounts and checking accounts if the ATM Terminal or Bank Branch Terminal accepts shared deposits for any other shared deposit service; and
  - e. Convert a cash withdrawal performed without account selection to a withdrawal from no account specified.
2. An ATM Terminal or Bank Branch Terminal may offer:
  - a. Cash withdrawals from no account specified; and
  - b. Shared Deposit to savings and checking accounts if the Terminal does not accept shared deposits for any other shared deposit service.

### **7.6 Hybrid Terminal Requirements**

In the U.S. Region, the Rule on this subject is modified as follows.

A Hybrid Terminal deployed in the U.S. Region must be configured as online-only or online-preferring for both Contact Chip Transaction and Contactless Transaction processing. "Online-only" means that the Hybrid Terminal seeks online authorization for all Transactions. "Online-preferring" means that the Hybrid Terminal seeks an online authorization for all Transactions, but may approve a Transaction that does not exceed the applicable Terminal offline chip authorization limit when in the "unable to go online" mode. This may occur when the Terminal temporarily loses online connectivity or does not receive an authorization response from the Issuer. For more information, refer to *M/Chip Requirements for Contact and Contactless*.

## Additional U.S. Region and U.S. Territory Rules

---

The following modifications to the Rules apply in the United States Region and in American Samoa, Guam, Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands (herein, "the U.S. Territories").

These Rules apply in addition to any that apply within the Asia/Pacific Region, with respect to Customers located in American Samoa, Guam, and Northern Mariana Islands; the Latin America and the Caribbean Region, with respect to Customers located in Puerto Rico and the U.S. Virgin Islands; and the United States Region, with respect to U.S. Region Customers.

### 7.6 Hybrid Terminal Requirements

#### 7.6.1 Hybrid POS Terminal Requirements

##### Hybrid POS Terminal and Chip-only MPOS Terminal Displays

In the U.S. Region and U.S. Territories, the Rule on this subject is replaced with the following:

A Hybrid POS Terminal (including any Hybrid MPOS Terminal) and a Chip-only MPOS Terminal must:

1. For each debit Account (including any prepaid debit Account) on a Card, display to the Cardholder at least one mutually supported application label or preferred name, which the Merchant may select.
2. For each credit Account on a Card, display all mutually supported application labels or preferred names. Multiple matching applications must be displayed in the Issuer's priority sequence.
3. Display to the Cardholder the Transaction amount and Transaction currency, if different from the Merchant's or cash disbursement agent's local currency.

For more information, refer to the U.S. Region section in Chapter 2 of the *M/Chip Requirements for Contact and Contactless* manual.

---

# Appendix A Geographic Regions

*This appendix provides listings of geographic regions.*

---

Asia/Pacific Region.....	233
Canada Region.....	234
Europe Region.....	234
Single European Payments Area (SEPA).....	235
Latin America and the Caribbean Region.....	235
Middle East/Africa Region.....	236
United States Region.....	237



## Asia/Pacific Region

The Asia/Pacific Region includes the following countries or territories.

American Samoa	Myanmar
Australia	Nauru
Bangladesh	Nepal
Bhutan	New Caledonia
Brunei Darussalam	New Zealand
Cambodia	Niue
China	Norfolk Island
Christmas Island	Northern Mariana Islands
Cocos (Keeling) Islands	Palau
Cook Islands	Papua New Guinea
Fiji	Philippines
French Polynesia	Pitcairn
Guam	Samoa
Heard and McDonald Islands	Singapore
Hong Kong	Solomon Islands
India	Sri Lanka
Indonesia	Taiwan
Japan	Thailand
Kiribati	Timor-Leste
Korea, Republic of	Tokelau
Lao People's Democratic Republic	Tonga
Macao	Tuvalu
Malaysia	U.S. Minor Outlying Islands
Maldives	Vanuatu
Marshall Islands	Viet Nam
Micronesia, Federated States of	Wallis and Futuna
Mongolia	

## Canada Region

The Canada Region is composed of Canada.

## Europe Region

The Europe Region includes the following countries or territories.

Albania	Greece	Poland
Andorra	Hungary	Portugal <sup>4</sup>
Antarctica	Iceland	Romania
Armenia	Ireland	Russian Federation
Austria	Isle of Man	San Marino
Azerbaijan	Israel	Serbia
Belarus	Italy	Slovakia
Belgium	Kazakhstan	Slovenia
Bosnia and Herzegovina	Kosovo	Spain <sup>5</sup>
Bulgaria	Kyrgyzstan	St. Helena, Ascension and Tristan Da Cunha
Channel Islands <sup>6</sup>	Latvia	Sweden
Croatia	Liechtenstein	Switzerland
Cyprus	Lithuania	Tajikistan
Czech Republic	Luxembourg	Turkey
Denmark <sup>7</sup>	Macedonia	Turkmenistan
Estonia	Malta	Ukraine
Finland <sup>8</sup>	Moldova	United Kingdom <sup>9</sup>
France <sup>10</sup>	Monaco	Uzbekistan
Georgia	Montenegro	Vatican City

<sup>4</sup> Includes Azores and Madeira.

<sup>5</sup> Includes Canary Islands, Ceuta and Melilla.

<sup>6</sup> Includes Guernsey and Jersey.

<sup>7</sup> Includes Faroe Islands and Greenland.

<sup>8</sup> Includes Aland Islands.

<sup>9</sup> Includes Falkland Islands, South Georgia and South Sandwich Islands.

<sup>10</sup> Includes Mayotte, Guadeloupe, Martinique, French Guiana, St. Martin (French Part), Réunion, and St. Barthélemy.

Germany	Netherlands
Gibraltar	Norway <sup>11</sup>

Changes in allegiance or national affiliation of a part of any of the countries listed in this appendix shall not affect the geographic coverage of the definition.

## Single European Payments Area (SEPA)

The Single European Payments Area includes the following countries or territories.

Andorra	Gibraltar	Norway <sup>12</sup>
Antarctica	Greece	Poland
Austria	Hungary	Portugal
Belgium	Iceland	Romania
Bulgaria	Ireland	Saint Helena, Ascension and Tristan da Cunha
Channel Islands <sup>13</sup>	Isle of Man	San Marino
Croatia	Italy	Slovakia
Cyprus	Latvia	Slovenia
Czech Republic	Liechtenstein	Spain
Denmark <sup>14</sup>	Lithuania	Sweden
Estonia	Luxembourg	Switzerland
Finland <sup>15</sup>	Malta	United Kingdom <sup>16</sup>
France <sup>17</sup>	Monaco	Vatican City
Germany		Netherlands

## Latin America and the Caribbean Region

The Latin America and the Caribbean Region includes the following countries or territories.

<sup>11</sup> Includes Svalbard and Jan Mayen.

<sup>12</sup> Includes Svalbard and Jan Mayen.

<sup>13</sup> Includes Guernsey and Jersey.

<sup>14</sup> Includes Faroe Islands and Greenland.

<sup>15</sup> Includes Aland Islands.

<sup>16</sup> Includes Falkland Islands, South Georgia and South Sandwich Islands.

<sup>17</sup> Includes Mayotte, Guadeloupe, Martinique, French Guiana, St. Martin (French Part), Réunion, and St. Barthélemy.

Anguilla	Cuba	Panama
Antigua and Barbuda	Curacao	Paraguay
Argentina	Dominica	Peru
Aruba	Dominican Republic	Puerto Rico
Bahamas	Ecuador	St. Kitts-Nevis
Barbados	El Salvador	St. Lucia
Belize	Grenada	St. Maarten
Bermuda	Guatemala	St. Vincent and the Grenadines
BES Islands <sup>18</sup>	Guyana	Suriname
Bolivia	Haiti	Trinidad and Tobago
Brazil	Honduras	Turks and Caicos Islands
Cayman Islands	Jamaica	Uruguay
Chile	Mexico	Venezuela
Colombia	Montserrat	Virgin Islands, British
Costa Rica	Nicaragua	Virgin Islands, U.S.

## Middle East/Africa Region

The Middle East/Africa Region includes the following countries or territories.

Afghanistan	Gabon	Pakistan
Algeria	Gambia	Palestine
Angola	Ghana	Qatar
Bahrain	Guinea	Rwanda
Benin	Guinea-Bissau	Sao Tome and Principe
Botswana	Iraq	Saudi Arabia
Bouvet Island	Jordan	Senegal
British Indian Ocean Territory	Kenya	Seychelles
Burkina Faso	Kuwait	Sierra Leone

<sup>18</sup> Bonaire, St. Eustatius and Saba.

---

Burundi	Lebanon	Somalia
Cameroon	Lesotho	South Africa
Cape Verde	Liberia	South Sudan
Central African Republic	Libyan Arab Jamahiriya	Swaziland
Chad	Madagascar	Syrian Arab Republic
Comoros	Malawi	Tanzania
Congo	Mali	Togo
Côte D'Ivoire	Mauritania	Tunisia
Democratic Republic of the Congo	Mauritius	Uganda
Djibouti	Morocco	United Arab Emirates
Egypt	Mozambique	Western Sahara
Equatorial Guinea	Namibia	Yemen
Eritrea	Niger	Zambia
Ethiopia	Nigeria	Zimbabwe
French Southern Territories	Oman	

---

## United States Region

---

The United States Region is composed of the United States.

---

# Appendix B Compliance Zones

*The following table identifies the noncompliance category that the Corporation has assigned to the Standards described within this manual.*

---

Compliance Zones..... 239

---

## Compliance Zones

---

The following table identifies the noncompliance category that Mastercard has assigned to the Standards described within this manual. These noncompliance categories are assigned for the purposes of noncompliance assessments under the compliance framework in Rule 2.1.4 of the *Mastercard Rules* manual.

Rule Number	Rule Title	Category
1.1	Connecting to the Interchange System	A
1.2	Authorization Routing—Mastercard POS Transactions	A
1.3	Authorization Routing—Maestro, Cirrus, and ATM Transactions	A
1.3.1	Routing Instructions and System Maintenance	C
1.3.2	Chip Transaction Routing	A
1.3.3	Domestic Transaction Routing	A
1.4	ATM Terminal Connection to the Interchange System	A
1.5	Gateway Processing	A
1.6	POS Terminal Connection to the Interchange System	A
2.1	Acquirer Authorization Requirements	A
2.2	Issuer Authorization Requirements	A
2.3	Authorization Responses	A
2.4	Performance Standards	A
2.5	Preauthorizations	A
2.6	Undefined Authorizations	A
2.7	Final Authorizations	A
2.8	Message Reason Code 4808 Chargeback Protection Period	A
2.9	Multiple Authorizations	A
2.10	Multiple Clearing Messages	A
2.11	Full and Partial Reversals	A
2.12	Full and Partial Approvals and Account Balance Responses	A
2.13	Refund Transactions and Corrections	A

Rule Number	Rule Title	Category
2.14	Balance Inquiries	B
2.15	CVC 2 Verification for POS Transactions	A
2.16	CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless Transactions—Brazil Only	A
2.17	Euro Conversion—Europe Region Only	C
2.18	Transaction Queries and Disputes	B
2.18.1	Retrieval Requests and Fulfillments	C
2.18.2	Compliance with Dispute Procedures	A
2.19	Chargebacks for Reissued Cards	C
2.20	Correction of Errors	A
2.21	Co-badged Cards—Acceptance Brand Identifier	B
3.1	Card-Present Transactions	B
3.1.1	Mastercard Card Acceptance Procedures	B
3.1.2	Maestro Card Acceptance Procedures	B
3.2	Card-Not-Present Transactions	B
3.3	Obtaining an Authorization	A
3.3.1	Mastercard POS Transaction Authorization Procedures	A
3.3.2	Maestro POS Transaction Authorization Procedures	A
3.4	Mastercard Cardholder Verification Requirements	A
3.5	Maestro Cardholder Verification Requirements	A
3.6	Use of a PIN for Transactions at ATM Terminals and Bank Branch Terminals	A
3.7	Use of a Consumer Device CVM	A
3.8	POI Currency Conversion	B
3.9	Multiple Transactions—Mastercard POS Transactions Only	B
3.10	Partial Payment—Mastercard POS Transactions Only	B
3.11	Specific Terms of a Transaction	B



Rule Number	Rule Title	Category
3.12	Charges for Loss, Theft, or Damage—Mastercard POS Transactions Only	B
3.13	Providing a Transaction Receipt	B
3.13.1	POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements	B
3.13.2	ATM and Bank Branch Terminal Transaction Receipt Requirements	B
3.13.3	Primary Account Number (PAN) Truncation and Expiration Date Omission	B
3.13.4	Prohibited Information	A
3.13.5	Standard Wording for Formsets	B
3.14	Returned Products and Canceled Services	B
3.14.1	Refund Transactions	B
3.15	Transaction Records	B
4.1	Chip Transactions at Hybrid Terminals	A
4.2	Offline Transactions Performed on Board Planes, Trains, and Ships	B
4.3	No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions—Europe Region Only	B
4.4	Contactless Transactions at POS Terminals	A
4.5	Contactless Transit Aggregated Transactions	A
4.6	Contactless Transactions at ATM Terminals	A
4.7	Contactless-only Acceptance	B
4.8	Mastercard Consumer-Presented QR Transactions at POS Terminals	B
4.9	Quick Payment Service (QPS) Program—Mastercard POS Transactions Only	B
4.10	Purchase with Cash Back Transactions	A
4.11	Transactions at Unattended POS Terminals	A
4.11.1	Automated Fuel Dispenser Transactions	A
4.12	PIN-based Debit Transactions—United States Region Only	A
4.13	PIN-less Single Message Transactions—United States Region Only	A

Rule Number	Rule Title	Category
4.14	Merchant-approved Maestro POS Transactions	A
4.15	Mastercard Manual Cash Disbursement Transactions	A
4.15.1	Non-discrimination Regarding Cash Disbursement Services	A
4.15.2	Maximum Cash Disbursement Amounts	B
4.15.3	Discount or Service Charges	B
4.15.4	Mastercard Acceptance Mark Must Be Displayed	B
4.16	Encashment of Mastercard Travelers Cheques	B
4.17	ATM Transactions	A
4.18	ATM Access Fees	B
4.19	Merchandise Transactions at ATM Terminals	A
4.20	Shared Deposits—United States Region Only	A
5.1	Electronic Commerce Transactions	A
5.2	Mail Order and Telephone Order (MO/TO) Transactions	A
5.3	Credential-on-File Transactions	A
5.4	Recurring Payment Transactions	A
5.5	Installment Billing for Domestic Transactions—Participating Countries Only	A
5.6	Transit Transactions Performed for Debt Recovery	B
5.7	Use of Automatic Billing Updater	B
5.8	Authentication Requirements—Europe Region Only	A
5.9	Merchant-initiated Transactions—EEA Only	A
6.1	Payment Transactions	A
6.2	Gaming Payment Transactions	A
6.3	MoneySend Payment Transactions	A
7.1	Terminal Eligibility	A
7.2	Terminal Requirements	A
7.2.1	Terminal Function Keys	C

Rule Number	Rule Title	Category
7.2.2	Terminal Responses	B
7.2.3	Terminal Transaction Log	A
7.3	Contactless Payment Functionality	A
7.4	POS Terminal Requirements	A
7.5	ATM Terminal and Bank Branch Terminal Requirements	A
7.6	Hybrid Terminal Requirements	A
7.7	Mastercard Consumer-Presented QR Functionality	A
	Appendix C—Transaction Identification Requirements	A
	Appendix D—Cardholder-Activated Terminal (CAT) Requirements	A
	Appendix F—Signage, Screen, and Receipt Text Display	B

## Appendix C Transaction Identification Requirements

*This appendix contains requirements for transaction identification. In the EEA, a Customer must identify Transactions in authorization and clearing messages using the values and in the fields defined by the registered switch of its choice.*

---

Transaction Date.....	245
Contactless Transactions.....	245
Contactless Transit Aggregated Transactions.....	246
Contactless-only Transactions.....	248
Quick Payment Service Transactions.....	250
Payment Transactions.....	251
Electronic Commerce Transactions.....	253
Electronic Commerce Transactions at Automated Fuel Dispensers .....	260
Digital Secure Remote Payment Transactions.....	263
Digital Secure Remote Payment Transactions Containing Chip Data.....	263
Digital Secure Remote Payment Transactions Containing UCAF Data.....	265
Partial Shipments or Recurring Payments Following Digital Secure Remote Payment Transactions.....	267
Mastercard Mobile Remote Payment Transactions.....	269
Mastercard Biometric Card Program Transactions.....	269

---

## Transaction Date

---

The Transaction date appearing in DE 12 (Date and Time, Local Transaction) is specified as follows.

<b>For the following transaction...</b>	<b>The transaction date is the date on which...</b>
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.
All In-Flight Commerce Transactions except those involving mailed purchases	The flight departs from the originating city. The Transaction date for in-flight commerce mailed purchases is the shipment date unless otherwise disclosed to the Cardholder.
Mastercard Contactless Transit Aggregated	One or more contactless taps performed with one Mastercard Account and occurring at one transit Merchant are aggregated in a First Presentment/1240 message.
Maestro Contactless Transit Aggregated	A Financial Transaction Request/0200 (or in the Europe Region, an Authorization Request/0100) message is sent for an estimated or maximum amount in connection with the use of one Maestro Account at one transit Merchant.

---

## Contactless Transactions

---

The Acquirer must identify each Contactless Transaction with the following values. A Transaction must not be identified as a Contactless Transaction if the Card information is contact chip-read, magnetic stripe-read, or key-entered. In addition, a Transaction must not be identified as a Maestro Contactless Transaction if the Card information is contactless magnetic stripe-read, except in Brazil with respect to Maestro Magnetic Stripe Mode Contactless Transactions (referred to herein as “Maestro Magstripe”).

### Contactless Transaction Values for Authorization Request/0100 or Financial Transaction Request/0200 Messages

Data Element	Subfield	Value
22 (Point of Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	One of the following: <ul style="list-style-type: none"> <li>• <b>07</b> (PAN auto-entry via contactless M/Chip)</li> <li>• <b>91</b> (PAN auto-entry via contactless magnetic stripe—the full track data had been read from the data on the card and transmitted within the authorization request in DE 35 [Track 2 Data] or DE 45 [Track 1 Data] without alteration or truncation)</li> </ul>
61 (Point-of-Service [POS] Data)	11 (POS Card Data Terminal Input Capabilities)	One of the following: <ul style="list-style-type: none"> <li>• <b>3</b> (Contactless M/Chip)</li> <li>• <b>4</b> (Contactless Magnetic Stripe)</li> </ul>

### Contactless Transaction Values for First Presentment/1240 Messages

Data Element	Subfield	Value
22 (Point of Service Data Code)	1 (Terminal Data: Card Data Capability)	One of the following: <ul style="list-style-type: none"> <li>• <b>A</b> (PAN auto-entry via contactless magnetic stripe)</li> <li>• <b>M</b> (PAN auto-entry via contactless M/Chip)</li> </ul>
	7 (Card Data: Input Mode)	One of the following: <ul style="list-style-type: none"> <li>• <b>A</b> (PAN auto-entry via contactless magnetic stripe)</li> <li>• <b>M</b> (PAN auto-entry via contactless M/Chip)</li> </ul>

### Contactless Transit Aggregated Transactions

The Acquirer must identify each Contactless transit aggregated Transaction with the following values.

## Contactless Transit Aggregated Transaction Values for Authorization Request/0100 or Financial Transaction Request/0200 Messages

Data Element	Subfield	Value
18 (Merchant Type)		One of the following: <ul style="list-style-type: none"> <li>• <b>4111</b> (Transportation—Suburban and Local Commuter Passenger, including Ferries)</li> <li>• <b>4131</b> (Bus Lines)</li> <li>• <b>4784</b> (Bridge and Road Fees, Tolls)</li> </ul>
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	Any of the values shown in “Contactless Transactions Values for Authorization Request/0100 or Financial Transaction Request/0200 Messages.” Please note that additionally, the value of 82 appears in Contactless debt repayment Transactions.
48 (Additional Data—Private Use)	1 (Transaction Category Code [TCC])	<b>X</b> (Airline and Other Transportation Services)
48 (Additional Data—Private Use), subelement 64 (Transit Program)	1 (Transit Transaction Type)	One of the following: <ul style="list-style-type: none"> <li>• <b>03</b> (Mastercard Contactless Transit Aggregated)</li> <li>• <b>06</b> (Maestro Contactless Transit Aggregated)</li> </ul>
61 (Point-of-Service [POS] Data)	1 (POS Terminal Attendance)	<b>1</b> (Unattended terminal)
	3 (POS Terminal Location)	<b>0</b> (On premises of merchant facility)
	4 (POS Cardholder Presence)	<b>0</b> (Cardholder present)
	5 (POS Card Presence)	<b>0</b> (Card present)
	6 (POS Card Capture Capabilities)	<b>0</b> (Terminal/Operator has no card capture capability)
	7 (POS Transaction Status)	One of the following: <ul style="list-style-type: none"> <li>• <b>0</b> (Normal request)</li> <li>• <b>4</b> (Pre-authorized request) Note: This value is only for Europe Region-acquired Transactions.</li> </ul>
	10 (Cardholder-Activated Terminal Level)	<b>0</b> (Not a CAT transaction)
	11 (POS Card Data Terminal Input Capability)	One of the following: <ul style="list-style-type: none"> <li>• <b>3</b> (Contactless M/Chip)</li> <li>• <b>4</b> (Contactless Magnetic Stripe)</li> </ul>

### Contactless Transit Aggregated Transaction Values for First Presentment/1240 Messages

Data Element/PDS	Subfield	Value
22 (Point of Service Data Code)	1 (Terminal Data: Card Data Capability)	One of the following: <ul style="list-style-type: none"> <li><b>A</b> (PAN auto-entry via contactless magnetic stripe)</li> <li><b>M</b> (PAN auto-entry via contactless M/Chip)</li> </ul>
	3 (Terminal Data: Card Capture Capability)	<b>0</b> (No capture capability)
	4 (Terminal Operating Environment)	<b>2</b> (On merchant premises; unattended terminal)
	5 (Card Present Data)	<b>0</b> (Cardholder present)
	6 (Card Present Data)	<b>1</b> (Card present)
	7 (Card Data: Input Mode)	One of the following: <ul style="list-style-type: none"> <li><b>A</b> (PAN auto-entry via contactless magnetic stripe)</li> <li><b>M</b> (PAN auto-entry via contactless M/Chip)</li> </ul>
26 (Merchant Business Code [MCC])		One of the following: <ul style="list-style-type: none"> <li><b>4111</b> (Transportation-Suburban and Local Commuter Passenger, including Ferries)</li> <li><b>4131</b> (Bus Lines)</li> <li><b>4784</b> (Bridge and Road Fees, Tolls)</li> </ul>
PDS 0210 (Transit Transaction Type)	1 (Transit Transaction Type)	One of the following: <ul style="list-style-type: none"> <li><b>03</b> (Mastercard Contactless Transit Aggregated)</li> <li><b>06</b> (Maestro Contactless Transit Aggregated)</li> </ul>

### Contactless-only Transactions

The Acquirer must identify each Contactless-only Transaction with the following values.

### Contactless-Only Transaction Values for Authorization Request/0100 or Financial Transaction Request/0200 Messages

Data Element	Subfield	Value
18 (Merchant Type)		An MCC approved to be Contactless-only as published from time to time in the <i>Global Operations Bulletin</i> .



Data Element	Subfield	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	Any of the values shown in “Contactless Transaction Values for Authorization Request/0100 or Financial Transaction Request/0200 Messages.”
61 (Point-of-Service [POS] Data)	1 (POS Terminal Attendance)	<b>1</b> (Unattended terminal)
	3 (POS Terminal Location)	One of the following: <ul style="list-style-type: none"> <li>• <b>0</b> (On premises of merchant facility)</li> <li>• <b>1</b> (Off premises of merchant facility [merchant terminal—remote location])</li> </ul>
	4 (POS Cardholder Presence)	<b>0</b> (Cardholder present)
	5 (POS Card Presence)	<b>0</b> (Card present)
	7 (POS Transaction Status)	<b>0</b> (Normal request)
	10 (Cardholder-Activated Terminal Level)	One of the following: <ul style="list-style-type: none"> <li>• <b>1</b> (Authorized Level 1 CAT: Automated dispensing machine with PIN)</li> <li>• <b>2</b> (Authorized Level 2 CAT: Self-service terminal)</li> <li>• <b>3</b> (Authorized Level 3 CAT: Limited-amount terminal)</li> </ul>
	11 (POS Card Data Terminal Input Capability)	One of the following: <ul style="list-style-type: none"> <li>• <b>3</b> (Contactless M/Chip)</li> <li>• <b>4</b> (Contactless Magnetic Stripe)</li> </ul>

### Contactless-Only Transaction Values for First Presentment/1240 Messages

Data Element	Subfield	Value
22 (Point of Service Data Code)	1 (Terminal Data: Card Data Capability)	One of the following: <ul style="list-style-type: none"> <li>• <b>A</b> (PAN auto-entry via contactless magnetic stripe)</li> <li>• <b>M</b> (PAN auto-entry via contactless M/Chip)</li> </ul>
	4 (Terminal Operating Environment)	One of the following: <ul style="list-style-type: none"> <li>• <b>2</b> (On merchant premises; unattended terminal)</li> <li>• <b>4</b> (Off merchant premises; unattended)</li> <li>• <b>6</b> (Off cardholder premises; unattended)</li> </ul>
	5 (Card Present Data)	<b>0</b> (Cardholder present)
	6 (Card Present Data)	<b>1</b> (Card present)

Data Element	Subfield	Value
	7 (Card Data: Input Mode)	One of the following: <ul style="list-style-type: none"> <li>• <b>A</b> (PAN auto-entry via contactless magnetic stripe)</li> <li>• <b>M</b> (PAN auto-entry via contactless M/Chip)</li> </ul>
26 (Merchant Business Code [MCC])		An MCC approved to be contactless-only as published from time to time in the <i>Global Operations Bulletin</i> .

## Quick Payment Service Transactions

The Acquirer must identify each Quick Payment Service (QPS) Transaction with the following values.

### QPS Transaction Values for First Presentment/1240 Messages

Data Element	Subfield	Value
22 (Point of Service Data Code)	1 (Terminal Data: Card Data Capability)	One of the following: <ul style="list-style-type: none"> <li>• <b>2</b> (Magnetic stripe reader capability)</li> <li>• <b>5</b> (Integrated circuit card [ICC] capability)</li> <li>• <b>B</b> (Magnetic stripe reader and key entry capability)</li> <li>• <b>C</b> (Magnetic stripe reader, ICC, and key entry capability)</li> <li>• <b>D</b> (Magnetic stripe reader and ICC capability)</li> <li>• <b>E</b> (ICC and key entry capability)</li> </ul>
	4 (Terminal Operating Environment)	<ul style="list-style-type: none"> <li>• <b>1</b> (On merchant premises; attended terminal)</li> <li>• <b>3</b> (Off merchant premises; attended terminal)</li> </ul>
	5 (Cardholder Present Data)	<b>0</b> (Cardholder present)
	6 (Card Present Data)	<b>1</b> (Card present)
	7 (Card Data: Input Mode)	One of the following: <ul style="list-style-type: none"> <li>• <b>2</b> (Magnetic stripe reader input)</li> <li>• <b>B</b> (Magnetic stripe reader input; track data captured and passed unaltered)</li> <li>• <b>C</b> (Online Chip)</li> <li>• <b>F</b> (Offline Chip)</li> </ul>
26 (Merchant Business Code [MCC])		An eligible Quick Payment Service (QPS) MCC.

Data Element	Subfield	Value
PDS 0044 (Program Participation Indicator)	2 (QPS/Contactless Chargeback Eligibility Indicator)	I (Ineligible for chargeback)—Value added by Mastercard.

## Payment Transactions

Each Payment Transaction must be identified with the following values. For the purposes of subfields and values included in the tables below, Cardholder includes Account Holder, where applicable.

### Payment Transaction Values for Authorization Request/0100 or Financial Transaction Request/0200 Messages

Data Element	Subfield	Value
3 (Processing Code)	1 (Cardholder Transaction Type)	28

Data Element	Subfield	Value
18 (Merchant Type)		<p>One of the following:</p> <ul style="list-style-type: none"> <li>• <b>6532</b>—for a Payment Transaction processed by a Customer or its authorized agent.</li> <li>• <b>6533</b>—for a Payment Transaction processed by a Merchant.</li> <li>• <b>7800</b>—for Gaming Payment Transactions (Government-owned Lottery, U.S. Region only)</li> <li>• <b>7995</b>—for Gaming Payment Transactions (Gambling Transactions, Europe and MEA Regions only)</li> <li>• A value specified for Payment Transactions in the applicable Customer-to-Customer intracountry, or intercountry business service arrangement, if one is in place.</li> <li>• For MoneySend Payment Transactions, the MCC that reflects the primary business of the Merchant or Submerchant or other entity as described in the <i>MoneySend Program Guide</i>.</li> <li>• For Payment Transactions (other than MoneySend Payment Transactions), the program defined MCC as described in the applicable Standards.</li> </ul>
48 (Additional Data—Private Use)	TCC (Transaction Category Code)	Refer to the <i>Quick Reference Booklet</i> .
48 (Additional Data—Private Use)	77 (Payment Transaction Type Indicator)	Payment Transaction program type identified in the <i>Customer Interface Specification</i> and the <i>Single Message System Specifications</i> .

**Payment Transaction Values for First Presentment/1240 Messages**

Data Element	Subfield	Value
3 (Processing Code)	1 (Cardholder Transaction Type)	28
26 (Merchant Business Code)		As described for DE 18 (Merchant Type) in the Authorization Request/0100 message
48 (Additional Data—Private Use)	PDS 0043 (Program Registration ID)	Payment Transaction program type identified in the <i>IPM Clearing Formats Manual</i>

The value used for the Payment Transaction program type must be that which best describes the purpose of the Payment Transaction.

Customers must refer to the *MoneySend Program Guide* for message specifications that must be followed to process MoneySend Payment Transactions. The *MoneySend Program Guide* includes specific Payment Transaction program type values that must be used to properly identify different types of MoneySend Payment Transactions.

The Acquirer also should provide either the customer service phone number in PDS 0170 (Merchant Inquiry Information), subfield 1 (Customer Service Phone Number) or the URL address in PDS 0175 (Merchant URL) in the clearing message.

A Payment Transaction Detail addendum may also be submitted with a Payment Transaction. This addendum provides the Issuer and Cardholder with enhanced data about the Merchant, the recipient of funds, and other Payment Transaction details.

**Electronic Commerce Transactions**

The Acquirer must identify each electronic commerce Transaction with the following values.

**Authorization Request/0100 or Financial Transaction Request/0200 Message**

Data Element	Subfield or Subelement	Field	Value	Description
18		Merchant Type	<b>5542</b>	Fuel Dispenser, Automated

Data Element	Subfield or Subelement	Field	Value	Description
22	01	POS Terminal PAN Entry Mode	<b>09, 10, or 81</b>	<b>09</b> = PAN/Token entry via electronic commerce containing DSRP cryptogram in DE 55 (Integrated Circuit Card [ICC] System-Related Data) <b>10</b> = Credential on File <b>81</b> = PAN/Token entry via electronic commerce with optional SecureCode-AAV or DSRP cryptogram in UCAF
	02	POS Terminal PIN Entry Mode	<b>2</b>	Terminal does not have PIN entry capability
48	01	Transaction Category Code	<b>T</b>	Phone, Mail, or Electronic Commerce Order
	42/SF 1	Electronic Commerce Security Level Indicator and UCAF Collection Indicator	<b>As appropriate</b>	

Data Element	Subfield or Subelement	Field	Value	Description
61	1	POS Terminal Attendance	<b>1</b>	Unattended terminal (cardholder-activated terminal [CAT], home PC, mobile phone, PDA)
	3	POS Terminal Location	<b>4</b>	On premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA)
	4	POS Cardholder Presence	<b>5</b>	Cardholder not present (Electronic order [home PC, Internet, mobile phone, PDA])
	5	POS Card Presence	<b>1</b>	Card not present
	6	POS Card Capture Capabilities	<b>0</b>	Terminal/ operator does not have card capture capability
	7	POS Transaction Status	<b>0 or 4</b>	<b>0</b> = Normal request <b>4</b> = Preauthorized request
	8	POS Transaction Security	<b>0</b>	No security concern
	10	Cardholder-Activated Terminal Level	<b>6</b>	Authorized Level 6 CAT: Electronic commerce

Data Element	Subfield or Subelement	Field	Value	Description
	11	POS Card Data Terminal Input Capability Indicator	<b>1</b>	No terminal used (voice/ARU authorization); server

#### Authorization Advice/0120 or 0400 Message

Data Element	Subfield or Subelement	Field	Value	Description
<b>18</b>		Merchant Type	<b>5542</b>	Fuel Dispenser, Automated
<b>22</b>	<b>01</b>	POS Terminal PAN Entry Mode	<b>09, 10, or 81</b>	<b>09</b> = PAN/Token entry via electronic commerce containing DSRP cryptogram in DE 55 (Integrated Circuit Card [ICC] System-Related Data) <b>10</b> = Credential on File <b>81</b> = PAN/Token entry via electronic commerce with optional SecureCode-AAV or DSRP cryptogram in UCAF
	<b>02</b>	POS Terminal PIN Entry Mode	<b>2</b>	Terminal does not have PIN entry capability



Data Element	Subfield or Subelement	Field	Value	Description
<b>48</b>	<b>01</b>	Transaction Category Code	<b>T</b>	Phone, Mail, or Electronic Commerce Order
	<b>42/SF 1</b>	Electronic Commerce Security Level Indicator and UCAF Collection Indicator	<b>As appropriate</b>	
<b>61</b>	<b>1</b>	POS Terminal Attendance	<b>1</b>	Unattended terminal (cardholder-activated terminal [CAT], home PC, mobile phone, PDA)
	<b>3</b>	POS Terminal Location	<b>4</b>	On premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA)
	<b>4</b>	POS Cardholder Presence	<b>5</b>	Cardholder not present (Electronic order [home PC, Internet, mobile phone, PDA])
	<b>5</b>	POS Card Presence	<b>1</b>	Card not present
	<b>6</b>	POS Card Capture Capabilities	<b>0</b>	Terminal/operator does not have card capture capability
	<b>7</b>	POS Transaction Status	<b>0</b>	Normal request (original presentment)

### First Presentment/1240 message

Data Element	Subfield or Subelement	Field	Value	Description
22	1	Terminal Data: Card	1	Manual; no terminal; server
		Data Input Capability		
		Terminal Data:		
	2	Cardholder Authentication Capability	0	No electronic authentication capability
	3	Terminal Data: Card Capture Capability	0	No capture capability
	4	Terminal Operating Environment	2	On card acceptor premises; unattended terminal
	5	Cardholder Present Data	5	Cardholder not present (electronic order [PC, Internet, mobile phone, or PDA])
	6	Card Present Data	0	Card not present 7 = Credential on File R = PAN/Token entry via electronic commerce containing
	7	Card Data: Input Mode	7, R, or S	DSRP cryptogram in DE 55 (Integrated Circuit Card [ICC] System-Related Data)

Data Element	Subfield or Subelement	Field	Value	Description
				S = Electronic commerce
	<b>12</b>	PIN Capture Capability	<b>0</b>	No PIN capture capability
<b>26</b>	-	Card Acceptor Business Code (MCC)	<b>5542</b>	Fuel Dispenser, Automated

#### Electronic Commerce Transaction Values for Authorization Request/0100 or Financial Transaction Request/0200 Messages

Data Element	Subfield	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	<b>81</b> (PAN entry via e-commerce, including chip)
61 (Point-of-Service [POS] Data)	4 (POS Cardholder Presence)	One of the following: <ul style="list-style-type: none"> <li><b>4</b> (Standing order/recurring transactions) [If the Transaction is the first payment in a recurring payment arrangement]</li> <li><b>5</b> (Electronic order)</li> </ul>
61 (Point-of-Service [POS] Data)	10 (CAT Level)	<b>6</b> (Electronic commerce)

#### Electronic Commerce Transaction Values for First Presentment/1240 Messages

Data Element	Subfield	Value
22 (Point of Service Data Code)	5 (Cardholder Present Data)	One of the following: <ul style="list-style-type: none"> <li><b>4</b> (Cardholder not present (standing order/ recurring transactions) [If the Transaction is the first payment in a recurring payment arrangement]</li> <li><b>5</b> (Cardholder not present [electronic order])</li> </ul>

Data Element	Subfield	Value
22 (Point of Service Data Code)	7 (Card Data: Input Mode)	<b>S</b> (Electronic commerce)

## Electronic Commerce Transactions at Automated Fuel Dispensers

### Authorization Request/0100, Authorization Advice/0120, Acquirer Reversal Advice/0420, and Financial Transaction Request/0200 Messages

Data Element	Subfield or Subelement	Field	Value	Description
18		Merchant Type	<b>5542</b>	Fuel Dispenser, Automated
22	01	POS Terminal PAN Entry Mode	<b>09</b> , <b>10</b> , or <b>81</b>	<p><b>09</b> = PAN/Token entry via electronic commerce containing DSRP cryptogram in DE 55 (Integrated Circuit Card [ICC] System-Related Data)</p> <p><b>10</b> = Credential on File</p> <p><b>81</b> = PAN/Token entry via electronic commerce with optional SecureCode-AAV or DSRP cryptogram in UCAF</p>
	02	POS Terminal PIN Entry Mode	<b>2</b>	Terminal does not have PIN entry capability

Data Element	Subfield or Subelement	Field	Value	Description
48	01	Transaction Category Code	<b>T</b>	Phone, Mail, or Electronic Commerce Order
	42/SF 1	Electronic Commerce Security Level Indicator and UCAF Collection Indicator	<b>As appropriate</b>	
61	1	POS Terminal Attendance	<b>1</b>	Unattended terminal (Cardholder-Activated Terminal [CAT], home PC, mobile phone, PDA)
	3	POS Terminal Location	<b>4</b>	On premises of Card acceptor facility (Cardholder terminal including home PC, mobile phone, PDA)
	4	POS Cardholder Presence	<b>5</b>	Cardholder not present (Electronic order [home PC, Internet, mobile phone, PDA])
	5	POS Card Presence	<b>1</b>	Card not present
	6	POS Card Capture Capabilities	<b>0</b>	Terminal/operator does not have card capture capability
	7	POS Transaction Status	<b>0 or 4</b>	<b>0</b> = Normal request <b>4</b> = Preauthorized request
	8	POS Transaction Security	<b>0</b>	No security concern
	10	Cardholder-Activated Terminal Level	<b>6</b>	Authorized Level 6 CAT: Electronic Commerce

Data Element	Subfield or Subelement	Field	Value	Description
	11	POS Card Data Terminal Input Capability Indicator	<b>6</b>	Terminal supports key entry input only

#### First Presentment/1240 Message

Data Element	Subfield or Subelement	Field	Value	Description
22	1	Terminal Data: Card Data Input Capability	<b>6</b>	Terminal supports key entry input only
	2	Terminal Data: Cardholder Authentication Capability	<b>0</b>	No electronic authentication capability
	3	Terminal Data: Card Capture Capability	<b>0</b>	No capture capability
	4	Terminal Operating Environment	<b>2</b>	On Card acceptor premises; unattended terminal
22	5	Cardholder Present Data	<b>5</b>	Cardholder not present (Electronic order [PC, Internet, mobile phone, or PDA])
	6	Card Present Data	<b>0</b>	Card not present

Data Element	Subfield or Subelement	Field	Value	Description
	7	Card Data: Input Mode	<b>7, R, or S</b>	<b>7</b> = Credential on File <b>R</b> = PAN/Token entry via Electronic commerce containing DSRP cryptogram in DE 55 (Integrated Circuit Card [ICC] System-Related Data) <b>S</b> = Electronic commerce
	12	PIN Capture Capability	<b>0</b>	No PIN capture capability
26	-	Card Acceptor Business Code (MCC)	<b>5542</b>	Fuel Dispenser, Automated
PDS	0023	Terminal Type	<b>CT6</b>	CAT Level 6 (Electronic commerce transaction)
PDS	0052	Electronic Commerce Security Level Indicator	<b>As appropriate</b>	

## Digital Secure Remote Payment Transactions

A Digital Secure Remote Payment Transaction is an electronic commerce Transaction that contains cryptographic information, in the form of either full EMV chip data passed in DE 55 or a cryptographic value derived from an M/Chip cryptogram passed in the Universal Cardholder Authentication Field (UCAF). Subsequent to the initial Digital Secure Remote Payment Transaction, a related Transaction for a partial shipment may occur, in which case cryptographic information is not passed. When a Digital Secure Remote Payment Transaction contains tokenized account information, the Mastercard Digital Enablement Service performs token mapping and cryptographic validation services.

### Digital Secure Remote Payment Transactions Containing Chip Data

### Authorization Request/0100 and Financial Transaction Request/0200 Messages

Data Element	Subfield/Subelement	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	<b>09</b> (PAN entry via electronic commerce, including remote chip)
48 (Additional Data—Private Use)	33 (PAN Mapping File Information)	Present when the Mastercard Digital Enablement Service performs token mapping.
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs token mapping:  Subfield 1 (On-behalf [OB] Service) = <b>50</b> (Mastercard Digital Enablement Service PAN Mapping); and  Subfield 2 (On-behalf [OB] Result 1) = <b>C</b> (Conversion of Token to PAN completed successfully)
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs cryptographic validation:  <ul style="list-style-type: none"> <li>Subfield 1 = <b>51</b> (Mastercard Digital Enablement Service Chip Pre-Validation); and</li> <li>Subfield 2 = <b>V</b> (Valid)</li> </ul>
61 (Point-of-Service [POS] Data)	3 (POS Terminal Location)	One of the following: <ul style="list-style-type: none"> <li><b>2</b> (Off premises of card acceptor facility [cardholder terminal including home PC, mobile phone, PDA]); or</li> <li><b>4</b> (On premises of card acceptor facility [cardholder terminal including home PC, mobile phone, PDA])</li> </ul>
	4 (POS Cardholder Presence)	<b>5</b> (Electronic order [home PC, Internet, mobile phone, PDA])
	10 (Cardholder-Activated Terminal Level)	<b>6</b> (Authorized Level 6 CAT: Electronic commerce)



### First Presentment/1240 Messages

Data Element	Subfield/PDS	Value
22 (Point-of-Service [POS] Data Code)	4 (Terminal Operating Environment)	One of the following: <ul style="list-style-type: none"> <li>• <b>2</b> (On card acceptor premises; unattended terminal); or</li> <li>• <b>4</b> (Off card acceptor premises; unattended)</li> </ul>
	5 (Cardholder Present Data)	<b>5</b> (Cardholder not present [electronic order (PC, Internet, mobile phone, or PDA)])
	7 (Card Data: Input Mode)	<b>R</b> (PAN Entry via electronic commerce, including remote chip)
48 (Additional Data)	PDS 0023 (Terminal Type)	<b>CT 6</b> (CAT level 6 [electronic commerce transaction])

## Digital Secure Remote Payment Transactions Containing UCAF Data

### Authorization Request/0100 and Financial Transaction Request/0200 Messages

Data Element	Subfield/ Subelement	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	<b>81</b> (PAN entry via electronic commerce, including chip)
48 (Additional Data—Private Use)	33 (PAN Mapping File Information)	Present when the Mastercard Digital Enablement Service performs token mapping.
	42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator)	All of the following: Position 1 = <b>2</b> Position 2 = <b>4</b> Position 3 = <b>2 or 6</b>

71 (On-behalf Services)		Present when the Mastercard Digital Enablement Service performs token mapping:  Subfield 1 (On-behalf [OB] Result 1) = <b>50</b> (Mastercard Digital Enablement Service PAN Mapping); and  Subfield 2 (On-behalf [OB] Service) = <b>C</b> (Conversion of Token to PAN completed successfully)
71 (On-behalf Services)		Present when the Mastercard Digital Enablement Service performs cryptographic validation:  Subfield 1 = <b>51</b> (Mastercard Digital Enablement Service Chip Pre-Validation); and  Subfield 2 = <b>V</b> (Valid)
61 (Point-of-Service [POS] Data)	3 (POS Terminal Location)	One of the following: <ul style="list-style-type: none"> <li>• <b>2</b> (off premises of card acceptor facility [cardholder terminal including home PC, mobile phone, PDA]); or</li> <li>• <b>4</b> (On premises of card acceptor facility [cardholder terminal including home PC, mobile phone, PDA])</li> </ul>
	4 (POS Cardholder Presence)	<b>5</b> (Electronic order [home PC, Internet, mobile phone, PDA])
	10 (Cardholder-Activated Terminal Level)	<b>6</b> (Authorized Level 6 CAT: Electronic commerce)

### First Presentment/1240 Messages

Data Element	Subfield/PDS	Value
22 (Point-of-Service [POS] Data Code)	4 (Terminal Operating Environment)	One of the following: <ul style="list-style-type: none"> <li>• <b>2</b> (On card acceptor premises; unattended terminal); or</li> <li>• <b>4</b> (Off card acceptor premises; unattended)</li> </ul>

48 (Additional Data)	5 (Cardholder Present Data)	<b>5</b> (Cardholder not present [electronic order (PC, Internet, mobile phone, or PDA)])
	7 (Card Data: Input Mode)	<b>S</b> (Electronic commerce)
	PDS 0023 (Terminal Type)	<b>CT 6</b> (CAT level 6 [electronic commerce transaction])
	PDS 0052 (Electronic Commerce Security Level Indicator)	All of the following: Position 1 = <b>2</b> Position 2 = <b>4</b> Position 3 = <b>2 or 6</b>

## Partial Shipments or Recurring Payments Following Digital Secure Remote Payment Transactions

### Authorization Request/0100 and Financial Transaction Request/0200 Messages

Data Element	Subfield/ Subelement	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	<b>81</b> (PAN entry via electronic commerce, including chip)
48 (Additional Data—Private Use)	33 (PAN Mapping File Information)	Present when the Mastercard Digital Enablement Service performs token mapping.
	42 (Electronic Commerce Indicators), Subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator)	All of the following: Position 1 = <b>2</b> Position 2 = <b>4</b> Position 3 = <b>7</b>
<b>NOTE: DE 48, Subelement 43 is not required. Liability will depend on the original UCAF indicator value in the matching initial DSRP transaction.</b>		

71 (On-behalf Services)	<p>Present when the Mastercard Digital Enablement Service performs token mapping:</p> <p>Subfield 1 (On-behalf [OB] Service) = <b>50</b> (Mastercard Digital Enablement Service PAN Mapping); and</p> <p>Subfield 2 (On-behalf [OB] Result 1) = <b>C</b> (Conversion of Token to PAN completed successfully)</p> <p><b>Note:</b> Value 51 (Mastercard Digital Enablement Service Chip Pre-Validation) does not appear in a partial shipment or recurring payment.</p>
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#### First Presentment/1240 Messages

Data Element	Subfield/PDS	Value
22 (Point-of-Service [POS] Data Code)	4 (Terminal Operating Environment)	<p>One of the following:</p> <ul style="list-style-type: none"> <li><b>2</b> (On card acceptor premises; unattended terminal); or</li> <li><b>4</b> (Off card acceptor premises; unattended)</li> </ul>
	5 (Cardholder Present Data)	<b>5</b> (Cardholder not present [electronic order (PC, Internet, mobile phone, or PDA)])
	7 (Card Data: Input Mode)	<b>5</b> (Electronic commerce)
48 (Additional Data)	PDS 0023 (Terminal Type)	<b>CT 6</b> (CAT level 6 [electronic commerce transaction])
	PDS 0052 (Electronic Commerce Security Level Indicator)	<p>All of the following:</p> <p>Position 1 = <b>2</b></p> <p>Position 2 = <b>4</b></p> <p>Position 3 = <b>7</b></p>

## Mastercard Mobile Remote Payment Transactions

The Acquirer must identify each Mastercard Mobile Remote Payment Transaction with the following values.

### Mastercard Mobile Remote Payment Transaction Values for Authorization Request/0100 or Financial Transaction Request/0200 Messages

Data Element	Subfield/Subelement	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	82 (PAN auto entry via server [issuer, acquirer, or third party vendor system])
48 (Additional Data—Private Use)	1 (Remote Payments Program Type Identifier)	1 (Issuer domain) or 2 (Acquirer Domain)

### Mastercard Mobile Remote Payment Transaction Values for First Presentment/1240 Messages

Data Element	Subfield/Subelement	Value
22 (Point of Service [POS] Entry Mode)	7 (Card Data: Input Mode)	T (PAN auto entry via server [issuer, acquirer, or third party vendor system])
48 (Additional Data)	1 (Remote Payments Program Data)	1 (Issuer domain) or 2 (Acquirer Domain)

## Mastercard Biometric Card Program Transactions

A biometric Card Transaction with successful biometric Cardholder verification is identified as follows:

- Byte 1, bit 5 of Tag 82 (Application Interchange Profile) is set to “0”
- The Cardholder verification results (CVR) present in DE 55, specifically:
  - Byte 1, bit 1 will contain a value of 1 to reflect that biometric was successful.
  - Byte 2, bit 2 will contain a value of 1 to reflect that biometric was used.

---

## Appendix D Cardholder-Activated Terminal (CAT) Transactions

*This appendix provides requirements for the use of CAT level indicators and the processing of Mastercard POS Transactions at Cardholder-Activated Terminals (CATs).*

---

CAT Transactions.....	271
CAT Level Requirements.....	272
Dual Capability for CAT 1 and CAT 2.....	272
CAT Level 1: Automated Dispensing Machines (CAT 1).....	272
CAT Level 2: Self-Service Terminal (CAT 2).....	273
CAT Level 3: Limited Amount Terminals (CAT 3).....	274
CAT Level 4: In-Flight Commerce (IFC) Terminals (CAT 4).....	276
CAT Level 6: Electronic Commerce Transactions (CAT 6).....	278
CAT Level 7: Transponder Transactions (CAT 7).....	278
CAT Level 9: Mobile POS (MPOS) Acceptance Device Transactions (CAT 9).....	279

## CAT Transactions

---

The requirements in these Cardholder-Activated Terminal (CAT) Rules apply to Mastercard POS Transactions only, with the following exceptions:

- CAT 6 must be used to identify all electronic commerce Transactions; and
- CAT 9 must be used to identify all Transactions occurring at a Mobile POS (MPOS) Terminal, whether attended or unattended.

An Acquirer may, at its option, use CAT 1 to identify any Transaction at an unattended Terminal where PIN is required, such as an ATM Terminal.

A CAT Transaction must be identified with the appropriate CAT level indicator value in authorization and clearing messages as follows:

- CAT Level 1: Automated Dispensing Machines (CAT 1)
- CAT Level 2: Self-Service Terminals (CAT 2)
- CAT Level 3: Limited Amount Terminals (CAT 3)
- CAT Level 4: In-Flight Commerce Terminals (CAT 4)
- CAT Level 6: Electronic Commerce Transactions (CAT 6)
- CAT Level 7: Transponder Transactions (CAT 7)
- CAT Level 9: Mobile POS (MPOS) Acceptance Device Transactions (CAT 9)

In Authorization Request/0100 and Authorization Request Response/0110 messages, the CAT level indicator is located in DE 61 (Point-of-Service Data), subfield 10 (Cardholder-Activated Terminal Level). In First Presentment/1240, Chargeback/1442, Second Presentment/1240, and Arbitration Chargeback/1442 messages, the CAT level indicator is located in PDS 0023 (Terminal Type). For additional requirements, see the *Customer Interface Specification* and the *IPM Clearing Formats* manuals.

The First Presentment/1240 message of a CAT Transaction must contain one of the following values in DE 22 (Point of Service Data Code), subfield 7 (Card Data: Input Mode):

- **A**—(PAN auto-entry via contactless magnetic stripe)
- **B**—(Magnetic stripe reader input, with track data captured and passed unaltered; does not apply to CAT 3)
- **C**—(Online Chip)
- **F**—(Offline Chip)
- **M**—(PAN auto-entry via contactless M/Chip)
- **N**—(Contactless input, ContactlessMapping Service applied [This value is visible only to Issuer; Acquirers use value A or M])
- **S**—(Electronic commerce; applies to CAT 6 only)
- **2**—(Magnetic stripe reader input; applies to CAT 3 only)

## CAT Level Requirements

The following requirements apply to the specific CAT levels indicated.

### Dual Capability for CAT 1 and CAT 2

A CAT device may have dual capability as a CAT 1 and a CAT 2. Dual capability allows a CAT device to identify each Transaction as CAT 1 or CAT 2, depending on the use of PIN (online or offline) or Consumer Device CVM (CDCVM).

IF...	THEN...
A Cardholder is prompted for a PIN or CDCVM and enters a PIN (online or offline) or completes CDCVM	The Acquirer must identify the Transaction with the CAT Level 1 indicator.
A Cardholder is not prompted for a PIN or CDCVM and does not enter a PIN (online or offline) or does not complete CDCVM	The Acquirer must identify the Transaction with the CAT Level 2 indicator.

A CAT device that supports offline PIN, CDCVM or both, but not online PIN, must have dual capability as a CAT 1 and CAT 2 device and comply with all CAT 2 requirements (including support of "No CVM").

A PIN-capable Hybrid POS Terminal identified with MCC 5542 (Fuel Dispenser, Automated) should:

- Always function as a CAT 1 device when a Chip Card is used or a Contactless Transaction occurs for an amount exceeding the applicable contactless CVM limit; and
- Only function as a CAT 2 device when a magnetic stripe Card is used or a Contactless Transaction occurs for an amount equal to or less than the applicable contactless CVM limit.

### CAT Level 1: Automated Dispensing Machines (CAT 1)

The following CVM requirements apply to CAT 1 devices:

1. CAT 1 devices must accept PIN as the CVM.
2. CAT 1 devices must support online PIN and may also support offline PIN and CDCVM.
  - a. Online PIN is the mandatory CVM for magnetic stripe Transactions.
  - b. PIN (online or offline) is the mandatory CVM for Contact Chip Transactions.
  - c. Either online PIN or CDCVM must be used as the CVM for Contactless Transactions.
  - d. CDCVM is the mandatory CVM for Mastercard Consumer-Presented QR Transactions.
3. CDCVM must be used as the CVM for Mastercard Consumer-Presented QR Transactions.
4. CAT 1 devices must not support only offline PIN as CVM.
5. CAT 1 devices must not perform CVM fallback.



6. CAT 1 devices must not accept signature or “No CVM” as the CVM.
7. The Standards relating to PIN and key management security apply to CAT 1 devices.

The following authorization requirements apply to CAT 1 devices:

1. All magnetic stripe Transactions, regardless of amount, must be authorized online by the Issuer.
2. All Mastercard Consumer-Presented QR Transactions, regardless of amount, must be authorized online by the Issuer.
3. A Chip Transaction must be authorized either online by the Issuer or for a Transaction less than or equal to USD 200 (EUR 200 in the Europe Region), a Chip Transaction may be authorized offline by the EMV chip.
4. The MIP X-Code authorization response must be a decline. The Issuer is liable for Transactions that are approved under acquirer MIP X-Code, up to the MIP X-Code limits specified by the Corporation.

The following additionally apply to CAT 1 devices:

1. There is no maximum amount limit.
2. A CAT 1 Hybrid POS Terminal must be capable of performing fallback procedures from chip to magnetic stripe, unless it is prohibited by a region.
3. CAT 1 devices may support Address Verification Service (AVS) and CVC 2 validation.
4. Chargeback rights apply to Transactions at CAT 1 devices under message reason code 4808, and do not apply with respect to message reason codes 4837 and 4863.
5. Card retention at CAT 1 devices is not required; however, if the capability is available, the Merchant may do so only at the Issuer's specific direction and in accordance with the procedures set forth in Chapter 5, “Card Recovery and Return Standards,” of the *Security Rules and Procedures* manual.

## **CAT Level 2: Self-Service Terminal (CAT 2)**

The following CVM requirements apply to CAT 2 devices:

1. CAT 2 devices must accept “No CVM” as the CVM.
2. CAT 2 devices must not accept signature or PIN (online or offline) as the CVM.

The following authorization requirements apply to CAT 2 devices:

1. All magnetic stripe Transactions, regardless of amount, must be authorized online by the issuer.
2. A Chip Transaction must be authorized either online by the Issuer or for a Transaction less than or equal to USD 200 (EUR 200 in the Europe Region), a Chip Transaction may be authorized offline by the EMV chip.
3. The Issuer is liable for Transactions that are approved under Acquirer MIP X-Code, up to the MIP X-Code limits specified by Mastercard.

The following additionally apply to CAT 2 devices:

1. There is no maximum amount limit.

2. A CAT 2 Hybrid POS Terminal must be capable of performing fallback procedures from chip to magnetic stripe, unless it is prohibited by a region.
3. CAT 2 devices may support AVS and CVC 2 validation.
4. Chargeback rights apply to Transactions at CAT 2 devices under message reason codes 4808 and 4837 and do not apply with respect to message reason codes 4840, 4863, and 4871. With respect to Contactless Transactions, an Issuer may use message reason code 4837 if the Transaction amount exceeds the applicable CVM limit.

An Issuer in Taiwan may use message reason code 4837 to charge back a Taiwan Domestic Transaction at a CAT 2 device identified with one of the below MCCs only if the Transaction was a magnetic stripe Transaction:

- 4011—Railroads – Freight
  - 4111—Transportation – Suburban and Local Commuter Passenger, including Ferries
  - 4225—Public Warehousing-Farm Products Refrigerated Goods, Household Goods, and Storage
  - 5399—Miscellaneous General Merchandise
  - 5411—Grocery Stores and Supermarkets
  - 5422—Freezer and Locker Meat Provisioners
  - 5542—Automated Fuel Dispensers
  - 5812—Eating Places and Restaurants
  - 5814—Fast Food Restaurants
  - 5999—Miscellaneous and Specialty Retail Stores
  - 7011—Lodging - Hotels, Motels, and Resorts
  - 7012—Timeshares
  - 7210—Laundry, Cleaning, and Garment Services
  - 7278—Buying and Shopping Services and Clubs
  - 7512—Automobile Rental Agency
  - 7523—Parking Lots and Garages
  - 7832—Motion Picture Theaters
  - 8062—Hospitals
  - 9402—Postal Services - Government Only
5. Card retention at CAT 2 devices is not required; however, if the capability is available, the Merchant may do so only at the Issuer's specific direction and in accordance with the procedures set forth in Chapter 5 of the *Security Rules and Procedures* manual.

### **CAT Level 3: Limited Amount Terminals (CAT 3)**

The following CVM requirements apply to CAT 3 devices:

1. CAT 3 devices must accept "No CVM" as the CVM.
  2. CAT 3 devices may accept offline PIN as the CVM for Contact Chip Transactions, in accordance with the security requirements for PIN and key management.
  3. CAT 3 devices must not accept signature as the CVM.
- Use of CAT 3 devices is restricted to the following MCCs:

- 4784—Bridges and Road Fees, Tolls
  - 7523—Automobile Parking Lots and Garages
  - 7542—Car Washes
  - 5499—Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores (solely for Contactless-only Transactions)
4. CAT 3 devices may accept Consumer Device CVM (CDCVM) for EMV Mode Contactless Transactions.

The following authorization requirements apply to CAT 3 devices:

1. The CAT 3 device must not have online capability. Chip Transactions may be authorized offline by the EMV chip.
2. The CAT 3 device must check the Account number against the Electronic Warning Bulletin when the device has such capability.
3. X-code processing does not apply.

The following maximum Transaction amount requirements apply to CAT 3 devices:

1. At CAT 3 devices with both contact and contactless payment functionality, the maximum Transaction amount for Contactless Transactions must be the same as for Contact Chip Transactions.
2. At Contactless-only CAT 3 devices, the maximum Transaction amount is the CVM limit for the Merchant location provided in Appendix E.
3. For all CAT 3 Transactions that are Domestic Transactions occurring in Hong Kong and Macao and identified with MCC 7523 (Automobile Parking Lots and Garages), the maximum Transaction amount is HKD 500.
4. For all CAT 3 Transactions occurring in the Europe Region, the maximum Transaction amount is EUR 50, or its local currency equivalent.
5. For all other CAT 3 Transactions, the maximum Transaction amount is USD 40, or its local currency equivalent.
6. The maximum Transaction amount for a magnetic stripe Transaction, including a Magnetic Stripe Mode Contactless Transaction, is zero, except in Hong Kong and Macao where the limit for Domestic Transactions occurring at MCC 7523 (Automobile Parking Lots and Garages) is HKD 500 and MOP 500, respectively.
7. Effective 16 October 2020, the maximum Transaction amount for a magnetic stripe Transaction occurring in Hong Kong or Macao, including a Magnetic Stripe Mode Contactless Transaction, is zero.

The following additionally apply to CAT 3 devices:

1. A hybrid CAT 3 device that also is a Hybrid POS Terminal is prohibited from performing fallback procedures from chip to magnetic stripe.
2. Chargeback rights apply to Transactions at CAT 3 devices under message reason code 4808 and do not apply with respect to message reason codes 4837, 4863, and 4871.
3. There is no card retention requirement for CAT 3 devices.

## **CAT Level 4: In-Flight Commerce (IFC) Terminals (CAT 4)**

The following CVM requirements apply to CAT 4 devices:

1. CAT 4 devices must accept “No CVM” as the CVM.
2. CAT 4 devices must not accept signature or PIN (online or offline) as the CVM.

The following authorization requirements apply to CAT 4 devices:

1. Prior to authorization, the Merchant must conduct a Mod-10 check digit routine to verify Card authenticity and must confirm that the Account number is within Mastercard BIN range 222100 to 272099 or 510000 to 559999.
2. A Chip Transaction must be authorized either online by the Issuer or for a Transaction less than or equal to USD 200 (EUR 200 in the Europe Region), a Chip Transaction may be authorized offline by the EMV chip.
3. Online authorization by the Issuer may occur either air-to-ground during the Transaction or in a delayed batch.
4. An authorization request must not contain a key-entered Account number or expiration date.
5. The Acquirer must convert all “refer to card issuer” and “capture card” messages received from Issuers to “decline.”
6. The Issuer is liable for Transactions that are approved under acquirer MIP X-Code, up to the MIP X-Code limits specified by the Corporation.

The following requirements also apply with respect to CAT 4 devices:

1. Acquirers must ensure timely delivery and installation of the IFC Blocked Gaming File to gambling service providers. IFC Blocked Gaming File access is required before every gambling Transaction.
2. Transactions at CAT 4 devices are conducted on interactive video terminals by passengers on airline flights.
3. Use of CAT 4 devices is restricted to the following six MCCs:
  - 4899—Cable, Satellite, and Other Pay Television and Radio Services
  - 5309—Duty Free Stores
  - 5964—Direct Marketing—Catalog Merchants
  - 7299—Other Services—not elsewhere classified
  - 7994—Video Game Arcades/Establishments
  - 7995—Gambling Transactions
4. For each flight, Acquirers must generate one Authorization Request/0100 message per MCC for each Account number. “Flight” is defined as one or more segments of a continuous air flight with the same flight number.
5. The Authorization Request/0100 message must contain a Transaction category code (TCC) of U for gambling Transactions or R for any other Transactions.
6. DE 43 must include the airline Merchant name and flight identification in subfield 1. The city field description must contain the Merchant customer service telephone number for mailed purchases and gambling Transactions; for all other CAT 4 Transactions, this information is optional. The telephone number is not required to be toll-free.

7. For all transactions at CAT 4 devices, except mailed purchase Transactions, the Transaction date is defined as the date that the flight departs from the originating city. The Transaction date for mailed purchases is defined as the shipment date unless otherwise disclosed to the Cardholder.
8. The Acquirer must ensure that the Merchant provides full disclosure to the Cardholder via the CAT 4 device before the initiation of any Transactions, as detailed below. The CAT 4 device must prompt the Cardholder to acknowledge these disclosure terms before initiating Transactions. Disclosure must include the following:
  - a. Full identification of the Merchant and provision for recourse in terms of Cardholder complaints or questions
  - b. Notification that Transactions will be billed upon the Issuer's approval of the authorization request
  - c. For mailed purchase Transactions only, any additional shipping or handling charges
  - d. Policy on refunds or returns
  - e. Provision for a paper TID

For gambling Transactions (where permitted), Merchants must additionally disclose the following:

- a. Maximum winnings (USD 3,500) and maximum losses (USD 350)
  - b. Notification that the total net Transaction amount (whether a net win or loss) will be applied to the Card account
  - c. Notification that Cardholder must be at least 18 years of age to play
  - d. Notification that some Issuers may not allow gambling
9. The Acquirer must ensure that the Merchant can provide an itemized TID to the Cardholder by printing a TID at the passenger's seat, printing a TID from a centralized printer on the plane, or sending the TID to the Cardholder by mail or electronic means. The device must describe any TID delivery offer and, if accepted, must require the Cardholder to input such information as may be required to complete the delivery (for example, name and address, email address, or mobile phone number). For gambling Transactions, the Merchant must provide a printed TID. Each TID must contain:
  - a. Identification of the passenger's flight, seat number, and date of departure
  - b. Itemized Transaction detail
  - c. Gambling Transaction specified as a net win or net loss
  - d. The truncated Card account number
10. The Acquirer must not submit declined Transactions into clearing.
11. No surcharges or service fees may be assessed on any Transaction, including gambling Transactions.

The following additional requirements apply with respect to gambling Transactions:

1. Gambling Transactions are not permitted at CAT 4 devices acquired within the Europe Region.
2. Net gambling losses cannot exceed USD 350 per flight per Account. Net payouts to Cardholders for gambling wins cannot exceed USD 3,500 per flight per Account. The Merchant must monitor losses and winnings throughout the flight to ensure compliance.

3. A gambling win Transaction will result in posting of net winnings (credit) to the Card account. Under no circumstance may winnings be paid in cash or other form of payment.
4. Before participating in gambling Activity, the Acquirer must undertake all reasonable and necessary steps to assure itself and, if requested, the Corporation, that such gambling Activity will be effected in full compliance with all applicable laws and regulations. By participating in gambling Activity, the Acquirer agrees to indemnify, defend, and hold the Corporation harmless with respect to any claim, damage, loss, fine, penalty, injury, or cause of action arising or resulting from or attributable to the Acquirer's gambling Activity.
5. The Card account number must be checked against the IFC Blocked Gaming File. Cardholders whose Card account numbers are listed on the IFC Blocked Gaming File must be prohibited from initiating gambling Transactions. Updates to the IFC Blocked Gaming File will be effective on the first and the 15th day of each month. The Corporation must receive Card account ranges or BINs that Issuers choose to list on the next effective updated IFC Blocked Gaming File at least two weeks before the effective date.
6. All gambling losses authorized post-flight must be submitted for authorization for the net amount. All gambling Transactions authorized during the flight will be for the full wager amount (USD 350 or a lower amount predetermined by the airline and gambling Merchant). No gambling wins will be submitted for authorization.
7. Gambling Transactions submitted for clearing must be for the net amount won or lost. Gambling win Transactions will be submitted as a refund Transaction (DE 3, subfield 1 must contain a value of 20). Interchange will be paid to Issuers by Acquirers on gambling win Transactions. An Acquirer may resubmit a gambling Transaction for a different amount within the specified Transaction limits if it previously was rejected for exceeding the specified Transaction limits—USD 3,500 for wins and USD 350 for losses.

The following additionally apply to CAT 4 devices:

1. There is no maximum amount limit for any Transaction at CAT 4 devices, except for gambling Transactions.
2. A CAT 4 device that also is a Hybrid POS Terminal is prohibited from performing fallback procedures from chip to magnetic stripe.
3. CAT 4 devices may support AVS and CVC 2 validation.
4. There are no chargeback restrictions for Transactions at CAT 4 devices.
5. There is no Card retention requirement for CAT 4 devices.

## **CAT Level 6: Electronic Commerce Transactions (CAT 6)**

Refer to Chapter 9, "Authorization Services Details," of the *Authorization Manual* for requirements regarding the identification of electronic commerce Transactions.

## **CAT Level 7: Transponder Transactions (CAT 7)**

The following CVM requirements apply to CAT 7 devices:

1. CAT 7 devices must accept "No CVM" as the CVM.
2. CAT 7 devices must not accept signature or PIN (online or offline) as the CVM.

The following authorization requirements apply to CAT 7 devices:

1. All magnetic stripe Transactions, regardless of amount, must be authorized online by the Issuer.
2. Chip Transactions must be authorized either online by the Issuer or offline by the EMV chip.
3. The Issuer is liable for Transactions that are approved under Acquirer MIP X-Code, up to the MIP X-Code limits specified by the Corporation.

The following additionally apply to CAT 7 devices:

1. There is no maximum amount limit for Transactions at CAT 7 devices.
2. A CAT 7 device that also is a Hybrid POS Terminal is prohibited from performing fallback procedures from chip to magnetic stripe.
3. CAT 7 devices may support AVS and CVC 2 validation.
4. There are no chargeback restrictions for Transactions at CAT 7 devices.
5. There is no card retention requirement for CAT 7 devices.

### **CAT Level 9: Mobile POS (MPOS) Acceptance Device Transactions (CAT 9)**

The Acquirer must submit the following values in Transaction messages for each Transaction conducted at an MPOS Terminal:

- A value of 9 (MPOS Acceptance Device) in DE 61 (Point-of-Service[POS] Data), subfield 10 (Cardholder-Activated Terminal Level) of the Authorization Request/0100 or Financial Transaction Request/0200 message; and
- A value of CT9 (MPOS Acceptance Device) in PDS 0023 (Terminal Type) of the First Presentment/1240 message.

---

# Appendix E CVM Limit Amounts

*This appendix specifies CVM limit amounts for Contactless Transactions, and the Quick Payment Service (QPS) program.*

---

Overview.....	281
CVM Limit Amounts.....	281



---

## Overview

---

The following sections present information on contactless POS transaction and Quick Payment Service transaction cardholder verification method (CVM) limit amounts. See Chapters 3 and 4 of the *Transaction Processing Rules* for more information.

## CVM Limit Amounts

---

Access the CVM limit amounts in Microsoft Excel® file format, which can be copied and pasted as needed.

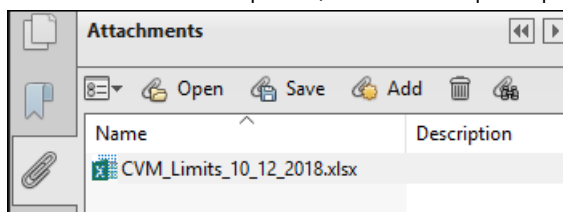
From the **HTML** edition of this document, you can access the CVM Limit Amounts spreadsheet.

1. In the upper right corner, click the file download icon.
2. Click [CVM\\_Limit\\_Amounts.xls](#).
3. When the file opens, save it to a location on your computer.

**NOTE: The CVM Limit Amounts spreadsheet is very large. Before printing this document, please be aware that, depending on your printer settings and paper selection, the printed spreadsheet may exceed 250 pages.**

From the **PDF** edition of this document, you can access the CVM Limit Amounts spreadsheet.

1. From the left-hand panel, click the Paperclip icon. The Attachments panel appears.



2. Double-click **CVM\_Limit\_Amounts.xls**.
3. When the file opens, save it to a location on your computer.

## Appendix F Signage, Screen, and Receipt Text Display

*This appendix provides ATM Terminal and unattended POS Terminal signage, screen, and receipt text display requirements.*

Screen and Receipt Text Standards.....	284
Models for ATM Access Fee Notification at ATM Terminals.....	284
Models for Standard Signage Notification of an ATM Access Fee.....	285
Asia/Pacific Region.....	285
Australia.....	285
Canada Region.....	286
Europe Region.....	286
United Kingdom.....	287
Latin America and the Caribbean Region.....	288
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.....	288
Middle East/Africa Region.....	289
United States Region.....	290
Models for Generic Terminal Signage Notification of an ATM Access Fee.....	290
Asia/Pacific Region.....	290
Australia.....	291
Canada Region.....	292
Europe Region.....	292
United Kingdom.....	293
Latin America and the Caribbean Region.....	294
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.....	294
Middle East/Africa Region.....	295
United States Region.....	296
Models for Screen Display Notification of an ATM Access Fee.....	296
Asia/Pacific Region.....	296
Australia.....	297
Canada Region.....	298
Europe Region.....	298
United Kingdom.....	299
Latin America and the Caribbean Region.....	300
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.....	300

Middle East/Africa Region.....	301
United States Region.....	302
Model for an ATM Access Fee Transaction Receipt.....	303
Model Screens Offering POI Currency Conversion.....	303
Model Receipt for Withdrawal Completed with POI Currency Conversion.....	304
Model Screen Displays for Offering Installment Payments.....	304
Model Receipt Texts for Installments.....	311

## Screen and Receipt Text Standards

Response Code	Recommended Screen Text	Recommended Receipt Text
<ul style="list-style-type: none"> <li>Format error</li> <li>Invalid acquirer</li> <li>Cardholder not on file</li> <li>Do not honor/Restricted card</li> <li>Unable to process/System error</li> <li>ATM processor inoperative</li> <li>Cardholder processor inoperative/Not found</li> </ul>	"I am sorry. I am unable to process your request. Please contact your financial institution."	"Denied Unable to Process"
<ul style="list-style-type: none"> <li>Invalid transaction</li> <li>Invalid transaction selection</li> </ul>	"I am sorry. You have selected an invalid transaction. Do you want to try another transaction?"	"Denied Invalid Transaction"
<ul style="list-style-type: none"> <li>Invalid amount</li> </ul>	"You have selected an invalid amount. Please select an amount in multiples of _____."	"Denied Invalid Amount"
<ul style="list-style-type: none"> <li>Insufficient funds</li> </ul>	"I am unable to process for insufficient funds. Please contact your financial institution."	"Denied Insufficient Funds"
<ul style="list-style-type: none"> <li>Invalid PIN</li> </ul>	"You have entered your PIN incorrectly. Do you want to try again?"	"Denied Invalid PIN"
<ul style="list-style-type: none"> <li>PIN tries exceed permitted number of attempts</li> </ul>	"You have exceeded the number of attempts permitted to enter your PIN. Please contact your financial institution."	"Denied Invalid PIN"
<ul style="list-style-type: none"> <li>Exceeds withdrawal limit</li> </ul>	"You have exceeded the withdrawal limit. Do you want to select another amount?"	"Denied Invalid Amount"
<ul style="list-style-type: none"> <li>Denied—Capture card</li> </ul>	"Your card has been retained. Please contact your financial institution."	"Denied Card Retained"

## Models for ATM Access Fee Notification at ATM Terminals

The following table sets forth minimum screen height, screen width, heading text, and body text requirements for ATM Access Fee signage and screen displays at ATM Terminals.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type
Body text	Must be at least 14 point type

## Models for Standard Signage Notification of an ATM Access Fee

Each of the following model forms illustrate the standard ATM Terminal signage notification that an ATM Access Fee may be charged, including the fee amount.

### Asia/Pacific Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Asia/Pacific Region, except Australia.

Fee Notice

The owner of this terminal, (name), may charge cardholders with a card issued in a country other than (country <sup>a</sup>) a fee of (currency code <sup>b</sup>) (amount) for a cash disbursement from your account. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. This additional charge will be added to the transaction amount and posted to your account.

<sup>a</sup> Insert country where ATM is located.

<sup>b</sup> Insert currency code for the country where the ATM is located.

### Australia

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for Australia only.

### Fee Notice

The owner of this terminal, (name), may charge cardholders a fee of AUD (amount) for a cash disbursement from your account, and in addition may charge cardholders with a card issued in Australia a fee of AUD (amount) for a non-financial transaction. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. This additional charge will be added to the transaction amount and posted to your account.

## Canada Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Canada Region only.

### Fee Notice

The owner of this terminal, (name), may charge cardholders a fee of CAD (amount) for a cash disbursement from your account. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. This additional charge will be added to the transaction amount and posted to your account.

## Europe Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Europe Region only, except the United Kingdom.

### Fee Notice

The owner of this terminal, (name), may charge cardholders with a card issued in a country other than (country <sup>a</sup>) a fee of (currency code <sup>b</sup>) (amount) for a cash disbursement from your account. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. This additional charge will be added to the transaction amount and posted to your account.

a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

### United Kingdom

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the United Kingdom only.

### Fee Notice

The owner of this terminal, (name), may charge cardholders a fee of GBP (amount) for withdrawals from your account or cash advances. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. This additional charge will be added to the transaction amount and posted to your account.

---

## Latin America and the Caribbean Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for Latin America and the Caribbean Region except the following countries: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.

Fee Notice

The owner of this terminal, (name),  
may charge cardholders with a card  
issued in a country other than  
(country <sup>a</sup>) a fee of (currency code <sup>b</sup>)  
(amount) for a withdrawal from  
your account or cash advances.  
This charge is in addition to any  
fees that may be assessed by your  
card-issuing financial institution.  
This additional charge will be added  
to the transaction amount and  
posted to your account.

a    Insert country where ATM is located.

b    Insert currency code for the country where the ATM is located.

## Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for only the following countries in the Latin America and the Caribbean Region: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.



### Fee Notice

The owner of this terminal, (name), may charge cardholders a fee of (currency code <sup>a</sup>) (amount) for a withdrawal from your account or cash advances. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. This additional charge will be added to the transaction amount and posted to your account.

<sup>a</sup> Insert currency code for the country where the ATM is located.  
Argentina (ARS), Brazil (BRL), Chile (CLP), Colombia (COP),  
Ecuador (USD), Mexico (MXN), Panama (PAB or USD),  
Peru (PEN), Puerto Rico (USD), or Venezuela (VEB).

## Middle East/Africa Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Middle East/Africa Region.

### Fee Notice

The owner of this terminal, (name), may charge cardholders with a card issued in a country other than (country <sup>a</sup>) a fee of (currency code <sup>b</sup>) (amount) for a withdrawal from your account or cash advances. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. This additional charge will be added to the transaction amount and posted to your account.

<sup>a</sup> Insert country where ATM is located.  
<sup>b</sup> Insert currency code for the country where the ATM is located.

## United States Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the United States only.

Fee Notice

The owner of this terminal, (name),  
may charge cardholders a fee of  
USD (amount) for a cash  
disbursement from your account.  
This charge is in addition to any  
fees that may be assessed by your  
card-issuing financial institution.  
This additional charge will be added  
to the transaction amount and  
posted to your account.

## Models for Generic Terminal Signage Notification of an ATM Access Fee

---

Each of the following models illustrate the generic ATM Terminal signage notification that an ATM Access Fee may be charged.

### Asia/Pacific Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Asia/Pacific Region, except Australia.

### Fee Notice

The owner of this terminal, (name), may charge cardholders with a card issued in a country other than (country <sup>a</sup>) a fee for withdrawals from your account or cash advances. The amount of this fee will be disclosed on the terminal screen prior to your completion of the transaction. This fee is in addition to any fees charged by your financial institution. It will be added to the transaction amount and posted to your account.

<sup>a</sup> Insert country where ATM is located.

### Australia

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for Australia only.

### Fee Notice

The owner of this terminal, (name), may charge cardholders a fee for withdrawals from your account or cash advances, and in addition may charge cardholders with a card issued in Australia a fee for a non-financial transaction. The amount of this fee will be disclosed on the terminal screen prior to your completion of the transaction. This fee is in addition to any fees that may be charged by your financial institution. This additional charge will be added to the transaction amount and posted to your account.

## Canada Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Canada Region only.

Fee Notice

The owner of this terminal, (name), may charge cardholders a fee for withdrawals from your account or cash advances. The amount of this fee will be disclosed on the terminal screen prior to your completion of the transaction. This fee is in addition to any fees that may be charged by your financial institution. This additional charge will be added to the transaction amount and posted to your account.

## Europe Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Europe Region only, except the United Kingdom.

### Fee Notice

The owner of this terminal, (name), may charge cardholders with a card issued in a country other than (country <sup>a</sup>) a fee for withdrawals from your account or cash advances. The amount of this fee will be disclosed on the terminal screen prior to your completion of the transaction. This fee is in addition to any fees that may be charged by your financial institution. This additional charge will be added to the transaction amount and posted to your account.

<sup>a</sup> Insert country where ATM is located.

### United Kingdom

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the United Kingdom only.

### Fee Notice

The owner of this terminal, (name), may charge cardholders a fee for withdrawals from your account or cash advances. The amount of this fee will be disclosed on the terminal screen prior to your completion of the transaction. This fee is in addition to any fees that may be charged by your financial institution. This additional charge will be added to the transaction amount and posted to your account.

## Latin America and the Caribbean Region

The following model form illustrates dimensions for ATM Terminal signage notification of an ATM Access Fee for Latin America and the Caribbean Region except the following countries: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.

Fee Notice

The owner of this terminal, (name), may charge cardholders with a card issued in a country other than (country <sup>a</sup>) a fee for withdrawals from your account or cash advances. The amount of this fee will be disclosed on the terminal screen prior to your completion of the transaction. This fee is in addition to any fees that may be charged by your financial institution. This additional charge will be added to the transaction amount and posted to your account.

<sup>a</sup> Insert country where ATM is located.

## Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for only the following countries in the Latin America and the Caribbean Region: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.

### Fee Notice

The owner of this terminal, (name), may charge cardholders a fee for withdrawals from your account or cash advances. The amount of this fee will be disclosed on the terminal screen prior to your completion of the transaction. This fee is in addition to any fees charged by your financial institution, will be added to the transaction amount, and posted to your account.

## Middle East/Africa Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Middle East/Africa Region.

### Fee Notice

The owner of this terminal, (name), may charge cardholders with a card issued in a country other than (country <sup>a</sup>) a fee for withdrawals from your account or cash advances. The amount of this fee will be disclosed on the terminal screen prior to your completion of the transaction. This fee is in addition to any fees that may be charged by your financial institution. This additional charge will be added to the transaction amount and posted to your account.

<sup>a</sup> Insert country where ATM is located.

## United States Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the United States only.

**Fee Notice**

The owner of this terminal, (name),  
may charge cardholders a fee for  
withdrawals from your account or  
cash advances. The amount of this  
fee will be disclosed on the terminal  
screen prior to your completion of  
the transaction. This fee is in  
addition to any fees that may be  
charged by your financial institution.  
This additional charge will be added  
to the transaction amount and  
posted to your account.

a    Insert country where ATM is located.

b    Insert currency code for the country where the ATM is located.

---

## Models for Screen Display Notification of an ATM Access Fee

Each of the following model forms illustrate the ATM Terminal screen display notification that an ATM Access Fee will be charged if the Cardholder chooses to proceed with the Transaction.

### Asia/Pacific Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Asia/Pacific Region, except Australia.



### Fee Notice

The owner of this terminal, (name), will charge cardholders with a card issued in a country other than (country <sup>a</sup>) (currency code <sup>b</sup>) (amount) as its fee for the transaction you have chosen. This fee is in addition to any fees your card-issuing financial institution may charge.

If you agree to this fee and wish to continue, press ---.

If you do not wish pay a fee and want to cancel this transaction, press ---.

a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

### Australia

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for Australia only.

### Fee Notice

The owner of this terminal, (name), will charge cardholders AUD (amount) as its fee for the transaction you have chosen. This fee is in addition to any fees your card-issuing financial institution may charge.

If you agree to this fee and wish to continue, press ---.

If you do not wish pay a fee and want to cancel this transaction, press ---.

## Canada Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for Canada only.

Fee Notice

The owner of this terminal, (name),  
will charge cardholders CAD  
(amount) as its fee for the  
transaction you have chosen. This  
fee is in addition to any fees your  
card-issuing financial institution may  
charge.

If you agree to this fee and wish to  
continue, press ---.

If you do not wish pay a fee and  
want to cancel this transaction, press  
---.

## Europe Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Europe Region, except the United Kingdom.

### Fee Notice

The owner of this terminal, (name),  
will charge cardholders with a card  
issued in a country other than  
(country <sup>a</sup>) (currency code <sup>b</sup>)  
(amount) as its fee for the  
transaction you have chosen. This  
fee is in addition to any fees your  
card-issuing financial institution may  
charge.

If you agree to this fee and wish to  
continue, press ---.

If you do not wish pay a fee and  
want to cancel this transaction, press  
---.

a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

### United Kingdom

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for United Kingdom only.

### Fee Notice

The owner of this terminal, (name),  
will charge cardholders GBP  
(amount) as its fee for the  
transaction you have chosen. This  
fee is in addition to any fees your  
card-issuing financial institution may  
charge.

If you agree to this fee and wish to  
continue, press ---.

If you do not wish pay a fee and  
want to cancel this transaction, press  
---.

## Latin America and the Caribbean Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Latin America and the Caribbean Region except the following countries: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.

Fee Notice

The owner of this terminal, (name),  
will charge cardholders with a card  
issued in a country other than  
(country <sup>a)</sup>) (currency code <sup>b)</sup>)  
(amount) as its fee for the  
transaction you have chosen. This  
fee is in addition to any fees your  
card-issuing financial institution may  
charge.

If you agree to this fee and wish to  
continue, press ---.

If you do not wish pay a fee and  
want to cancel this transaction, press  
---.

<sup>a</sup> Insert country where ATM is located.

<sup>b</sup> Insert currency code for the country where the ATM is located.

## Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for only the following countries in the Latin America and the Caribbean Region: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.

### Fee Notice

The owner of this terminal, (name), will charge cardholders (currency code <sup>a)</sup> (amount) as its fee for the transaction you have chosen. This fee is in addition to any fees your card-issuing financial institution may charge.

If you agree to this fee and wish to continue, press ---.

If you do not wish pay a fee and want to cancel this transaction, press ---.

<sup>a</sup> Insert currency code for the country where the ATM is located: Argentina (ARS), Brazil (BRL), Chile (CLP), Colombia (COP), Ecuador (USD), Mexico (MXN), Panama (PAB or USD), Peru (PEN), Puerto Rico (USD), or Venezuela (VEB).

## Middle East/Africa Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Middle East/Africa Region.

### Fee Notice

The owner of this terminal, (name),  
will charge cardholders with a card  
issued in a country other than  
(country <sup>a</sup>) (currency code <sup>b</sup>)  
(amount) as its fee for the  
transaction you have chosen. This  
fee is in addition to any fees your  
card-issuing financial institution may  
charge.

If you agree to this fee and wish to  
continue, press ---.

If you do not wish pay a fee and  
want to cancel this transaction, press  
---.

a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

## United States Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for United States only.

### Fee Notice

The owner of this terminal, (name),  
will charge cardholders USD  
(amount) as its fee for the  
transaction you have chosen. This  
fee is in addition to any fees your  
card-issuing financial institution may  
charge.

If you agree to this fee and wish to  
continue, press ---.

If you do not wish pay a fee and  
want to cancel this transaction, press  
---.

---

## Model for an ATM Access Fee Transaction Receipt

---

\$100.00	Paid to Cardholder
\$ 1.00	Terminal Owners Fee
\$101.00	Withdrawal from checking

---

---

## Model Screens Offering POI Currency Conversion

---

### Option A, Screen 1

YOU MAY PAY FOR THIS TRANSACTION IN YOUR HOME CURRENCY.	
CASH WITHDRAWAL	GBP 50.00
ACCESS FEE	GBP 1.50
TOTAL AMOUNT	GBP 51.50
TERMINAL EXCHANGE RATE	GBP 1.00 = EUR 1.25
TRANSACTION AMOUNT	EUR 64.38
<<< CHARGE MY ACCOUNT GBP 51.50	CHARGE MY ACCOUNT EUR 64.38 >>>

### Screen 2

MAKE SURE YOU UNDERSTAND THE COSTS OF CURRENCY CONVERSION AS THEY MAY BE DIFFERENT DEPENDING ON WHETHER YOU SELECT YOUR HOME CURRENCY OR THE TRANSACTION CURRENCY

<<< PROCEED WITH CONVERSION                      RETURN TO PREVIOUS SCREEN >>>

### Option B, Screen 1

PLEASE CHOOSE THE CURRENCY TO BE CHARGED TO YOUR ACCOUNT	
CASH WITHDRAWAL	GBP 50.00
ACCESS FEE	GBP 1.50
TOTAL AMOUNT	GBP 51.50
TERMINAL EXCHANGE RATE	GBP 1.00 = EUR 1.25
TRANSACTION AMOUNT WITH CONVERSION	EUR 64.38
	CHARGE MY ACCOUNT GBP 51.50                      >>>
	CHARGE MY ACCOUNT EUR 64.38                      >>>

### Screen 2

MAKE SURE YOU UNDERSTAND THE COSTS OF CURRENCY CONVERSION AS THEY MAY BE DIFFERENT DEPENDING ON WHETHER YOU SELECT YOUR HOME CURRENCY OR THE TRANSACTION CURRENCY

<<< PROCEED WITH CONVERSION

RETURN TO PREVIOUS SCREEN >>>

## Model Receipt for Withdrawal Completed with POI Currency Conversion

CASH WITHDRAWAL	GBP 50.00
ACCESS FEE	GBP 1.50
TOTAL AMOUNT	GBP 51.50
TERMINAL EXCHANGE RATE	GBP 1.00 = EUR 1.25
TRANSACTION AMOUNT	EUR 64.38

## Model Screen Displays for Offering Installment Payments

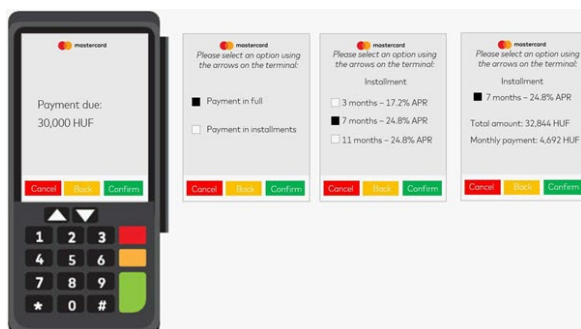
### Hungary

#### POS Terminal Displays in Hungarian





## POS Terminal Displays in English



## Poland

### POS Terminal Displays in Polish



### POS Terminal Displays in English



## E-commerce Displays in Polish


### AKCEPTANT / SKLEP

Zamówienie		
Szczegóły	Ilość	Kwota
xxxxxx	1	550 zł
<b>ŁĄCZNIE</b>		<b>550 zł</b>

**Dane do płatności**  
Właściciel karty  
Imię i nazwisko  
Numer karty  
5442 - xxxx - xxxx - xxx  
Ważna do 09/2021 CVC xxx  
☐ Przeczytałem i akceptuję regulamin  
Anuluj **Zapłać**

### AKCEPTANT / SKLEP

Zamówienie	
	Kwota
<b>ŁĄCZNIE</b>	<b>550 zł</b>

 **Płatność zaakceptowana**  
Właściciel karty  
Imię i nazwisko  
Numer karty  
5442 - xxxx - xxxx - xxx  
Numer transakcji:  
xyz  
**Czy chcesz rozłożyć zakup na raty?**  
Nie, dziękuję **Tak, rozkładam na raty**

### AKCEPTANT / SKLEP

Zamówienie		
	Kwota	
<b>ŁĄCZNIE</b>	<b>550 zł</b>	

**Wybierz liczbę rat na ile chcesz rozłożyć swój zakup**

Czas	Kwota raty	Łączna kwota do spłaty
<input type="checkbox"/> 3 miesiące	200 zł	600 zł
<input checked="" type="checkbox"/> 9 miesięcy	70 zł	630 zł
<input type="checkbox"/> 12 miesięcy	60 zł	720 zł

  
Wróć do sklepu **Dalej**

#### AKCEPTANT / SKLEP

Zamówienie

	Kwota
<b>ŁĄCZNIE</b>	<b>550 zł</b>

**Potwierdź wybór rozłożenia zakupu na raty**

Czas	Kwota raty	Łączna kwota do spłaty
▼ 9 miesięcy	70 zł	630 zł


Wróć do wyboru liczby rat

**Potwierdzam**

#### AKCEPTANT / SKLEP

Zamówienie

	Kwota
<b>ŁĄCZNIE</b>	<b>550 zł</b>

 **Dyspozycja rozłożenia na raty została zaakceptowana**

Plan ratowy zostanie uruchomiony. W razie pytań skontaktuj się ze swoim bankiem.

**Wróć do sklepu**

### E-commerce Displays in English

CUSTOMER EXPERIENCE DURING PURCHASE - E-COMMERCE

ENG

**MERCHANT NAME**

Your order


Details	Quantity	Price
xxxxxx	1	550 zł
<b>TOTAL</b>		<b>550 zł</b>

**Payment details**

Cardholder

Name

Card Number


5442 - xxxx - xxxx - xxxx 

Expires  CVC

09/2021

☒ I have read the Terms & Conditions

Cancel **Pay Now**

 **mastercard**

\* Proposition of splitting purchase into installments is proposed once positive authorization is granted by issuer and purchase meets specific criteria (e.g. purchase above 400 zł, bank offers this service etc. - conditions described in operational bulletin). Once installment plan is proposed there is no possibility to have transaction declined (transaction approved by issuer).

6

CUSTOMER EXPERIENCE  
DURING PURCHASE - ECOMMERCE

ENG

MERCHANT NAME

Your order

Price

TOTAL550 zł

✓

Payment has been processed

Cardholder

Name

Card Number

5442 - XXXX - XXXX - XXX

Transaction ID:

xyz

Do you want to split your purchase into installments?

No, thank you

Yes, pay with installments

\* Propagation of splitting purchase into installments is proposed once positive authorization is granted by issuer and purchase meets specific criteria (e.g. purchase above 400 zł, bank offers this service etc. - conditions described in operational bulletin). Once installment plan is proposed there is no possibility to have transaction declined (transaction approved by issuer).

7

CUSTOMER EXPERIENCE  
DURING PURCHASE - ECOMMERCE

ENG

MERCHANT NAME

Your order

Price

TOTAL550 zł

Select number of installments

Tenor	Installment amount	Total amount
<input type="checkbox"/> 3 months	200 zł	600 zł
<input checked="" type="checkbox"/> 6 months	110 zł	660 zł
<input type="checkbox"/> 12 months	60 zł	720 zł

Back to store

Continue

\* Propagation of splitting purchase into installments is proposed once positive authorization is granted by issuer and purchase meets specific criteria (e.g. purchase above 400 zł, bank offers this service etc. - conditions described in operational bulletin). Once installment plan is proposed there is no possibility to have transaction declined (transaction approved by issuer).

8

CUSTOMER EXPERIENCE  
DURING PURCHASE - ECOMMERCE

ENG

MERCHANT NAME

Your order

Price

TOTAL550 zł

Installments confirmation

Tenor	Installment amount	Total amount
<input checked="" type="checkbox"/> 6 months	110 zł	660 zł

Back to installments selection

Confirm

\* Propagation of splitting purchase into installments is proposed once positive authorization is granted by issuer and purchase meets specific criteria (e.g. purchase above 400 zł, bank offers this service etc. - conditions described in operational bulletin). Once installment plan is proposed there is no possibility to have transaction declined (transaction approved by issuer).

9

CUSTOMER EXPERIENCE  
DURING PURCHASE - E-COMMERCE

ENG

**MERCHANT NAME**

Your order

	Price
<b>TOTAL</b>	<b>550 zł</b>

**Request for installments has been processed**

Installment plan will be launched. If you have any questions, please contact your issuing bank.

[Back to store](#)

\* Proposal of splitting purchase into installments is proposed once positive authorization is granted by issuer and purchase meets specific criteria (e.g. purchase above 400 zł, bank offers this service etc. - conditions described in operational bulletin). Once installment plan is proposed there is no possibility to have transaction declined (transaction approved by issuer).

10

## Ukraine

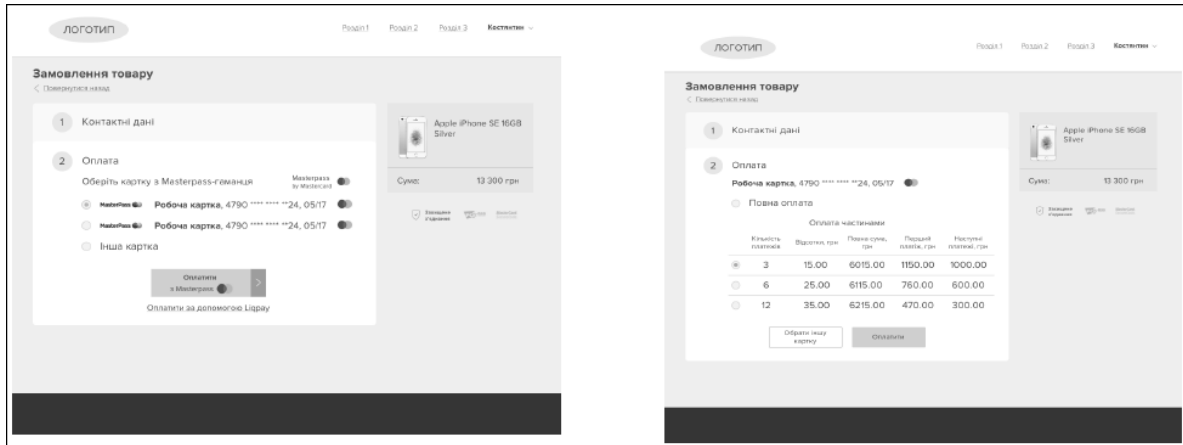
### POS Terminal Displays in Ukrainian



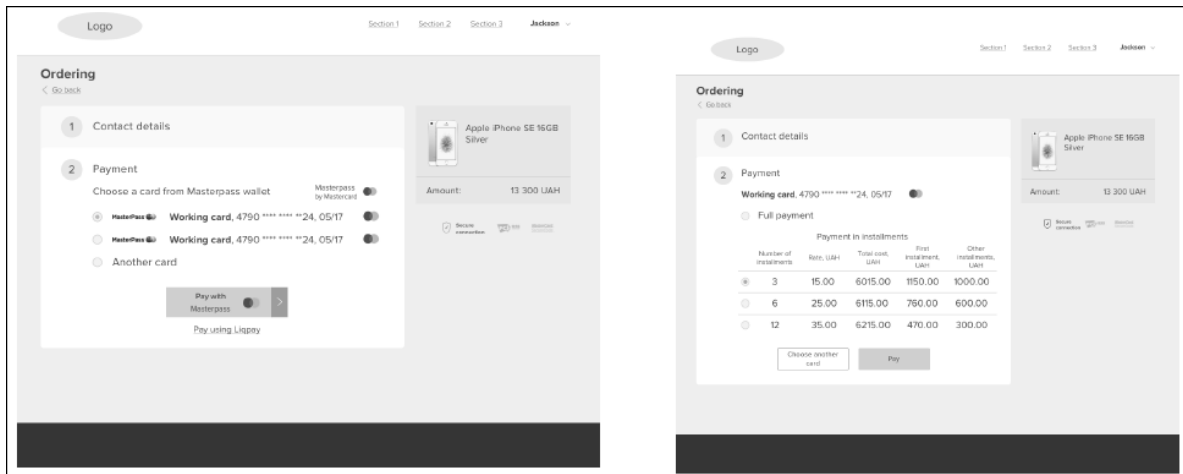
### POS Terminal Displays in English



## E-commerce Displays in Ukrainian



## E-commerce Displays in English



## Model Receipt Texts for Installments

### Czech Republic

For Receipts in Czech	For Receipts in English
"Celkové náklady: XXXXXXXX CZK"	"Total cost: XXXXXXXX CZK"
"Počet splátek: YY"	"Number of payments: YY"
"První splátka: XX CZK"	"First payment: XX CZK"
"Následující splátka: XX CZK"	"Subsequent payment"
"Úroková sazba: XX %"	"Interest rate:XX%"
"Roční procentní sazba nákladů: XX %"	"APR: XX%"
"Poplatek: XX CZK"	"Fee: XX CZK"

## Hungary

For Receipts in Hungarian	For Receipts in English
"Teljes összeg: XXX Ft"	"Total amount: XXX HUF"
"Részletek száma: YY"	"Number of payments: YY"
"Első Havi részlet: XX Ft"	"First Monthly payment: XX HUF"
"Havi részlet: XX Ft"	"Subsequent payment"
"Kamat: 00,X%"	"Interest rate: XX%" subfield 2.
"THM: 00,XX%"	"APR: XX,XX%"
"Díj: XX Ft"	"Fee: XX HUF"

## Poland

Language	Receipt Text
Polish	Plan ratałny zostanie uruchomiony. W razie pytań skontaktuj się ze swoim bankiem.
English	Installment plan will be launched. If you have any questions, please contact your issuing bank.



## Ukraine

For Receipts in Ukrainian	For Receipts in English
"Загальна вартість: XXXXXXXX ГРН"	"Total cost: XXXXXXXX UAH"
"Кількість платежів: YY"	"Number of payments: YY"
"Перший платіж: XX ГРН"	"First payment: XX UAH"
"Наступні платежі: XX ГРН"	"Subsequent payment"
"Реальна річна процентна ставка: XX%"	"Interest rate:XX%"
"Комісія: XX ГРН"	"Fee: XX UAH"
"З умовами та правилами, які застосовуються до послуги оплати частинами на [bank's WEB site address] ознайомлений та згоден"	"I've read and agree with the rules and conditions of payment in installments posted on [bank's WEBSITE address]"

---

## Appendix G Best Practices

---

Digital Goods Purchases.....	315
------------------------------	-----

## Digital Goods Purchases

---

A Merchant conducting e-commerce Transactions for the purchase of Digital Goods is advised to offer Cardholders, at a minimum, all of the following purchase controls:

- The option, enabled as a default setting, for the Cardholder to disable all Digital Goods purchases;
- The time period during which a Digital Goods purchase can be made on the Cardholder's account with the Merchant (the "account open" period) should not exceed 15 minutes after the Cardholder's entry of account authentication credentials;
- Functionality that allows the Cardholder to confirm or to cancel the clearly displayed total Transaction amount of each pending Digital Goods purchase before completion of the Transaction.

If a Merchant conducting e-commerce Transactions of under USD 25 for the purchase of Digital Goods does not implement these purchase controls, the Acquirer may be subject to chargebacks under message reason code 4841 (Cancelled Recurring Transactions and Digital Goods Purchases Under USD 25).

The following additional Digital Goods purchase controls are strongly recommended for **application** (for example, games, books, and music downloaded onto an electronic device) and **in-application** (for example, game pieces, books, and music used within a multi-player electronic game) purchases:

- Cardholder authentication for each purchase if purchasing is enabled (no default option); and
- The closure of the "account open" period immediately after completion of the initial purchase.

For **application** purchases:

- The maximum number of Transactions permitted during the "account open" period should not exceed 10 Transactions, with a maximum of one Transaction as the default setting; and
- The maximum Transaction amount permitted during the "account open" period should be no more than USD 500 (or the local currency equivalent), with a maximum Transaction amount of USD 100 (or the local currency equivalent) as the default setting.

For **in-application** purchases:

- The maximum number of Transactions permitted during the "account open" period should not exceed 30 transactions, with a maximum of one Transaction as the default setting; and
- The maximum Transaction amount during the "account open" period should not exceed USD 100 (or the local currency equivalent), with a maximum Transaction amount of USD 10 (or the local currency equivalent) as the default setting.

The Merchant should use the default settings set forth above if a Cardholder has not established purchase control settings. If established, the Merchant must honor a Cardholder's purchase control settings.

## Appendix H Definitions

*This appendix contains defined terms used in this manual. Additional and/or revised terms may also appear in a particular chapter or section of this manual.*

Acceptance Mark.....	322
Access Device.....	322
Account.....	322
Account Enablement System.....	322
Account Holder.....	323
Account PAN.....	323
Account PAN Range.....	323
Acquirer.....	323
Activity(ies).....	323
Affiliate Customer, Affiliate.....	323
Area of Use.....	323
Association Customer, Association.....	324
ATM Access Fee.....	324
ATM Owner Agreement.....	324
Automated Teller Machine (ATM).....	324
ATM Terminal.....	324
ATM Transaction.....	324
Bank Branch Terminal.....	325
BIN.....	325
Brand Fee.....	325
Brand Mark.....	325
Card.....	325
Cardholder.....	325
Cardholder Communication.....	325
Cardholder Verification Method (CVM).....	326
Chip Card (Smart Card, Integrated Circuit Card, IC Card, or ICC).....	326
Chip-only MPOS Terminal.....	326
Chip Transaction.....	326
Cirrus Acceptance Mark.....	327
Cirrus Access Device.....	327
Cirrus Account.....	327
Cirrus Brand Mark.....	327
Cirrus Card.....	327

---

Cirrus Customer.....	327
Cirrus Payment Application.....	327
Cirrus Word Mark.....	328
Competing ATM Network.....	328
Competing International ATM Network.....	328
Competing EFT POS Network.....	328
Competing North American ATM Network.....	329
Consumer Device Cardholder Verification Method, Consumer Device CVM, CDCVM.....	329
Contact Chip Transaction.....	329
Contactless Payment Device.....	329
Contactless Transaction.....	329
Control, Controlled.....	330
Corporation.....	330
Corporation System.....	330
Credentials Management System.....	330
Cross-border Transaction.....	330
Customer.....	331
Customer Report.....	331
Data Storage Entity (DSE).....	331
Device Binding.....	331
Digital Activity(ies).....	331
Digital Activity Agreement.....	332
Digital Activity Customer.....	332
Digital Activity Service Provider (DASP).....	332
Digital Activity Sponsoring Customer.....	332
Digital Goods.....	332
Digital Wallet.....	332
Digital Wallet Operator (DWO).....	332
Digital Wallet Operator Mark, DWO Mark.....	333
Digital Wallet Operator (DWO) Security Incident, DWO Security Incident .....	333
Digitization, Digitize.....	333
Domestic Transaction.....	333
Dual Interface.....	333
Electronic Money.....	333
Electronic Money Issuer.....	334
Electronic Money Institution.....	334
EMV Mode Contactless Transaction.....	334
Gateway Customer.....	334
Gateway Processing.....	334

---

Gateway Transaction.....	334
Global Collection Only (GCO) Data Collection Program.....	334
Host Card Emulation (HCE).....	335
Hybrid Terminal.....	335
ICA.....	335
Identification & Verification (ID&V).....	335
Independent Sales Organization (ISO).....	335
Interchange System.....	336
Inter-European Transaction.....	336
Interregional Transaction.....	336
Intracountry Transaction.....	336
Intra-European Transaction.....	336
Intra-Non-SEPA Transaction.....	337
Intraregional Transaction.....	337
Issuer.....	337
License, Licensed.....	337
Licensee.....	337
Maestro.....	337
Maestro Acceptance Mark.....	337
Maestro Access Device.....	338
Maestro Account.....	338
Maestro Brand Mark.....	338
Maestro Card.....	338
Maestro Customer.....	338
Maestro Payment Application.....	338
Maestro Word Mark.....	338
Magnetic Stripe Mode Contactless Transaction.....	339
Manual Cash Disbursement Transaction.....	339
Marks.....	339
Mastercard.....	339
Mastercard Acceptance Mark.....	339
Mastercard Access Device.....	339
Mastercard Account.....	339
Mastercard Biometric Card.....	340
Mastercard-branded Application Identifier (AID).....	340
Mastercard Brand Mark.....	340
Mastercard Card.....	340
Mastercard Cloud-Based Payments.....	340
Mastercard Consumer-Presented QR Transaction.....	340

---

Mastercard Customer.....	341
Mastercard Digital Enablement Service.....	341
Mastercard Europe.....	341
Mastercard Incorporated.....	341
Mastercard Payment Application.....	341
Mastercard Safety Net.....	341
Mastercard Symbol.....	342
Mastercard Token.....	342
Mastercard Token Account Range.....	342
Mastercard Token Vault.....	342
Mastercard Word Mark.....	342
Member, Membership.....	343
Merchandise Transaction.....	343
Merchant.....	343
Merchant Agreement.....	343
Merchant Token Requestor.....	343
Mobile Payment Device.....	343
Mobile POS (MPOS) Terminal.....	344
MoneySend Payment Transaction.....	344
Multi-Account Chip Card.....	344
Non-Mastercard Funding Source.....	344
Non-Mastercard Receiving Account.....	344
Non-Mastercard Systems and Networks Standards.....	344
On-behalf Token Requestor.....	344
On-Device Cardholder Verification.....	345
Originating Account Holder.....	345
Originating Institution (OI).....	345
Ownership, Owned.....	345
Participation.....	345
Pass-through Digital Wallet.....	345
Pass-through Digital Wallet Operator (DWO).....	345
Payment Account Reference (PAR).....	346
Payment Application.....	346
Payment Facilitator.....	346
Payment Transaction.....	346
Payment Transfer Activity(ies) (PTA).....	346
Personal Data.....	346
Point of Interaction (POI).....	347
Point-of-Sale (POS) Terminal.....	347

---

Point-of-Sale (POS) Transaction.....	347
Portfolio.....	347
Principal Customer, Principal.....	347
Processed PTA Transaction.....	347
Processed Transaction.....	348
Program.....	348
Program Service.....	348
PTA Account.....	348
PTA Account Number.....	348
PTA Account Portfolio.....	349
PTA Agreement.....	349
PTA Customer.....	349
PTA Originating Account.....	349
PTA Program.....	349
PTA Receiving Account.....	349
PTA Settlement Guarantee Covered Program.....	349
PTA Settlement Obligation .....	350
PTA Transaction.....	350
Quick Response (QR) Code .....	350
Receiving Account Holder.....	350
Receiving Agent.....	350
Receiving Customer.....	350
Receiving Institution (RI).....	350
Region.....	350
Remote Electronic Transaction.....	351
Rules.....	351
Service Provider.....	351
Settlement Obligation.....	351
Shared Deposit Transaction.....	351
Solicitation, Solicit.....	351
Special Issuer Program.....	352
Sponsor, Sponsorship.....	352
Sponsored Digital Activity Entity.....	352
Staged Digital Wallet.....	352
Staged Digital Wallet Operator (DWO).....	353
Standards.....	353
Stand-In Parameters.....	353
Stand-In Processing Service.....	353
Strong Customer Authentication (SCA).....	353



---

Sub-licensee.....	353
Submerchant.....	354
Submerchant Agreement.....	354
Terminal.....	354
Third Party Processor (TPP).....	354
Token.....	354
Tokenization, Tokenize.....	354
Token Requestor.....	354
Token Vault.....	355
Transaction.....	355
Transaction Data.....	355
Transaction Management System.....	355
Trusted Service Manager.....	355
Virtual Account.....	355
Volume.....	356
Wallet Token Requestor.....	356
Word Mark.....	356

## Acceptance Mark

---

Any one of the Corporation's Marks displayed at a Point of Interaction (POI) to indicate brand acceptance. See Cirrus Acceptance Mark, Maestro Acceptance Mark, Mastercard Acceptance Mark.

## Access Device

---

A device other than a Card that has successfully completed all applicable Mastercard certification and testing requirements, if any, and:

- Uses at least one Payment Application provisioned to the device by or with the approval of a Customer to provide access to an Account;
- Supports the transmission or exchange of data using one or both of the following:
  - Magnetic stripe or chip data containing a dynamic cryptogram to or with a Terminal, as applicable, by implementing the EMV Contactless Specifications (Book D) to effect Transactions at the Terminal without requiring direct contact of the device to the Terminal
  - Chip data containing a dynamic cryptogram to or with a Terminal, as applicable, by implementing the Mastercard Cloud-Based Payments (MCBP) documentation to effect Transactions at the Terminal by capture of a QR Code containing the Transaction Data
- May also support the transmission of magnetic stripe data containing a dynamic cryptogram to a Terminal to effect Transactions identified by the Acquirer in Transaction messages as magnetic stripe Transactions.

A Cirrus Access Device, Maestro Access Device, and Mastercard Access Device is each an Access Device. *Also see Mobile Payment Device.*

## Account

---

An account maintained by or on behalf of a Cardholder by an Issuer for the processing of Transactions, and which is identified with a bank identification number (BIN) or Issuer identification number (IIN) designated by the Corporation in its routing tables for routing to the Interchange System. *Also see Cirrus Account, Maestro Account, Mastercard Account.*

## Account Enablement System

---

Performs Account enablement services for Mastercard Cloud-Based Payments, which may include Account and Access Device eligibility checks, Identification & Verification (ID&V), Digitization, and subsequent lifecycle management.

---

## Account Holder

---

A user who holds a PTA Account and has agreed to participate in a PTA Transaction.

---

## Account PAN

---

The primary account number (PAN) allocated to an Account by an Issuer.

---

## Account PAN Range

---

The range of Account PANs designated by an Issuer for Digitization.

---

## Acquirer

---

A Customer in its capacity as an acquirer of a Transaction.

---

## Activity(ies)

---

The undertaking of any lawful act that can be undertaken only pursuant to a License granted by the Corporation. Payment Transfer Activity is a type of Activity. *Also see Digital Activity(ies).*

---

## Affiliate Customer, Affiliate

---

A Customer that participates indirectly in Activity through the Sponsorship of a Principal or, solely with respect to Mastercard Activity, through the Sponsorship of an Association. An Affiliate may not Sponsor any other Customer.

---

## Area of Use

---

The country or countries in which a Customer is Licensed to use the Marks and conduct Activity or in which a PTA Customer is permitted to Participate in a PTA Program, and, as a rule, set forth in the License or PTA Agreement or in an exhibit to the License or PTA Agreement.

## **Association Customer, Association**

---

A Mastercard Customer that participates directly in Mastercard Activity using its assigned BINs and which may Sponsor one or more Mastercard Affiliates but may not directly issue Mastercard Cards or acquire Mastercard Transactions, or in the case of a PTA Association, may not directly hold PTA Accounts, without the express prior written consent of the Corporation.

## **ATM Access Fee**

---

A fee charged by an Acquirer in connection with a cash withdrawal or Shared Deposit Transaction initiated at the Acquirer's ATM Terminal with a Card, and added to the total Transaction amount transmitted to the Issuer.

## **ATM Owner Agreement**

---

An agreement between an ATM owner and a Customer that sets forth the terms pursuant to which the ATM accepts Cards.

## **Automated Teller Machine (ATM)**

---

An unattended self-service device that performs basic banking functions such as accepting deposits, cash withdrawals, ordering transfers among accounts, loan payments and account balance inquiries.

## **ATM Terminal**

---

An ATM that enables a Cardholder to effect a Transaction with a Card in accordance with the Standards.

## **ATM Transaction**

---

A cash withdrawal effected at an ATM Terminal with a Card and processed through the Mastercard ATM Network. An ATM Transaction is identified with MCC 6011 (Automated Cash Disbursements—Customer Financial Institution).

## Bank Branch Terminal

---

An attended device, located on the premises of a Customer or other financial institution designated as its authorized agent by the Corporation, that facilitates a Manual Cash Disbursement Transaction by a Cardholder.

## BIN

---

A bank identification number (BIN, sometimes referred to as an Issuer identification number, or IIN) is a unique number assigned by Mastercard for use by a Customer in accordance with the Standards.

## Brand Fee

---

A fee charged for certain Transactions not routed to the Interchange System.

## Brand Mark

---

A Word Mark as a custom lettering legend placed within the Corporation's interlocking circles device. The Mastercard Brand Mark, Maestro Brand Mark, and Cirrus Brand Mark is each a Brand Mark. The Mastercard Symbol is also a Brand Mark.

## Card

---

A card issued by a Customer pursuant to License and in accordance with the Standards and that provides access to an Account. Unless otherwise stated herein, Standards applicable to the use and acceptance of a Card are also applicable to an Access Device and, in a Card-not-present environment, an Account. A Cirrus Card, Maestro Card, and Mastercard Card is each a Card.

## Cardholder

---

The authorized user of a Card or Access Device issued by a Customer.

## Cardholder Communication

---

Any communication by or on behalf of an Issuer to a Cardholder or prospective Cardholder. A Solicitation is one kind of Cardholder Communication.

## Cardholder Verification Method (CVM)

---

A process used to confirm that the person presenting the Card is an authorized Cardholder. The Corporation deems the following to be valid CVMs when used in accordance with the Standards:

- The comparison, by the Merchant or Acquirer accepting the Card, of the signature on the Card's signature panel with the signature provided on the Transaction receipt by the person presenting the Card;
- The comparison, by the Card Issuer or the EMV chip on the Card, of the value entered on a Terminal's PIN pad with the personal identification number (PIN) given to or selected by the Cardholder upon Card issuance; and
- The use of a Consumer Device CVM (CDCVM) that Mastercard approved as a valid CVM for Transactions upon the successful completion of the certification and testing procedures set forth in section 3.11 of the *Security Rules and Procedures*.

In certain Card-present environments, a Merchant may complete the Transaction without a CVM ("no CVM" as the CVM), such as in Quick Payment Service (QPS) Transactions, Contactless Transactions less than or equal to the CVM limit, and Transactions at an unattended Point-of-Sale (POS) Terminal identified as Cardholder-activated Terminal (CAT) Level 2 or Level 3.

## Chip Card (Smart Card, Integrated Circuit Card, IC Card, or ICC)

---

A Card with an embedded EMV-compliant chip containing memory and interactive capabilities used to identify and store additional data about a Cardholder, an Account, or both.

## Chip-only MPOS Terminal

---

An MPOS Terminal that has a contact chip reader and no magnetic stripe-reading capability and that must:

1. Operate as an online-only POS Terminal for authorization purposes;
2. Support either signature or No CVM Required as a Cardholder Verification Method, and may also support PIN verification if conducted by means of a PIN entry device (PED) that is in compliance with the Payment Card Industry (PCI) POS PED Security Requirements and Evaluation Program; and
3. Otherwise comply with the Corporation's requirements for Hybrid POS Terminals.

## Chip Transaction

---

A Contact Chip Transaction or a Contactless Transaction.

## Cirrus Acceptance Mark

---

A Mark consisting of the Cirrus Brand Mark placed on the dark blue acceptance rectangle, available at [www.mastercardbrandcenter.com](http://www.mastercardbrandcenter.com).

## Cirrus Access Device

---

An Access Device that uses at least one Cirrus Payment Application to provide access to a Cirrus Account when used at an ATM Terminal or Bank Branch Terminal.

## Cirrus Account

---

An account eligible to be a Cirrus Account, as set forth in Rule 6.1.3.2 of the *Mastercard Rules* manual, and identified with a BIN/IIN associated with a Portfolio designated by the Corporation as a Cirrus Portfolio in its routing tables.

## Cirrus Brand Mark

---

A Mark consisting of the Cirrus Word Mark as a custom lettering legend placed within the Corporation's interlocking circles device. The Corporation is the exclusive owner of the Cirrus Brand Mark.

## Cirrus Card

---

A Card that provides access to a Cirrus Account.

## Cirrus Customer

---

A Customer that has been granted a Cirrus License in accordance with the Standards.

## Cirrus Payment Application

---

A Payment Application that stores Cirrus Account data.

## **Cirrus Word Mark**

---

A Mark consisting of the word “Cirrus” followed by a registered trademark ® or ™ symbol (depending on its trademark status in a particular country) or the local law equivalent. “Cirrus” must appear in English and be spelled correctly, with the letter “C” capitalized. “Cirrus” must not be abbreviated, hyphenated, used in the plural or possessive, or translated from English into another language. The Corporation is the exclusive owner of the Cirrus Word Mark.

## **Competing ATM Network**

---

A Competing International ATM Network or a Competing North American ATM Network, as the case may be.

## **Competing International ATM Network**

---

A network of ATMs and payment cards, other than the Corporation, identified by a common brand mark that is used exclusively or primarily for ATM interchange that:

1. Operates in at least three countries;
2. Uses a common service mark or marks to identify the ATMs and payment cards which provide account access through it; and
3. Provides account access to at least 40,000,000 debit cards and by means of at least 25,000 ATMs.

## **Competing EFT POS Network**

---

A network, other than any network owned and operated by the Corporation, which provides access to Maestro Accounts at POS Terminals by use of payment cards and has the following characteristics:

1. It provides a common service mark or marks to identify the POS Terminal and payment cards, which provide Maestro Account access;
2. It is not an affiliate of the Corporation; and
3. It operates in at least one country in which the Corporation has granted a License or Licenses.

The following networks are designated without limitation to be Competing EFT POS Networks: Interlink; Electron; and V-Pay.



## Competing North American ATM Network

---

A network of ATMs and access cards, other than the Corporation, identified by a common brand mark that is used exclusively or primarily for ATM interchange and that possesses each of the following characteristics:

1. It operates in at least 40 of the states or provinces of the states and provinces of the United States and Canada;
2. It uses a common service mark or common service marks to identify the terminals and cards which provide account access through it;
3. There are at least 40,000,000 debit cards that provide account access through it; and
4. There are at least 12,000 ATMs that provide account access through it.

## Consumer Device Cardholder Verification Method, Consumer Device CVM, CDCVM

---

A CVM that occurs when personal credentials established by the Cardholder to access an Account by means of a particular Access Device are entered on the Access Device and verified, either within the Access Device or by the Issuer during online authorization. A CDCVM is valid if the Issuer has approved the use of the CVM for the authentication of the Cardholder.

## Contact Chip Transaction

---

A Transaction in which data is exchanged between the Chip Card and the Terminal through the reading of the chip using the contact interface, in conformance with EMV specifications.

## Contactless Payment Device

---

A means other than a Card by which a Cardholder may access an Account at a Terminal in accordance with the Standards. A Contactless Payment Device is a type of Access Device that exchanges data with the Terminal by means of radio frequency communications. *Also see* Mobile Payment Device.

## Contactless Transaction

---

A Transaction in which data is exchanged between the Chip Card or Access Device and the Terminal through the reading of the chip using the contactless interface, by means of radio frequency communications. *Also see* EMV Mode Contactless Transaction, Magnetic Stripe Mode Contactless Transaction.

## **Control, Controlled**

---

As used herein, Control has such meaning as the Corporation deems appropriate in its sole discretion given the context of the usage of the term and all facts and circumstances the Corporation deems appropriate to consider. As a general guideline, Control often means to have, alone or together with another entity or entities, direct, indirect, legal, or beneficial possession (by contract or otherwise) of the power to direct the management and policies of another entity.

## **Corporation**

---

Mastercard International Incorporated, Maestro International Inc., and their subsidiaries and affiliates. As used herein, Corporation also means the President and Chief Executive Officer of Mastercard International Incorporated, or his or her designee, or such officers or other employees responsible for the administration and/or management of a program, service, product, system or other function. Unless otherwise set forth in the Standards, and subject to any restriction imposed by law or regulation, or by the Board of Directors of Mastercard International Incorporated, or by the Mastercard International Incorporated Certificate of Incorporation or the Mastercard Incorporated Certificate of Incorporation (as each such Certificate of Incorporation may be amended from time to time), each such person is authorized to act on behalf of the Corporation and to so act in his or her sole discretion.

## **Corporation System**

---

The Interchange System as defined in this manual.

## **Credentials Management System**

---

Facilitates credential preparation and/or remote mobile Payment Application management for Mastercard Cloud-Based Payments.

## **Cross-border Transaction**

---

A Transaction that occurs at a Card acceptance location in a different country from the country in which the Card was issued.

---

## Customer

---

A financial institution or other entity that has been approved for Participation. A Customer may be a Principal, Association, Affiliate, Digital Activity Customer, Sponsored Digital Activity Entity, or PTA Customer. Also see Cirrus Customer, Maestro Customer, Mastercard Customer, Member.

---

## Customer Report

---

Any report that a Customer is required to provide to the Corporation, whether on a one-time or repeated basis, pertaining to its License, Activities, Digital Activity Agreement, Digital Activities, PTA Agreement, Payment Transfer Activities, use of any Mark, or any such matters. By way of example and not limitation, the Quarterly Mastercard Report (QMR) is a Customer Report.

---

## Data Storage Entity (DSE)

---

A Service Provider that performs any one or more of the services described in Rule 7.1 of the *Mastercard Rules* manual as DSE Program Service.

---

## Device Binding

---

The process by which a Wallet Token Requestor binds a Mastercard Token corresponding to a Cardholder's Account to that Cardholder's Mobile Payment Device, which may consist of:

- The provisioning of the Token and its associated encryption keys into the secure element within the Mobile Payment Device;
- The loading of an application for a remotely-managed secure server into the Mobile Payment Device and the successful communication of the device with the application; or
- Other methodology acceptable to the Corporation.

---

## Digital Activity(ies)

---

The undertaking of any lawful act pursuant to approval by the Corporation as set forth in a Digital Activity Agreement or other written documentation. Participation in the Mastercard Digital Enablement Service as a Wallet Token Requestor is a Digital Activity.

## Digital Activity Agreement

---

The contract between the Corporation and a Digital Activity Customer granting the Digital Activity Customer the right to participate in Digital Activity and a limited License to use one or more of the Marks in connection with such Digital Activity, in accordance with the Standards.

## Digital Activity Customer

---

A Customer that participates in Digital Activity pursuant to a Digital Activity Agreement and which may not issue Cards, acquire Transactions, or Sponsor any other Customer into the Corporation.

## Digital Activity Service Provider (DASP)

---

A Service Provider that performs any one or more of the services described in Rule 7.1 of the *Mastercard Rules* as DASP Program Service.

## Digital Activity Sponsoring Customer

---

A Principal Customer or Digital Activity Customer that sponsors a Sponsored Digital Activity Entity to participate in Digital Activity.

## Digital Goods

---

Any goods that are stored, delivered, and used in electronic format, such as, by way of example but not limitation, books, newspapers, magazines, music, games, game pieces, and software (excluding gift cards). The delivery of a purchase of Digital Goods may occur on a one-time or subscription basis.

## Digital Wallet

---

A Pass-through Digital Wallet or a Staged Digital Wallet.

## Digital Wallet Operator (DWO)

---

A Service Provider that operates a Staged Digital Wallet or a Customer that operates a Pass-through Digital Wallet. A Merchant that stores Mastercard or Maestro Account data solely on its own behalf to effect Transactions initiated by the consumer is not deemed to be a DWO.

## Digital Wallet Operator Mark, DWO Mark

---

A Mark identifying a particular Pass-through Digital Wallet and/or Staged Digital Wallet, and which may be displayed at the POI to denote that a retailer, or any other person, firm, or corporation, accepts payments effected by means of that Pass-through Digital Wallet and/or Staged Digital Wallet. A “Staged DWO Mark” and a “Pass-through DWO Mark” are both types of DWO Marks.

## Digital Wallet Operator (DWO) Security Incident, DWO Security Incident

---

Any incident pertaining to the unintended or unlawful disclosure of Personal Data in connection with such Personal Data being processed through a DWO.

## Digitization, Digitize

---

Data preparation performed by, or on behalf of, an Issuer prior to the provisioning of Account credentials or a PTA Customer prior to the provisioning of PTA Account credentials, in the form of a Mastercard Token, onto a Payment Device or into a server. Digitization includes Tokenization.

## Domestic Transaction

---

See Intracountry Transaction.

## Dual Interface

---

The description of a Terminal or Card that is capable of processing Contactless Transactions by means of its contactless interface and Contact Chip Transactions by means of its contact interface.

## Electronic Money

---

Electronically (including magnetically) accessed monetary value as represented by a claim on the Electronic Money Issuer which:

1. Is issued on receipt of funds for the purpose of making transactions with payment cards; and

2. Is accepted by the Electronic Money Issuer or a person other than the Electronic Money Issuer.

---

## **Electronic Money Issuer**

---

An Electronic Money Institution with respect only to its issuing activities.

---

## **Electronic Money Institution**

---

An entity authorized by applicable regulatory authority or other government entity as an “electronic money institution”, “e-money institution”, “small electronic money institution”, or any other applicable qualification under which an entity is authorized to issue or acquire Electronic Money transactions under applicable law or regulation.

---

## **EMV Mode Contactless Transaction**

---

A Contactless Transaction in which the Terminal and the chip exchange data, enabling the chip to approve the Transaction offline on the Issuer’s behalf or to request online authorization from the Issuer, in compliance with the Standards.

---

## **Gateway Customer**

---

A Customer that uses the Gateway Processing service.

---

## **Gateway Processing**

---

A service that enables a Customer to forward a Gateway Transaction to and/or receive a Gateway Transaction from the Mastercard ATM Network®.

---

## **Gateway Transaction**

---

An ATM transaction effected with a payment card or other access device not bearing a Mark that is processed through or using the Mastercard ATM Network®.

---

## **Global Collection Only (GCO) Data Collection Program**

---

A program of the Corporation pursuant to which a Customer must provide collection-only reporting of non-Processed Transactions effected with a Card, Access Device, or Account

issued under a Mastercard-assigned BIN via the Corporation's Global Clearing Management System (GCMS), in accordance with the requirements set forth in the *Mastercard Global Collection Only* manual.

## Host Card Emulation (HCE)

---

The presentation on a Mobile Payment Device of a virtual and exact representation of a Chip Card using only software on the Mobile Payment Device and occurring by means of its communication with a secure remote server.

## Hybrid Terminal

---

A Terminal, including any POS or MPOS Terminal ("Hybrid POS Terminal", "Hybrid MPOS Terminal"), ATM Terminal ("Hybrid ATM Terminal"), or Bank Branch Terminal ("Hybrid Bank Branch Terminal"), that:

1. Is capable of processing both Contact Chip Transactions and magnetic stripe Transactions;
2. Has the equivalent hardware, software, and configuration as a Terminal with full EMV Level 1 and Level 2 type approval status with regard to the chip technical specifications; and
3. Has satisfactorily completed the Corporation's Terminal Integration Process (TIP) in the appropriate environment of use.

## ICA

---

A unique number assigned by the Corporation to identify a Customer in relation to Activity.

## Identification & Verification (ID&V)

---

The identification and verification of a person as the Cardholder to whom the Issuer allocated the Account PAN to be Tokenized.

## Independent Sales Organization (ISO)

---

A Service Provider that performs any one or more of the services described in Rule 7.1 of the *Mastercard Rules* manual as ISO Program Service.

## Interchange System

---

The computer hardware and software operated by and on behalf of the Corporation for the routing, processing, and settlement of Transactions and PTA Transactions including, without limitation, the Mastercard Network, the Mastercard ATM Network, the Dual Message System, the Single Message System, the Global Clearing Management System (GCMS), and the Settlement Account Management (SAM) system.

## Inter-European Transaction

---

A Transaction completed using a Card issued in a country or territory listed in Single European Payments Area (SEPA) at a Terminal located in a country or territory listed in Non-Single European Payments Area (Non-SEPA) or Transaction completed using a Card issued in a country or territory listed in Non-Single European Payments Area (Non-SEPA) at a Terminal located in a country or territory listed in Single European Payments Area (SEPA).

## Interregional Transaction

---

A Transaction that occurs at a Card acceptance location in a different Region from the Region in which the Card was issued. In the Europe Region, the term “Interregional Transaction” includes any “Inter-European Transaction,” as such term is defined in the “Europe Region” chapter of the *Mastercard Rules*.

## Intracountry Transaction

---

A Transaction that occurs at a Card acceptance location in the same country as the country in which the Card was issued. A Transaction conducted with a Card bearing one or more of the Brand Marks, either alone or in combination with the marks of another payment scheme, and processed as a Transaction, as shown by the Card type identification in the Transaction record, via either the Interchange System or a different network, qualifies as an Intracountry Transaction. “Domestic Transaction” is an alternative term for Intracountry Transaction.

## Intra-European Transaction

---

An Intra-Non-SEPA Transaction or an Intra-SEPA Transaction, but not an Inter-European Transaction.



## Intra–Non–SEPA Transaction

---

A Transaction completed using a Card issued in a country or territory listed in Non–Single European Payments Area (Non–SEPA) at a Terminal located in a country or territory listed in Non–Single European Payments Area (Non–SEPA).

## Intraregional Transaction

---

A Transaction that occurs at a Card acceptance location in a different country from the country in which the Card was issued, within the same Region. In the Europe Region, this term is replaced by “Intra-European Transaction,” as such term is defined in the “Europe Region” chapter of the *Mastercard Rules*.

## Issuer

---

A Customer in its capacity as an issuer of a Card or Account.

## License, Licensed

---

The contract between the Corporation and a Customer granting the Customer the right to use one or more of the Marks in accordance with the Standards and in the case of Payment Transfer Activity, includes a PTA Agreement. To be “Licensed” means to have such a right pursuant to a License.

## Licensee

---

A Customer or other person authorized in writing by the Corporation to use one or more of the Marks.

## Maestro

---

Maestro International Incorporated, a Delaware U.S.A. corporation or any successor thereto.

## Maestro Acceptance Mark

---

A Mark consisting of the Maestro Brand Mark placed on the dark blue acceptance rectangle, as available at [www.mastercardbrandcenter.com](http://www.mastercardbrandcenter.com).

## Maestro Access Device

---

An Access Device that uses at least one Maestro Payment Application to provide access to a Maestro Account when used at a Terminal.

## Maestro Account

---

An account eligible to be a Maestro Account, as set forth in Rule 6.1.2.1 of the *Mastercard Rules* manual, and identified with a BIN/IIN associated with a Portfolio designated by the Corporation as a Maestro Portfolio in its routing tables.

## Maestro Brand Mark

---

A Mark consisting of the Maestro Word Mark as a custom lettering legend placed within the Corporation's interlocking circles device. The Corporation is the exclusive owner of the Maestro Brand Mark.

## Maestro Card

---

A Card that provides access to a Maestro Account.

## Maestro Customer

---

A Customer that has been granted a Maestro License in accordance with the Standards.

## Maestro Payment Application

---

A Payment Application that stores Maestro Account data.

## Maestro Word Mark

---

A Mark consisting of the word "Maestro" followed by a registered trademark ® or ™ symbol (depending on its trademark status in a particular country) or the local law equivalent. "Maestro" must appear in English and be spelled correctly, with the letter "M" capitalized. "Maestro" must not be abbreviated, hyphenated, used in the plural or possessive, or translated from English into another language. Maestro is the exclusive owner of the Maestro Word Mark.

## Magnetic Stripe Mode Contactless Transaction

---

A Contactless Transaction in which the Terminal receives static and dynamic data from the chip and constructs messages that can be transported in a standard magnetic stripe message format, in compliance with the Standards.

## Manual Cash Disbursement Transaction

---

A disbursement of cash performed upon the acceptance of a Card by a Customer financial institution teller. A Manual Cash Disbursement Transaction is identified with MCC 6010 (Manual Cash Disbursements—Customer Financial Institution).

## Marks

---

The names, logos, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks that the Corporation owns, manages, licenses, or otherwise Controls and makes available for use by Customers and other authorized entities in accordance with a License. A “Mark” means any one of the Marks.

## Mastercard

---

Mastercard International Incorporated, a Delaware U.S.A. corporation.

## Mastercard Acceptance Mark

---

A Mark consisting of the Mastercard Brand Mark or Mastercard Symbol placed on the dark blue acceptance rectangle, as available at [www.mastercardbrandcenter.com](http://www.mastercardbrandcenter.com).

## Mastercard Access Device

---

An Access Device that uses at least one Mastercard Payment Application to provide access to a Mastercard Account when used at a Terminal.

## Mastercard Account

---

Any type of account (credit, debit, prepaid, commercial, etc.) identified as a Mastercard Account with a primary account number (PAN) that begins with a BIN in the range of 222100 to 272099 or 510000 to 559999.

## Mastercard Biometric Card

---

A Mastercard or Maestro Chip Card containing a fingerprint sensor and compliant with the Corporation's biometric Standards.

## Mastercard-branded Application Identifier (AID)

---

Any of the Corporation's EMV chip application identifiers for Mastercard, Maestro, and Cirrus Payment Applications as defined in the *M/Chip Requirements* manual.

## Mastercard Brand Mark

---

A Mark consisting of the Mastercard Word Mark as a custom lettering legend placed within the Mastercard Interlocking Circles Device. The Corporation is the exclusive owner of the Mastercard Brand Mark. The Mastercard Symbol is also a Mastercard Brand Mark.

## Mastercard Card

---

A Card that provides access to a Mastercard Account.

## Mastercard Cloud-Based Payments

---

A specification that facilitates the provisioning of Digitized Account data into a Host Card Emulation (HCE) server and the use of the remotely stored Digitized Account data, along with single-use payment credentials, in Transactions effected by a Cardholder using a Mobile Payment Device. The Mastercard Digital Enablement Service offers Mastercard Cloud-Based Payments as an on-behalf service.

## Mastercard Consumer-Presented QR Transaction

---

A Mastercard Consumer-Presented QR Transaction is an EMV Chip Transaction effected through the presentment of a QR Code by the Cardholder, using a Mobile Payment Device, and the capture of the QR Code by the Merchant containing the Transaction Data required to initiate a Transaction.

Each Mastercard Consumer-Presented QR Transaction must comply with all requirements set forth in the Standards applicable to a Mastercard Consumer-Presented QR Transaction, including but not limited to those herein, in the technical specifications for authorization

---

messages, in the *MIChip Requirements for Contact and Contactless* manual, and in the Mastercard Cloud-Based Payments (MCBP) documentation.

## **Mastercard Customer**

---

A Customer that has been granted a Mastercard License in accordance with the Standards. Also see Member.

## **Mastercard Digital Enablement Service**

---

Any of the services offered by the Corporation exclusively to Customers for the digital enablement of Account and/or PTA Account data, including but not limited to ID&V Service, Tokenization Service, Digitization Service, Token Mapping Service, Mastercard Cloud-Based Payments, Digital Card Image Database, CVC 3 pre-validation and other on-behalf cryptographic validation services, and Service Requests.

## **Mastercard Europe**

---

Mastercard Europe SA, a Belgian private limited liability (company).

## **Mastercard Incorporated**

---

Mastercard Incorporated, a Delaware U.S.A. corporation.

## **Mastercard Payment Application**

---

A Payment Application that stores Mastercard Account data.

## **Mastercard Safety Net**

---

A service offered by the Corporation that performs fraud monitoring at the network level for all Transactions processed on the Mastercard Network. The service invokes targeted measures to provide protective controls on behalf of a participating Issuer to assist in minimizing losses in the event of a catastrophic fraud attack.

## Mastercard Symbol

---

A Mark consisting of the Mastercard interlocking circles device. The Corporation is the exclusive owner of the Mastercard Symbol. The Mastercard Symbol is also a Mastercard Brand Mark.

## Mastercard Token

---

A Token allocated from a Mastercard Token Account Range that the Corporation has designated to an Issuer or PTA Customer and that corresponds to an Account PAN or a PTA Account Number. The Corporation exclusively owns all right, title, and interest in any Mastercard Token.

## Mastercard Token Account Range

---

A bank identification number (BIN) or portion of a BIN ("BIN range") designated by the Corporation to an Issuer or PTA Customer for the allocation of Mastercard Tokens in a particular Token implementation. A Mastercard Token Account Range must be designated from a BIN reserved for the Corporation by the ISO Registration Authority and for which the Corporation is therefore the "BIN Controller," as such term is defined in the EMV Payment Tokenization Specification Technical Framework (also see the term "Token BIN Range" in that document). A Mastercard Token Account Range is identified in the Corporation's routing tables as having the same attributes as the corresponding Account PAN Range or the range of PTA Account Numbers.

## Mastercard Token Vault

---

The Token Vault owned and operated by Mastercard and enabled by means of the Mastercard Digital Enablement Service.

## Mastercard Word Mark

---

A Mark consisting of the word "Mastercard" followed by a registered trademark ® symbol or the local law equivalent. "Mastercard" must appear in English and be spelled correctly, with the letters "M" and "C" capitalized. "Mastercard" must not be abbreviated, hyphenated, used in the plural or possessive, or translated from English into another language. The Corporation is the exclusive owner of the Mastercard Word Mark.

## Member, Membership

---

A financial institution or other entity that is approved to be a Mastercard Customer in accordance with the Standards and which, as a Mastercard Customer, has been granted membership (“Membership”) in and has become a member (“Member”) of the Corporation. “Membership” also means “Participation”.

## Merchandise Transaction

---

The purchase by a Cardholder of merchandise or a service, but not currency, in an approved category at an ATM Terminal and dispensed or otherwise provided by such ATM Terminal. A Merchandise Transaction is identified with MCC 6012 (Merchandise and Services—Customer Financial Institution), unless otherwise specified.

## Merchant

---

A retailer, or any other person, firm or corporation that, pursuant to a Merchant Agreement, agrees to accept Cards when properly presented.

## Merchant Agreement

---

An agreement between a Merchant and a Customer that sets forth the terms pursuant to which the Merchant is authorized to accept Cards.

## Merchant Token Requestor

---

A Merchant Token Requestor is a Merchant that connects directly to the Mastercard Digital Enablement Service (MDES) for the purpose of Tokenizing a Mastercard or Maestro Account primary account number (PAN) provided by a Cardholder for use in a future Transaction with the Merchant. A Merchant Token Requestor is a type of Token Requestor.

## Mobile Payment Device

---

A Cardholder-controlled mobile device containing a Payment Application compliant with the Standards, and which uses an integrated keyboard and screen to access an Account. A Mobile Payment Device may also be a Contactless Payment Device or a Mastercard Consumer-Presented QR payment device.

## **Mobile POS (MPOS) Terminal**

---

An MPOS Terminal enables a mobile device to be used as a POS Terminal. Card “reading” and software functionality that meets the Corporation’s requirements may reside within the mobile device, on a server accessed by the mobile device, or in a separate accessory connected (such as via Bluetooth or a USB port) to the mobile device. The mobile device may be any multi-purpose mobile computing platform, including, by way of example and not limitation, a feature phone, smart phone, tablet, or personal digital assistant (PDA).

## **MoneySend Payment Transaction**

---

A type of Payment Transaction that is effected pursuant to, and subject to, the MoneySend Standards.

## **Multi-Account Chip Card**

---

A Chip Card with more than one Account encoded in the chip.

## **Non-Mastercard Funding Source**

---

Any funding source used to fund a PTA Transaction other than an Account.

## **Non-Mastercard Receiving Account**

---

Any receiving account used to receive a PTA Transaction other than an Account.

## **Non-Mastercard Systems and Networks Standards**

---

The applicable rules, regulations, by-laws, standards, procedures, and any other obligations or requirements of an applicable payment network or system that is not owned, operated, or controlled by the Corporation.

## **On-behalf Token Requestor**

---

A Digital Activity Customer or other Customer, approved by the Corporation to conduct Digital Activity and authorized to Tokenize a Mastercard or Maestro primary account number (PAN) using the Mastercard Digital Enablement Service (MDES) on behalf of a DWO or Merchant.



## **On-Device Cardholder Verification**

---

The use of a CDCVM as the CVM for a Transaction.

## **Originating Account Holder**

---

The Account Holder originating the PTA Transaction.

## **Originating Institution (OI)**

---

A PTA Customer that Participates in a Payment Transfer Activity as an originator of PTA Transactions.

## **Ownership, Owned**

---

As used herein, ownership has such meaning as the Corporation deems appropriate in its sole discretion given the context of the usage of the term in all facts and circumstances the Corporation deems appropriate to consider. As a general guideline, ownership often means to own indirectly, legally, or beneficially more than fifty percent (50 percent) of an entity.

## **Participation**

---

The right to participate in Activity, Digital Activity, and/or Payment Transfer Activity granted to a Customer by the Corporation. For a Mastercard Customer, Participation is an alternative term for Membership.

## **Pass-through Digital Wallet**

---

Functionality which can be used at more than one Merchant, and by which the Pass-through Digital Wallet Operator stores Mastercard or Maestro Account data provided by the Cardholder to the DWO for purposes of effecting a payment initiated by the Cardholder to a Merchant or Submerchant, and upon the performance of a Transaction, transfers the Account data to the Merchant or Submerchant or to its Acquirer or the Acquirer's Service Provider.

## **Pass-through Digital Wallet Operator (DWO)**

---

A Digital Activity Customer or other Customer, approved by the Corporation to engage in Digital Activity, that operates a Pass-through Digital Wallet.

## Payment Account Reference (PAR)

---

A unique non-financial alphanumeric value assigned to an Account PAN or PTA Account Number that is used to link the Account PAN or PTA Account Number to all of its corresponding Tokens.

## Payment Application

---

A package of code and data stored in a Card, an Access Device, a server, or a combination of Access Device and server, that when exercised outputs a set of data that may be used to effect a Transaction, in accordance with the Standards. A Mastercard Payment Application, Maestro Payment Application, and Cirrus Payment Application is each a Payment Application.

## Payment Facilitator

---

A Service Provider registered by an Acquirer to facilitate the acquiring of Transactions by the Acquirer from Submerchants, and which in doing so, performs any one or more of the services described in Rule 7.1 of the *Mastercard Rules* manual as PF Program Service.

## Payment Transaction

---

A PTA Transaction that transfers funds to an Account. A Payment Transaction is not a credit that reverses a previous purchase. Includes MoneySend Payment Transactions.

## Payment Transfer Activity(ies) (PTA)

---

The undertaking of any lawful act that can be undertaken only pursuant to a PTA Agreement or pursuant to a License granted by the Corporation. Participation in a PTA Program is Payment Transfer Activity.

## Personal Data

---

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.

## Point of Interaction (POI)

---

The location at which a Transaction occurs or a PTA Transaction originates, as determined by the Corporation.

## Point-of-Sale (POS) Terminal

---

An attended or unattended device located in or at a Merchant's premises, including an MPOS Terminal, that enables a Cardholder to effect a Transaction for the purchase of products or services sold by such Merchant with a Card and/or Access Device, or attended device located in the premises of a Customer or its authorized agent that facilitates a Manual Cash Disbursement Transaction, including a Bank Branch Terminal. A POS Terminal must comply with the POS Terminal security and other applicable Standards.

## Point-of-Sale (POS) Transaction

---

The sale of products or services by a Merchant to a Cardholder pursuant to acceptance of a Card by the Merchant or Manual Cash Disbursement Transaction. A POS Transaction may be a Card-present Transaction taking place in a face-to-face environment or at an unattended POS Terminal, or a Card-not-present Transaction taking place in a non-face-to-face environment (for example, an e-commerce, mail order, phone order, or recurring payment Transaction).

## Portfolio

---

All Cards issued bearing the same major industry identifier, BIN/IIN, and any additional digits that uniquely identify Cards for routing purposes.

## Principal Customer, Principal

---

A Customer that participates directly in Activity using its assigned BINs/IINs and which may Sponsor one or more Affiliates.

## Processed PTA Transaction

---

A PTA Transaction which is:

1. Initiated by or on behalf of the Originating Institution via the Corporation System in accordance with the Standards; and

2. Cleared, meaning the Originating Institution transferred the PTA Transaction data within the applicable time frame to the Corporation via the Corporation System, for the purpose of a transfer of funds via the Corporation System, and such PTA Transaction data is subsequently transferred by the Corporation to the Receiving Customer for such purpose.

---

## Processed Transaction

---

A Transaction which is:

1. Authorized by the Issuer via the Interchange System, unless a properly processed offline Chip Transaction approval is obtained or no authorization is required, in accordance with the Standards; and
2. Cleared, meaning the Acquirer transferred the Transaction Data within the applicable presentment time frame to the Corporation via the Interchange System, for the purpose of a transfer of funds via the Interchange System, and such Transaction Data is subsequently transferred by the Corporation to the Issuer for such purpose.

---

## Program

---

A Customer's Card issuing program, Merchant acquiring program, ATM Terminal acquiring program, Digital Activity program, and/or a PTA Program in which a Customer is Participating.

---

## Program Service

---

Any service described in Rule 7.1 of the *Mastercard Rules* manual or elsewhere in the Standards that directly or indirectly supports a Program and regardless of whether the entity providing the service is registered as a Service Provider of one or more Customers. The Corporation has the sole right to determine whether a service is a Program Service.

---

## PTA Account

---

A PTA Originating Account and/or a PTA Receiving Account.

---

## PTA Account Number

---

The account number allocated to a PTA Account by a PTA Customer.

## **PTA Account Portfolio**

---

All PTA Accounts issued by a PTA Customer.

## **PTA Agreement**

---

The agreement between the Corporation and a PTA Customer granting the PTA Customer the right to Participate in a PTA Program, in accordance with the Standards.

## **PTA Customer**

---

A Customer that Participates in a PTA Program pursuant to a PTA Agreement.

## **PTA Originating Account**

---

The funding source of the Originating Account Holder, from where funds are acquired by the Originating Institution to initiate a PTA Transaction.

## **PTA Program**

---

A type of Payment Transfer Activity that is identified in the applicable Standards as being a PTA Program, including the MoneySend Program, the Mastercard Merchant Presented QR Program, and the Mastercard Send Cross-Border Service.

## **PTA Receiving Account**

---

The Account or, if applicable for a particular PTA Program (as set forth in the Standards for such PTA Program), the Non-Mastercard Receiving Account, held by a Receiving Account Holder and to which the Receiving Customer must ensure receipt of a PTA Transaction.

## **PTA Settlement Guarantee Covered Program**

---

A PTA Settlement Obligation arising from a PTA Transaction conducted pursuant to a PTA Program that is identified in the applicable Standards as being a PTA Settlement Guarantee Covered Program.

## PTA Settlement Obligation

---

A financial obligation of a Principal or Association PTA Customer to another Principal or Association PTA Customer arising from a PTA Transaction.

## PTA Transaction

---

A financial transaction in which funds are transferred from an Originating Institution to a Receiving Customer on behalf of Account Holders pursuant to a PTA Program.

## Quick Response (QR) Code

---

An ISO 18004-compliant encoding and visualization of data.

## Receiving Account Holder

---

The Account Holder receiving the PTA Transaction.

## Receiving Agent

---

A PTA Customer that Participates in Payment Transfer Activity as an agent for the purpose of receiving a PTA Transaction.

## Receiving Customer

---

A Receiving Agent or a Receiving Institution.

## Receiving Institution (RI)

---

A PTA Customer that Participates in Payment Transfer Activity as a receiver of PTA Transactions on behalf of a Receiving Account Holder.

## Region

---

A geographic region as defined by the Corporation from time to time. See Appendix A of the *Mastercard Rules* manual.

## Remote Electronic Transaction

---

In the Europe Region, all types of Card-not-present Transaction (e-commerce Transactions, recurring payments, installments, Card-on-file Transactions, in-app Transactions, and Transactions completed through a Digital Wallet, including Masterpass™). Mail order and telephone order (MO/TO) Transactions and Transactions completed with anonymous prepaid Cards are excluded from this definition.

## Rules

---

The Standards set forth in this manual.

## Service Provider

---

A person that performs Program Service. The Corporation has the sole right to determine whether a person is or may be a Service Provider and if so, the category of Service Provider. A Service Provider is an agent of the Customer that receives or otherwise benefits from Program Service, whether directly or indirectly, performed by such Service Provider.

## Settlement Obligation

---

A financial obligation of a Principal or Association Customer to another Principal or Association Customer arising from a Transaction.

## Shared Deposit Transaction

---

A deposit to a savings Account or checking Account conducted at an ATM Terminal located in the U.S. Region, initiated with a Card issued by a U.S. Region Customer other than the Acquirer, and processed through the Mastercard ATM Network.

## Solicitation, Solicit

---

An application, advertisement, promotion, marketing communication, or the like distributed as printed materials, in electronic format (including but not limited to an email, website, mobile application, or social media platform), or both intended to solicit the enrollment of a person or entity as a Cardholder or Account Holder or as a Merchant. To "Solicit" means to use a Solicitation.

## Special Issuer Program

---

Issuer Activity that the Corporation deems may be undertaken only with the express prior consent of the Corporation. As of the date of the publication of these Rules, Special Issuer Programs include Affinity Card Programs, Co-Brand Card Programs, and Prepaid Card Programs, and with respect to Mastercard Activity only, Brand Value Transaction and proprietary account, Remote Transaction Mastercard Account, and secured Mastercard Card Programs.

## Sponsor, Sponsorship

---

The relationship described in the Standards between a Principal or Association and an Affiliate that engages in Activity indirectly through the Principal or Association. In such event, the Principal or Association is the Sponsor of the Affiliate and the Affiliate is Sponsored by the Principal or Association. "Sponsorship" means the Sponsoring of a Customer.

## Sponsored Digital Activity Entity

---

A wholly-owned subsidiary (or other affiliated entity as approved by the Corporation) of a Digital Activity Sponsoring Customer. The Sponsored Digital Activity Entity may be approved at the sole discretion of the Corporation to participate in Digital Activity pursuant to a Digital Activity Agreement or other agreement with the Corporation.

## Staged Digital Wallet

---

Functionality that can be used at more than one retailer, and by which the Staged Digital Wallet Operator effects a two-stage payment to a retailer to complete a purchase initiated by a Cardholder. The following may occur in either order:

- **Payment stage**—In the payment stage, the Staged DWO pays the retailer by means of:
  - A proprietary non-Mastercard method (and not with a Mastercard Card); or
  - A funds transfer to an account held by the Staged DWO for or on behalf of the retailer.
- **Funding stage**—In the funding stage, the Staged DWO uses a Mastercard or Maestro Account provided to the Staged DWO by the Cardholder (herein, the "funding account") to perform a transaction that funds or reimburses the Staged Digital Wallet.

The retailer does not receive Mastercard or Maestro Account data or other information identifying the network brand and payment card issuer for the funding account.



## **Staged Digital Wallet Operator (DWO)**

---

A registered Service Provider that operates a Staged Digital Wallet.

## **Standards**

---

The organizational documents, operating rules, regulations, policies, and procedures of the Corporation, including but not limited to any manuals, guides, announcements or bulletins, as may be amended from time to time.

## **Stand-In Parameters**

---

A set of authorization requirements established by the Corporation or the Issuer that are accessed by the Interchange System using the Stand-In Processing Service to determine the appropriate responses to authorization requests.

## **Stand-In Processing Service**

---

A service offered by the Corporation in which the Interchange System authorizes or declines Transactions on behalf of and uses Stand-In Parameters provided by the Issuer (or in some cases, by the Corporation). The Stand-In Processing Service responds only when the Issuer is unavailable, the Transaction cannot be delivered to the Issuer, or the Issuer exceeds the response time parameters set by the Corporation.

## **Strong Customer Authentication (SCA)**

---

Authentication as required by the 2nd Payment Services Directive (Directive [EU] 2015/2366 of 25 November 2015) Regulatory Technical Standards on Strong Customer Authentication (as amended and replaced from time to time).

## **Sub-licensee**

---

A person authorized in writing to use a Mark either by a Licensee in accordance with the Standards or by the Corporation.

---

## Submerchant

---

A merchant that, pursuant to an agreement with a Payment Facilitator, is authorized to accept Cards when properly presented.

---

## Submerchant Agreement

---

An agreement between a Submerchant and a Payment Facilitator that sets forth the terms pursuant to which the Submerchant is authorized to accept Cards.

---

## Terminal

---

Any attended or unattended device that meets the Corporation requirements for the electronic capture and exchange of Account data and that permits a Cardholder to effect a Transaction in accordance with the Standards. An ATM Terminal, Bank Branch Terminal, and POS Terminal is each a type of Terminal.

---

## Third Party Processor (TPP)

---

A Service Provider that performs any one or more of the services described in Rule 7.1 of the *Mastercard Rules* manual as TPP Program Service.

---

## Token

---

A numeric value that (i) is a surrogate for the primary account number (PAN) used by a payment card issuer to identify a payment card account or is a surrogate for the PTA Account Number used by a PTA Customer to identify a PTA Account; (ii) is issued in compliance with the EMV Payment Tokenization Specification Technical Framework; and (iii) passes the basic validation rules for a PAN, including the Luhn Formula for Computing Modulus 10 Check Digit. Also see Mastercard Token.

---

## Tokenization, Tokenize

---

The process by which a Mastercard Token replaces an Account PAN or a PTA Account Number.

---

## Token Requestor

---

An entity that requests the replacement of Account PANs with Mastercard Tokens.

---

## Token Vault

---

A repository of tokens that are implemented by a tokenization system, which may also perform primary account number (PAN) mapping and cryptography validation.

---

## Transaction

---

A financial transaction arising from the proper acceptance of a Card or Account bearing or identified with one or more of the Brand Marks, either alone or in combination with the marks of another payment scheme, at a Card acceptance location and identified in messages with a Card Program identifier.

---

## Transaction Data

---

Any data and/or data element or subelement that the Standards and/or the Corporation's interface specifications require to be used to initiate, authorize, clear, and/or settle a Transaction or PTA Transaction (whether authorized, cleared, and/or settled via the Interchange System or otherwise) or that the Corporation requires to be provided.

---

## Transaction Management System

---

Performs Transaction management services for Mastercard Cloud-Based Payments, which may include credential authentication, application cryptogram mapping and validation, ensuring synchronization with the Credentials Management System, and forwarding of Transactions to the Issuer for authorization.

---

## Trusted Service Manager

---

Provisions an Access Device with the Payment Application, personalization data, or post-issuance application management commands by means of an over-the-air (OTA) communication channel.

---

## Virtual Account

---

A Mastercard Account issued without a physical Card or Access Device. A Virtual Account cannot be electronically read.

## Volume

---

The aggregate financial value of a group of Transactions. “Volume” does not mean the number of Transactions.

## Wallet Token Requestor

---

A Wallet Token Requestor is a Pass-through DWO that connects directly to the Mastercard Digital Enablement Service (MDES) for the purpose of Tokenizing a Mastercard or Maestro Account primary account number (PAN) provided by a Cardholder for use in a future Transaction.

## Word Mark

---

A Mark consisting of the name of one of the Corporation’s brands followed by a registered trademark ® or ™ symbol (depending on its trademark status in a particular country) or the local law equivalent. See Cirrus Word Mark, Maestro Word Mark, Mastercard Word Mark.

## Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

### Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively “Mastercard”), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

### Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

### Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

### Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers “AS IS” and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

### Information Available Online

Mastercard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on Mastercard Connect™. Go to Publications [Support](#) for centralized information.