Transaction Processing Rules

10 June 2025

TPR

Contents

Transaction Processing Rules overview....18

Applicability of Rules in this Manual....22

Chapter 1: Connecting to the Interchange System and Authorization Routing....24

1.1 Connecting to the Interchange System....26
1.2 Authorization Routing - Mastercard POS Transactions....26
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions....27
1.3.1 Routing Instructions and System Maintenance....27
1.3.2 Chip Transaction Routing....27
1.3.3 Domestic Transaction Routing....28
1.4 ATM Terminal Connection to the Interchange System....28
1.5 Gateway Processing....28
1.6 POS Terminal Connection to the Interchange System....29
Variations and Additions by Region....29
Asia/Pacific Region....29
1.4 ATM Terminal Connection to the Interchange System....29
1.6 POS Terminal Connection to the Interchange System....29
Canada Region....30
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions....30
1.3.3 Domestic Transaction Routing....30
1.4 ATM Terminal Connection to the Interchange System....30
Europe Region....30
1.1 Connecting to the Interchange System....30
1.2 Authorization Routing—Mastercard POS Transactions....31
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions....31
1.3.2 Chip Transaction Routing....31
1.3.3 Domestic Transaction Routing....31
1.4 ATM Terminal Connection to the Interchange System—SEPA Only....31
Latin America and the Caribbean Region....32
1.4 ATM Terminal Connection to the Interchange System....32
1.6 POS Terminal Connection to the Interchange System....32
United States Region....32
1.1 Connecting to the Interchange System....32
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions....32
1.3.1 Routing Instructions and System Maintenance....32
1.3.3 Domestic Transaction Routing....33

1.4 ATM Terminal Connection to the Interchange System....33
Additional U.S. Region and U.S. Territory Rules....33
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions....34

Chapter 2: Authorization and Clearing Requirements....35
2.1 Acquirer Authorization Requirements....39
2.1.1 Acquirer Host System Requirements....40
2.2 Issuer Authorization Requirements....40
2.2.1 Issuer Host System Requirements....42
2.2.2 Stand-In Processing Service....43
Accumulative Transaction Limits....43
Chip Cryptogram Validation in Stand-In....44
2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers....44
2.3 Authorization Responses....44
2.4 Performance Standards....45
2.4.1 Performance Standards—Acquirer Requirements....45
2.4.2 Performance Standards—Issuer Requirements....45
Issuer Failure Rate (Substandard Level 1)....45
Issuer Failure Rate (Substandard Level 2)....46
Calculation of the Issuer Failure Rate....46
2.5 Preauthorizations....46
2.5.1 Preauthorizations - Mastercard POS Transactions....46
2.5.2 Preauthorizations - Maestro POS Transactions....47
2.5.3 Preauthorizations - ATM and Manual Cash Disbursement Transactions....47
2.6 Undefined Authorizations....47
2.7 Final Authorizations....48
2.8 Message Reason Code 4808 Chargeback Protection Period....49
2.9 Multiple Authorizations....49
2.10 Clearing, Completion, and Chargeback Message Requirements....50
2.10.1 Multiple Clearing or Completion Messages....50
2.10.1.1 Mastercard and Debit Mastercard Transactions....51
2.10.2 Maestro Transactions....52
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....54
2.11.3 Reversal for Conversion of Approval to Decline....54
2.11.4 Reversal to Cancel Transaction....55
2.12 Full and Partial Approvals....55
2.13 Refund Transactions and Corrections....58
2.13.1 Refund Transactions - Acquirer Requirements....58
2.13.2 Refund Transactions - Issuer Requirements....59
2.14 Balance Inquiries....60

2.15 CVC 2 Verification for POS Transactions....61
2.16 CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless Transactions—Brazil Only....61
2.17 Euro Conversion—Europe Region Only....61
2.18 Transaction Clearing, Queries, and Disputes....61
2.18.1 Clearing Requirements....61
2.18.2 Compliance with Dispute Procedures....62
2.19 Chargebacks for Reissued Cards....62
2.20 Correction of Errors....62
2.21 Merchant Payment Gateway Identifier (MPG ID)....62
2.22 Co-badged Cards - Acceptance Brand Identifier....63
Variations and Additions by Region....63
Asia/Pacific Region....63
2.1 Acquirer Authorization Requirements....63
2.1.1 Acquirer Host System Requirements....64
2.2 Issuer Authorization Requirements....64
2.2.1 Issuer Host System Requirements....64
2.3 Authorization Responses....65
2.5 Preauthorizations....65
2.5.1 Preauthorizations - Mastercard POS Transactions....65
2.5.2 Preauthorizations—Maestro POS Transactions....65
2.7 Final Authorization....65
2.8 Message Reason Code 4808 Chargeback Protection Period....66
2.11 Full and Partial Reversals....66
2.11.1 Full and Partial Reversals—Acquirer Requirements....66
2.12 Full and Partial Approvals....66
2.13 Refund Transactions and Corrections....67
2.13.1 Refund Transactions - Acquirer Requirements....67
Canada Region....68
2.1 Acquirer Authorization Requirements....68
2.1.1 Acquirer Host System Requirements....68
2.2 Issuer Authorization Requirements....68
2.12 Full and Partial Approvals....69
Europe Region....69
2.1 Acquirer Authorization Requirements....69
2.2 Issuer Authorization Requirements....71
2.2.2 Stand-In Processing Service....72
2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers....72
2.3 Authorization Responses....72
2.4 Performance Standards....73
2.4.2 Performance Standards—Issuer Requirements....73
2.5 Preauthorizations....73
2.5.2 Preauthorizations—Maestro POS Transactions....73

2.5.3 Preauthorizations—ATM and Manual Cash Disbursement Transactions....74
2.7 Final Authorizations....75
2.8 Message Reason Code 4808 Chargeback Protection Period....75
2.9 Multiple Authorizations....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....77
2.12 Full and Partial Approvals....77
2.13 Refund Transactions and Corrections....78
2.13.1 Refund Transactions—Acquirer Requirements....78
2.13.2 Refund Transactions—Issuer Requirements....78
2.14 Balance Inquiries....78
2.15 CVC 2 Verification for POS Transactions....78
2.17 Euro Conversion....79
2.22 Co-badged Cards - Acceptance Brand Identifier....79
Latin America and the Caribbean Region....80
2.2 Issuer Authorization Requirements....80
2.2.1 Issuer Host System Requirements....80
2.5 Preauthorizations....80
2.5.2 Preauthorizations - Maestro POS Transactions....80
2.6 Undefined Authorizations....80
2.9 Multiple Authorizations....81
2.10 Multiple Clearing or Multiple Completion Messages....82
2.10.2 Maestro Transactions....82
2.16 CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless—Brazil Only....84
Middle East/Africa Region....84
2.1 Acquirer Authorization Requirements....84
2.7 Final Authorizations....85
2.12 Full and Partial Approvals....86
2.21 Merchant Payment Gateway Identifier (MPG ID)....86
United States Region....86
2.1 Acquirer Authorization Requirements....86
2.1.1 Acquirer Host System Requirements....86
2.2 Issuer Authorization Requirements....86
2.2.1 Issuer Host System Requirements....87
2.2.2 Stand-In Processing Service....87
2.4 Performance Standards....89
2.4.2 Performance Standards—Issuer Requirements....89
2.5 Preauthorizations....89
2.5.2 Preauthorizations—Maestro POS Transactions....89
2.11 Full and Partial Reversals....89
2.11.1 Full and Partial Reversals—Acquirer Requirements....89
2.11.2 Full and Partial Reversals—Issuer Requirements....90

2.14 Balance Inquiries....90
Additional U.S. Region and U.S. Territory Rules....90
2.2 Issuer Authorization Requirements....90
2.2.2 Stand-In Processing Service....90
2.5 Preauthorizations....90
2.5.2 Preauthorizations—Maestro POS Transactions....91
2.9 Multiple Authorizations....91
2.10 Multiple Clearing and Multiple Completion Messages....92
2.10.2 Maestro Transactions....93
2.18 Transaction Clearing, Queries, and Disputes....94

Chapter 3: Acceptance Procedures....96
3.1 Card-Present Transactions....99
3.1.1 Mastercard Card Acceptance Procedures....99
Suspicious Cards....99
3.1.2 Maestro Card Acceptance Procedures....100
3.2 Card-Not-Present Transactions....100
3.3 Obtaining an Authorization....100
3.3.1 Mastercard POS Transaction Authorization Procedures....100
Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions....102
Authorization When the Cardholder Adds a Gratuity....102
Card-Not-Present Transaction Declines....103
Use of Card Validation Code (CVC) 2....104
Capture Card Response....104
3.3.2 Maestro POS Transaction Authorization Procedures....104
3.4 Mastercard Cardholder Verification Requirements....104
CVM Not Required for Refund Transactions....105
Use of PIN for Mastercard Magnetic Stripe Transactions....105
3.5 Maestro Cardholder Verification Requirements....106
3.6 Use of a PIN for Transactions at ATM Terminals and Bank Branch Terminals....106
3.7 Use of a Consumer Device CVM....107
3.8 POI Currency Conversion....107
3.8.1 Cardholder Disclosure Requirements....108
3.8.2 Cardholder Disclosure - Transaction Receipt Information....109
3.8.3 Priority Check-Out....110
3.8.4 Transaction Processing Requirements....110
3.9 Multiple Transactions—Mastercard POS Transactions Only....110
3.10 Partial Payment—Mastercard POS Transactions Only....111
3.11 Specific Terms of a Transaction....111
3.11.1 Specific Terms of an E-commerce Transaction....111
3.12 Charges for Loss, Theft, or Damage—Mastercard POS Transactions Only....112
3.13 Transaction Receipts....112

3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements....114
3.13.2 ATM and Bank Branch Terminal Transaction Receipt Requirements....115
3.13.3 Primary Account Number (PAN) Truncation and Expiration Date Omission....116
3.13.4 Prohibited Information....116
3.13.5 Standard Wording for Formsets....116
3.14 Returned Products and Canceled Services....117
3.14.1 Refund Transactions....118
3.15 Transaction Records....119
3.15.1 Transaction Presentment Time Frames....119
3.15.2 Retention of Transaction Records....120
Variations and Additions by Region....120
Asia/Pacific Region....120
3.14 Returned Products and Canceled Services....120
3.14.1 Refund Transactions....120
3.15 Transaction Records....120
3.15.1 Transaction Presentment Time Frames....120
Europe Region....121
3.1 Card-Present Transactions....121
3.1.1 Mastercard Card Acceptance Procedures....121
3.2 Card-Not-Present Transactions....121
3.3 Obtaining an Authorization....121
3.3.1 Mastercard POS Transaction Authorization Procedures....121
Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions....122
Authorization When the Cardholder Adds a Gratuity....122
3.3.2 Maestro POS Transaction Authorization Procedures....122
3.5 Maestro Cardholder Verification Requirements....122
3.8 POI Currency Conversion....123
3.13 Transaction Receipts....123
3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements....124
3.13.3 Primary Account Number (PAN) Truncation and Expiration Date Omission....124
3.14 Returned Products and Canceled Services....125
3.14.1 Refund Transactions....125
Latin America and the Caribbean Region....126
3.4 Mastercard Cardholder Verification Requirements....126
3.5 Maestro Cardholder Verification Requirements....126
Middle East/Africa Region....126
3.14 Returned Products and Canceled Services....126
3.14.1 Refund Transactions....126
United States Region....127
3.3 Obtaining an Authorization....127
3.3.1 Mastercard POS Transaction Authorization Procedures....127

3.5 Maestro Cardholder Verification Requirements....127
Additional U.S. Region and U.S. Territory Rules....128
3.14 Returned Products and Canceled Services....128
3.14.1 Refund Transactions....128

Chapter 4: Card-Present Transactions....129
4.1 Chip Transactions at Hybrid Terminals....133
4.2 Offline Transactions Performed on Board Planes, Trains, and Ships....133
4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions—Europe Region Only....134
4.4 Contactless Transactions at POS Terminals....135
4.5 Contactless Transit Transactions....135
4.5.1 Mastercard Contactless Transit Aggregated Transactions....135
4.5.2 Maestro Contactless Transit Aggregated Transactions....136
4.6 Contactless Transactions at ATM Terminals....137
4.7 Contactless-only Acceptance....137
4.8 Mastercard Consumer-Presented QR Transactions at POS Terminals....138
4.9 Purchase with Cash Back Transactions....139
4.10 Transactions at Unattended POS Terminals....140
4.10.1 Automated Fuel Dispenser Transactions....141
4.10.2 Electric Vehicle Charging Transactions....142
4.11 PIN-based Debit Transactions—United States Region Only....143
4.12 PIN-less Single Message Transactions—United States Region Only....143
4.13 Merchant-approved Maestro POS Transactions....143
4.14 Mastercard Manual Cash Disbursement Transactions....144
4.14.1 Non-discrimination Regarding Cash Disbursement Services....145
4.14.2 Maximum Cash Disbursement Amounts....145
4.14.3 Discount or Service Charges....145
4.14.4 Mastercard Acceptance Mark Must Be Displayed....145
4.15 Encashment of Mastercard Travelers Cheques....146
4.16 ATM Transactions....146
4.16.1 "Chained" Transactions....146
4.16.2 ATM Transaction Branding....146
4.17 ATM Access Fees....146
4.17.1 ATM Access Fees - Domestic Transactions....147
4.17.2 ATM Access Fees - Cross-border Transactions....147
4.17.3 ATM Access Fee Requirements....147
Transaction Field Specifications for ATM Access Fees....147
Non-discrimination Regarding ATM Access Fees....147
Notification of ATM Access Fee....147
Cancellation of Transaction....147
Sponsor Approval of Proposed Signage, Screen Display, and Receipt....148

ATM Terminal Signage....148
ATM Terminal Screen Display....148
ATM Transaction Receipts....149
4.18 Merchandise Transactions at ATM Terminals....149
4.18.1 Approved Merchandise Categories....149
4.18.2 Screen Display Requirement for Merchandise Categories....150
4.19 Shared Deposits—United States Region Only....150
Variations and Additions by Region....151
Asia/Pacific Region....151
4.1 Chip Transactions at Hybrid Terminals....151
4.5 Contactless Transit Transactions....151
4.5.1 Mastercard Contactless Transit Aggregated Transactions....151
4.9 Purchase with Cash Back Transactions....151
4.10 Transactions at Unattended POS Terminals....152
4.10.1 Automated Fuel Dispenser Transactions....152
4.17 ATM Access Fees....152
4.17.1 ATM Access Fees—Domestic Transactions....152
Canada Region....153
4.9 Purchase with Cash Back Transactions....153
4.10 Transactions at Unattended POS Terminals....153
4.10.1 Automated Fuel Dispenser Transactions....153
4.17 ATM Access Fees....153
4.17.1 ATM Access Fees—Domestic Transactions....153
Europe Region....154
4.1 Chip Transactions at Hybrid Terminals....154
4.2 Offline Transactions Performed on Board Planes, Trains, and Ships....154
4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions....154
4.4 Contactless Transactions at POS Terminals....155
4.5 Contactless Transit Aggregated Transactions....156
4.5.1 Mastercard Contactless Transit Aggregated Transactions....156
4.5.2 Maestro Contactless Transit Aggregated Transactions....156
4.9 Purchase with Cash Back Transactions....157
4.10 Transactions at Unattended POS Terminals....161
4.10.1 Automated Fuel Dispenser Transactions....162
4.13 Merchant-approved Maestro POS Transactions....162
4.14 Mastercard Manual Cash Disbursement Transactions....162
4.14.2 Maximum Cash Disbursement Amounts....163
4.17 ATM Access Fees....163
4.17.1 ATM Access Fees - Domestic Transactions....163
4.18 Merchandise Transactions at ATM Terminals....163
4.18.1 Approved Merchandise Categories....163
Latin America and the Caribbean Region....164
4.4 Contactless Transactions at POS Terminals....164

4.5 Contactless Transit Aggregated Transactions....164
4.5.2 Maestro Contactless Transit Aggregated Transactions....164
4.9 Purchase with Cash Back Transactions....164
4.17 ATM Access Fees....166
4.17.1 ATM Access Fees—Domestic Transactions....166
Middle East/Africa Region....167
4.9 Purchase with Cash Back Transactions....167
United States Region....167
4.1 Chip Transactions at Hybrid Terminals....168
4.5 Contactless Transit Transactions....168
4.5.1 Mastercard Contactless Transit Aggregated Transactions....168
4.5.2 Maestro Contactless Transit Aggregated Transactions....169
4.9 Purchase with Cash Back Transactions....169
4.10 Transactions at Unattended POS Terminals....170
4.10.1 Automated Fuel Dispenser Transactions....170
4.11 PIN-based Debit Transactions....170
4.12 PIN-less Single Message Transactions....170
4.14 Mastercard Manual Cash Disbursement Transactions....171
4.14.2 Maximum Cash Disbursement Amounts....171
4.14.3 Discount or Service Charges....172
4.17 ATM Access Fees....172
4.17.1 ATM Access Fees—Domestic Transactions....172
4.18 Merchandise Transactions at ATM Terminals....172
4.18.1 Approved Merchandise Categories....172
4.19 Shared Deposits....172
4.19.1 Non-discrimination Regarding Shared Deposits....173
4.19.2 Terminal Signs and Notices....173
4.19.3 Maximum Shared Deposit Amount....173
4.19.4 Deposit Verification....173
4.19.5 ATM Terminal Clearing and Deposit Processing....174
4.19.6 Shared Deposits in Excess of USD 10,000....174
4.19.7 Notice of Return....174
4.19.8 Liability for Shared Deposits....175

Chapter 5: Card-Not-Present Transactions....176
5.1 Electronic Commerce Transactions....179
5.1.1 Acquirer and Merchant Requirements....179
5.1.2 Issuer Requirements....181
5.1.3 Use of Static AAV for Card-not-present Transactions....182
5.1.4 Debit Small-Ticket Digital Transaction Program: Brazil Only....182
5.2 Mail Order and Telephone Order (MO/TO) Transactions....182
5.3 Credential-on-File Transactions....183

5.4 Recurring Payment Transactions....184
5.4.1 Subscription Billing Merchants....186
5.4.1.1 Applicability of Standards....188
5.4.2 Negative Option Billing Merchants....188
5.4.3 China Domestic Recurring Payment Transactions....190
5.5 Installment Billing....190
5.5.1 Single-Authorization Installment Billing....191
5.5.1.1 Definitions....191
5.5.1.2 Transaction Processing Procedures....191
5.5.2 Multiple-Authorization Installment Billing....192
5.6 Transit Transactions Performed for Debt Recovery....194
5.6.1 Transit First Ride Risk Framework....195
5.7 Use of Automatic Billing Updater....198
5.8 Authentication Requirements—Europe Region Only....199
5.9 Merchant-initiated Transactions....199
5.10 Mastercard Micropayment Solution—United States Region Only....200
Variations and Additions by Region....200
Asia/Pacific Region....200
5.1 Electronic Commerce Transactions....200
5.1.1 Acquirer and Merchant Requirements....201
5.1.2 Issuer Requirements....201
5.2 Mail Order and Telephone Order (MO/TO) Transactions....202
5.3 Credential-on-File Transactions....203
5.4 Credential-on-File Transactions....203
5.4.2 China Domestic Recurring Payment Transactions....203
5.4.2.1 Transaction Requirements for Acquirers....204
5.4.2.2 Transaction Requirement for Issuers....206
5.5 Installment Billing....206
5.5.1 Single-Authorization Installment Billing....206
5.5.1.2 Transaction Processing Procedures....206
5.6 Transit Transactions Performed for Debt Recovery....206
5.6.1 Transit First Ride Risk Framework....207
5.7 Use of Automatic Billing Updater....208
5.9 Merchant-initiated Transactions....208
Canada Region....208
5.7 Use of Automatic Billing Updater....208
Europe Region....208
5.1 Electronic Commerce Transactions....208
5.1.1 Acquirer and Merchant Requirements....208
5.1.2 Issuer Requirements....210
5.1.3 Use of Static AAV for Card-not-present Transactions....211
5.2 Mail Order and Telephone Order (MO/TO) Maestro Transactions....211
5.2.1 Definitions....211

5.2.2 Intracountry Maestro MO/TO Transactions—Cardholder Authority....212
5.2.3 Intracountry Maestro MO/TO Transactions—Transactions Per Cardholder Authority....212
5.2.4 Intracountry Maestro MO/TO Transactions—CVC 2/AVS Checks....212
5.3 Credential-on-File Transactions....213
5.4 Recurring Payment Transactions....213
5.5 Installment Billing....215
5.5.1 Single-Authorization Installment Billing....215
5.5.1.2 Transaction Processing Procedures....215
5.5.2 Multiple-Authorization Installment Billing....215
5.6 Transit Transactions Performed for Debt Recovery....215
5.7 Use of Automatic Billing Updater....216
5.7.1 Issuer Requirements....216
5.7.2 Acquirer Requirements....217
5.8 Authentication Requirements....218
5.8.1 Acquirer Requirements....218
5.8.2 Issuer Requirements....219
5.9 Merchant-initiated Transactions....219
Latin America and the Caribbean Region....221
5.1 Electronic Commerce Transactions....221
5.1.1 Acquirer and Merchant Requirements....221
5.1.2 Issuer Requirements....221
5.1.4 Debit Small-Ticket Digital Transaction Program: Brazil Only....221
5.7 Use of Automatic Billing Updater....223
Middle East/Africa Region....223
5.1 Electronic Commerce Transactions....223
5.1.1 Acquirer and Merchant Requirements....223
5.1.2 Issuer Requirements....224
5.7 Use of Automatic Billing Updater....224
United States Region....224
5.7 Use of Automatic Billing Updater....224
5.10 Mastercard Micropayment Solution....224
Additional U.S. Region and U.S. Territory Rules....225
5.1 Electronic Commerce Transactions....225
5.1.1 Acquirer and Merchant Requirements....225
5.1.2 Issuer Requirements....226

Chapter 6: Payment Transactions and Funding Transactions....227
6.1 Payment Transactions....228
6.1.1 Payment Transactions - Acquirer and Merchant Requirements....228
6.1.2 Payment Transactions—Issuer Requirements....229
6.2 Gaming Payment Transactions....230

6.3 MoneySend Payment Transactions....230
6.4 China Deposit Transactions – China Only....231
6.5 China Funds Transfer Transactions – China Only....231
6.6 Funding Transactions....231
Variations and Additions by Region....231
Asia/Pacific Region....232
6.4 China Deposit Transactions – China Only....232
6.4.1 Non-discrimination Regarding Maximum Transaction Amount Limit....232
6.4.2 ATM Access Fee....232
6.4.3 Account Verification....232
6.4.4 Failed Transaction....232
6.5 China Funds Transfer Transactions – China Only....232
6.5.1 China Funds Transfer Transaction Terms....233
6.5.2 Non-discrimination Regarding Maximum Amount Limit....233
6.5.3 ATM Access Fee....233
6.5.4 Account Verification....234
6.5.5 Funds Availability....234
Europe Region....234
6.1 Payment Transactions....234
6.1.1 Payment Transactions—Acquirer and Merchant Requirements....234
6.1.2 Payment Transactions—Issuer Requirements....235

Chapter 7: Terminal Requirements....236
7.1 Terminal Eligibility....238
7.2 Terminal Requirements....238
7.2.1 Terminal Function Keys for PIN Entry....239
7.2.2 Terminal Responses....240
7.2.3 Terminal Transaction Log....240
7.2.4 Contactless-enabled Terminals and Contactless Reader Requirements....240
7.3 POS Terminal Requirements....241
7.3.1 Contactless-enabled POS Terminals....241
7.3.2 Contactless-only POS Terminals....242
7.4 Mobile POS (MPOS) Terminal Requirements....243
7.5 ATM Terminal and Bank Branch Terminal Requirements....244
7.5.1 ATM Terminals....245
7.5.2 Bank Branch Terminals....245
7.5.3 Contactless-enabled ATM and Bank Branch Terminals....246
7.6 Hybrid Terminal Requirements....246
7.6.1 Hybrid POS Terminal Requirements....247
Hybrid POS Terminal and Chip-only MPOS Terminal Displays....248
7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements....248
7.7 Mastercard Consumer-Presented QR Functionality....249

Variations and Additions by Region....250
Asia/Pacific Region....250
7.2 Terminal Requirements....250
7.3 POS Terminal Requirements....250
7.3.1 Contactless-enabled POS Terminals....251
7.4 Mobile POS (MPOS) Terminal Requirements....251
7.5 ATM Terminal and Bank Branch Terminal Requirements....252
7.6 Hybrid Terminal Requirements....252
7.6.1 Hybrid POS Terminal Requirements....252
Canada Region....253
7.3 POS Terminal Requirements....253
7.3.1 Contactless-enabled POS Terminals....253
7.4 Mobile POS (MPOS) Terminal Requirements....253
7.5 ATM Terminal and Bank Branch Terminal Requirements....253
7.5.3 Contactless-enabled ATM and Bank Branch Terminals....253
Europe Region....254
7.1 Terminal Eligibility....254
7.2 Terminal Requirements....254
7.2.4 Contactless-enabled Terminals and Contactless Reader Requirements....254
7.3 POS Terminal Requirements....254
7.3.1 Contactless-enabled POS Terminals....255
7.4 Mobile POS (MPOS) Terminal Requirements....256
7.5 ATM Terminal and Bank Branch Terminal Requirements....257
7.5.2 Bank Branch Terminals....257
7.5.3 Contactless-enabled ATM and Bank Branch Terminals....257
7.6 Hybrid Terminal Requirements....258
7.6.1 Hybrid POS Terminal Requirements....258
7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements....258
Latin America and the Caribbean Region....259
7.3 POS Terminal Requirements....259
7.3.1 Contactless-enabled POS Terminals....260
7.6 Hybrid Terminal Requirements....261
Middle East/Africa Region....261
7.3 POS Terminal Requirements....261
7.3.1 Contactless-enabled POS Terminals....261
7.6 Hybrid Terminal Requirements....261
7.6.1 Hybrid POS Terminal Requirements....261
United States Region....261
7.3 POS Terminal Requirements....262
7.3.1 Contactless-enabled POS Terminals....262
7.4 Mobile POS (MPOS) Terminal Requirements....262
7.5 ATM Terminal and Bank Branch Terminal Requirements....262
7.6 Hybrid Terminal Requirements....263

Additional U.S. Region and U.S. Territory Rules 263
7.6 Hybrid Terminal Requirements 263
7.6.1 Hybrid POS Terminal Requirements 263
Hybrid POS Terminal and Chip-only MPOS Terminal Displays 263

Appendix A: Geographic Regions 265
Asia/Pacific Region 266
Canada Region 267
Europe Region 267
Single European Payments Area (SEPA) 268
Non-Single European Payments Area (Non-SEPA) 268
Latin America and the Caribbean Region 269
Middle East/Africa Region 270
United States Region 271

Appendix B: Compliance Zones 272
Compliance Zones 273

Appendix C: Transaction Identification Requirements 277
Transaction Date 278
Account Status Inquiry (ASI) Requests 278
Contactless Transactions 279
Contactless Transit Aggregated Transactions 281
Contactless-only Transactions 283
Electronic Commerce Transactions 285
Digital Secure Remote Payment Transactions 287
Digital Secure Remote Payment Transactions Containing Chip Data 287
Digital Secure Remote Payment Transactions Containing Digital Payment Data 289
Merchant-initiated Transactions following Digital Secure Remote Payment Transactions 291
Mastercard Biometric Card Program Transactions 292
Transaction Type Identifier (TTI) 293
Merchant Country of Origin 293
China Deposit Transactions 293
China Funds Transfer Transactions 294
Cardholder-initiated Transactions (CITs) 296
Merchant-initiated Transactions (MITs) 297

Appendix D: Cardholder-Activated Terminal (CAT) Transactions 301
CAT Transactions 302

CAT Level Requirements....302
Dual Capability for CAT 1 and CAT 2....303
CAT Level 1: Automated Dispensing Machines (CAT 1)....303
CAT Level 2: Self-Service Terminal (CAT 2)....304
CAT Level 3: Limited Amount Terminals (CAT 3)....305
CAT Level 4: In-Flight Commerce (IFC) Terminals (CAT 4)....306
CAT Level 6: Electronic Commerce Transactions (CAT 6)....309
CAT Level 7: Transponder Transactions (CAT 7)....309
CAT Level 9: Mobile POS (MPOS) Acceptance Device Transactions (CAT 9)....310

Appendix E: CVM and Transit Limits....311
Overview....312
CVM and Transit Limits....312

Appendix F: Digital Goods and Lodging Merchant Services....313
Digital Goods Purchases....314
Guaranteed Reservations....315
Advance Resort Deposit....316

Appendix G: Signage, Screen, and Receipt Text Display....317
Screen and Receipt Text Standards....319
Models for ATM Access Fee Notification at ATM Terminals....320
Models for Standard Signage Notification of an ATM Access Fee....320
Asia/Pacific Region....320
Australia....321
Canada Region....321
Europe Region....322
United Kingdom....323
Latin America and the Caribbean Region....323
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela....324
Middle East/Africa Region....325
United States Region....326
Models for Generic Terminal Signage Notification of an ATM Access Fee....327
Asia/Pacific Region....327
Australia....327
Canada Region....328
Europe Region....329
United Kingdom....329
Latin America and the Caribbean Region....330

Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela....331
Middle East/Africa Region....332
United States Region....332
Models for Screen Display Notification of an ATM Access Fee....333
Asia/Pacific Region....333
Australia....334
Canada Region....335
Europe Region....335
United Kingdom....336
Latin America and the Caribbean Region....337
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela....337
Middle East/Africa Region....338
United States Region....339
Model for an ATM Access Fee Transaction Receipt....340
Model Screen Offering POI Currency Conversion....340
Model Receipt for Withdrawal Completed with POI Currency Conversion....341
Model Screen Displays for Offering Installment Payments....342
Model Receipt Texts for Installments....352

Appendix H: Definitions....354

Notices....398

Transaction Processing Rules overview

This document is part of a set of Standards that enable growth for Mastercard and for its Customers while ensuring integrity and reliability. This document contains the Rules that pertain to the processing of Transactions and Payment Transactions. A Payment Transaction means a Payment Transfer Activity (PTA) Transaction that transfers funds to an Account, not a credit that reverses a previous purchase.

Audience

This document is intended for Mastercard Customers and potential Customers who participate or have applied to participate in Activities and Digital Activity as Principals, Affiliates, or Associations.

Table 1: Details

Metadata	Value
Audience	• Acquirer Resellers • Acquirers • Branded Processors • Issuers • Merchants • Network Enablement Partners • Non-acquirer Resellers • Processors • Resellers • Vendors (Global Vendor Certification Program participants)
Region	Global
Type	Legal and compliance standards
Publication date	10 June 2025

Table 2: Summary of changes

Description of change	Where to look
Created the overview to align with current guide standards.	Transaction Processing Rules overview
Removed obsolete effective dates.	Throughout
Chapter 2 Authorization and Clearing Requirements	

Description of change	Where to look
CAN/US 10811.1 Revised Standards for Authorization Processing in the U.S. and Canada Regions LAC 11081 Revised Standards for Authorization Processing in the Latin America and the Caribbean Region	2.6 Undefined Authorizations 2.8 Message Reason Code 4808 Chargeback Protection Period Latin America and the Caribbean Region 2.6 Undefined Authorizations
Added text from the *Customer Interface Specification* manual stating that reversals must contain data referencing the original authorization request.	2.11 Full and Partial Reversals
GLB 8390.1 Revised Standards for Use of the Transaction Link Identifier CAN/US 10831.1 Revised Standards for Online Authorization of Refund Transactions in the Canada and United States Regions	2.13.1 Refund Transactions - Acquirer Requirements Canada Region United States Region 2.13.1 Refund Transactions - Acquirer Requirements (removed)
GLB 11051 Revised Standards Regarding Mastercom Access	2.18.2 Compliance with Dispute Procedures
Minor editorial changes were made.	Canada Region 2.2 Issuer Authorization Requirements
Made minor editorial changes. Removed text describing obsolete process: "The Acquirer of a U.S. Region Merchant participating in the substantiation of certain tax-qualified purchases (for example, medical-related, prescription drug, and vision care purchases) must be prepared to respond to an Issuer's request for the retrieval of documentation for a Transaction effected with an eligible U.S. Region-issued Card. The Acquirer must provide the requested documentation within 30 calendar days of the Central Site Business Date of the Issuer's request."	United States Region 2.2 Issuer Authorization Requirements 2.18 Transaction Clearing, Queries, and Disputes (removed)
Updated to include chip transactions; added text from Mastercard Network Processing - Dual Message System Guide: "Acquirers and prepaid Card Issuers must support POS balance inquiries for prepaid Debit Mastercard and prepaid Maestro Account ranges."	United States Region 2.14 Balance Inquiries
Chapter 3 Acceptance Procedures	

Description of change	Where to look
CAN/US 10831.1 Revised Standards for Online Authorization of Refund Transactions in the Canada and United States Regions	3.3.1 Mastercard POS Transaction Authorization Procedures Canada Region 3.3.1 Mastercard POS Transaction Authorization Procedures (removed) United States Region 3.3.1 Mastercard POS Transaction Authorization Procedures (removed)
CAN/US 10811.1 Revised Standards for Authorization Processing in the U.S. and Canada Regions; also reorganized content for clarity.	3.3.1 Mastercard POS Transaction Authorization Procedures Authorization When the Cardholder Adds a Gratuity United States Region 3.3.1 Mastercard POS Transaction Authorization Procedures "Authorization When the Cardholder Adds a Gratuity"
Due to product decommissioning, references to Cardless ATM transactions have been removed.	3.6 Use of a PIN for Transactions at ATM Terminals and Bank Branch Terminals
Removed redundant text; clarified that Payment Transactions must be presented within 24 hours of the time of authorization approval.	3.15.1 Transaction Presentment Time Frames
EUR 10726.1 Revised Standards for Refund Transactions in Select Countries in the Europe Region	Europe Region 3.14 Returned Products and Canceled Services
Chapter 4 Card-Present Transactions	
In "Authorization Before Fueling," clarified item 2 to state that the final transaction amount must not exceed the partial approval amount provided by the issuer; this includes when the issuer responds to a USD 1 request with a partial approval amount exceeding USD 1. Added authorization hold guidance for issuers. Removed outdated references to technical manuals.	4.10.1 Automated Fuel Dispenser Transactions
Chapter 5 Card-Not-Present Transactions	
GLB 8390.1 Revised Standards for Use of the Transaction Link Identifier	5.4 Recurring Payment Transactions 5.5.2 Multiple-Authorization Installment Billing
Updated reason code 4850-Installment Billing Disputes to 4850 (Participating Countries-Installment Billing Dispute)	5.5 Installment Billing

Description of change	Where to look
Changed "Message Reason Code 4850—Installment Billing Dispute" to "Installment Billing Dispute-Participating Countries (Reason Code 4850)"	5.5.1.1 Definitions
AP 10161.1 Revised Standards for Transit First Ride Risk in Australia	5.6 Transit Transactions Performed for Debt Recovery Asia/Pacific Region 5.6.1 Transit First Ride Risk Framework
Chapter 6 Payment Transactions and Funding Transactions	
Added Payment Transaction identification information; clarified that the clearing message must be submitted within 24 hours of the time of authorization approval.	6.1 Payment Transactions 6.1.1 Payment Transactions - Acquirer and Merchant Requirements
Removed and replaced Europe, Middle East/Africa, and U.S. regional variations with a reference to the *Mastercard Gaming and Gambling Payments Program Standards*, which contains applicable global and regional requirements.	6.2 Gaming Payment Transactions
Moved reference to using the switch of the customer's choice to Europe Region section 6.1, for all Payment Transaction types.	6.3 MoneySend Payment Transactions 6.1 Payment Transactions 6.3 MoneySend Payment Transactions (removed)
Appendix C Transaction Identification Requirements	
Added information relating to the Name Validation Service, including a service description and terms to which the Originating Institution must agree when using the service.	Account Status Inquiry (ASI) Requests
Removed Payment Transaction identification information.	Payment Transactions (removed)
Appendix E CVM and Transit Limits	
AP 10161.1 Revised Standards for Transit First Ride Risk in Australia AP 10335.1 Revised Standards for First Ride Risk Limit for Domestic Transit Transactions in New Zealand GLB 10656 Revised Standards for CVM Limits in Maldives GLB 10787 Revised Standards for Contactless Transit Aggregated Limits in Argentina	CVM and Transit Limits

Applicability of Rules in this Manual

This manual contains Rules for Activities.

The Rules[1] 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, Gaming Payment Transactions, and China Funds Transfer 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...	**Apply to...**
Mastercard POS Transactions	A POS Transaction conducted with a Mastercard Card. A China domestic POS Transaction conducted with a Mastercard Card (includes a "Debit Mastercard" Card).
Maestro POS Transactions	A POS Transaction conducted with: • A Maestro Card, or • A Mastercard Card issued from a country or territory other than China using a BIN identified by the Corporation as "Debit Mastercard" and routed to the Mastercard® Single Message System[2].
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: • A Customer financial institution teller or Bank Branch Terminal with a Mastercard Card, or • A Bank Branch Terminal with a Maestro or Cirrus Card and routed to the Interchange System.

[1] 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.

[2] In Mainland China, the Standards relating to POS Transactions apply to all domestic Transactions.

Rules relating to...	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, Gaming Payment Transactions, and China Funds Transfer 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.

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 26
1.2 Authorization Routing - Mastercard POS Transactions 26
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions 27
1.3.1 Routing Instructions and System Maintenance 27
1.3.2 Chip Transaction Routing 27
1.3.3 Domestic Transaction Routing 28
1.4 ATM Terminal Connection to the Interchange System 28
1.5 Gateway Processing 28
1.6 POS Terminal Connection to the Interchange System 29
Variations and Additions by Region 29
Asia/Pacific Region 29
1.4 ATM Terminal Connection to the Interchange System 29
1.6 POS Terminal Connection to the Interchange System 29
Canada Region 30
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions 30
1.3.3 Domestic Transaction Routing 30
1.4 ATM Terminal Connection to the Interchange System 30
Europe Region 30
1.1 Connecting to the Interchange System 30
1.2 Authorization Routing—Mastercard POS Transactions 31
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions 31
1.3.2 Chip Transaction Routing 31
1.3.3 Domestic Transaction Routing 31
1.4 ATM Terminal Connection to the Interchange System—SEPA Only 31
Latin America and the Caribbean Region 32
1.4 ATM Terminal Connection to the Interchange System 32
1.6 POS Terminal Connection to the Interchange System 32
United States Region 32
1.1 Connecting to the Interchange System 32
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions 32
1.3.1 Routing Instructions and System Maintenance 32

1.3.3 Domestic Transaction Routing..... 33
1.4 ATM Terminal Connection to the Interchange System.....33
Additional U.S. Region and U.S. Territory Rules.....33
1.3 Authorization Routing—Maestro, Cirrus, and ATM Transactions..... 34

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 22210000 to 27209999 BIN range or 51000000 to 55999999 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 Domestic 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, UK and Gibraltar the Rule on this subject is modified as follows.

For the processing of Transactions in the EEA, UK and Gibraltar, and if required by applicable law or regulation, Payment Transactions in the EEA, UK and Gibraltar, 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, UK and Gibraltar, 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, UK and Gibraltar the Rule on this subject is modified as follows.

Intra-EEA Transactions, Cross-border Transactions between the UK, Gibraltar and an EEA country, and Intracountry Transactions in the EEA, UK and Gibraltar may be processed using the registered switch of the Customer's choice.

1.3.3 Domestic Transaction Routing

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

Intra-EEA Transactions, Cross-border Transactions between the UK, Gibraltar and an EEA country, and Intracountry Transactions in the EEA, UK and Gibraltar 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.

Maintenance Requirements	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
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 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), MS POS (position 55), and Maestro Card-Not-Present (position 74) 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 39
2.1.1 Acquirer Host System Requirements 40
2.2 Issuer Authorization Requirements 40
2.2.1 Issuer Host System Requirements 42
2.2.2 Stand-In Processing Service 43
Accumulative Transaction Limits 43
Chip Cryptogram Validation in Stand-In 44
2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers 44
2.3 Authorization Responses 44
2.4 Performance Standards 45
2.4.1 Performance Standards—Acquirer Requirements 45
2.4.2 Performance Standards—Issuer Requirements 45
Issuer Failure Rate (Substandard Level 1) 45
Issuer Failure Rate (Substandard Level 2) 46
Calculation of the Issuer Failure Rate 46
2.5 Preauthorizations 46
2.5.1 Preauthorizations - Mastercard POS Transactions 46
2.5.2 Preauthorizations - Maestro POS Transactions 47
2.5.3 Preauthorizations - ATM and Manual Cash Disbursement Transactions 47
2.6 Undefined Authorizations 47
2.7 Final Authorizations 48
2.8 Message Reason Code 4808 Chargeback Protection Period 49
2.9 Multiple Authorizations 49
2.10 Clearing, Completion, and Chargeback Message Requirements 50
2.10.1 Multiple Clearing or Completion Messages 50
2.10.1.1 Mastercard and Debit Mastercard Transactions 51
2.10.2 Maestro Transactions 52
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 54
2.11.3 Reversal for Conversion of Approval to Decline 54
2.11.4 Reversal to Cancel Transaction 55

2.12 Full and Partial Approvals 55
2.13 Refund Transactions and Corrections 58
2.13.1 Refund Transactions - Acquirer Requirements 58
2.13.2 Refund Transactions - Issuer Requirements 59
2.14 Balance Inquiries 60
2.15 CVC 2 Verification for POS Transactions 61
2.16 CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless Transactions—Brazil Only 61
2.17 Euro Conversion—Europe Region Only 61
2.18 Transaction Clearing, Queries, and Disputes 61
2.18.1 Clearing Requirements 61
2.18.2 Compliance with Dispute Procedures 62
2.19 Chargebacks for Reissued Cards 62
2.20 Correction of Errors 62
2.21 Merchant Payment Gateway Identifier (MPG ID) 62
2.22 Co-badged Cards - Acceptance Brand Identifier 63
Variations and Additions by Region 63
Asia/Pacific Region 63
2.1 Acquirer Authorization Requirements 63
2.1.1 Acquirer Host System Requirements 64
2.2 Issuer Authorization Requirements 64
2.2.1 Issuer Host System Requirements 64
2.3 Authorization Responses 65
2.5 Preauthorizations 65
2.5.1 Preauthorizations - Mastercard POS Transactions 65
2.5.2 Preauthorizations—Maestro POS Transactions 65
2.7 Final Authorization 65
2.8 Message Reason Code 4808 Chargeback Protection Period 66
2.11 Full and Partial Reversals 66
2.11.1 Full and Partial Reversals—Acquirer Requirements 66
2.12 Full and Partial Approvals 66
2.13 Refund Transactions and Corrections 67
2.13.1 Refund Transactions - Acquirer Requirements 67
Canada Region 68
2.1 Acquirer Authorization Requirements 68
2.1.1 Acquirer Host System Requirements 68
2.2 Issuer Authorization Requirements 68
2.12 Full and Partial Approvals 69
Europe Region 69
2.1 Acquirer Authorization Requirements 69

2.2 Issuer Authorization Requirements 71
2.2.2 Stand-In Processing Service 72
2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers 72
2.3 Authorization Responses 72
2.4 Performance Standards 73
2.4.2 Performance Standards—Issuer Requirements 73
2.5 Preauthorizations 73
2.5.2 Preauthorizations—Maestro POS Transactions 73
2.5.3 Preauthorizations—ATM and Manual Cash Disbursement Transactions 74
2.7 Final Authorizations 75
2.8 Message Reason Code 4808 Chargeback Protection Period 75
2.9 Multiple Authorizations 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 77
2.12 Full and Partial Approvals 77
2.13 Refund Transactions and Corrections 78
2.13.1 Refund Transactions—Acquirer Requirements 78
2.13.2 Refund Transactions—Issuer Requirements 78
2.14 Balance Inquiries 78
2.15 CVC 2 Verification for POS Transactions 78
2.17 Euro Conversion 79
2.22 Co-badged Cards - Acceptance Brand Identifier 79
Latin America and the Caribbean Region 80
2.2 Issuer Authorization Requirements 80
2.2.1 Issuer Host System Requirements 80
2.5 Preauthorizations 80
2.5.2 Preauthorizations - Maestro POS Transactions 80
2.6 Undefined Authorizations 80
2.9 Multiple Authorizations 81
2.10 Multiple Clearing or Multiple Completion Messages 82
2.10.2 Maestro Transactions 82
2.16 CVC 3 Verification for Maestro Magnetic Stripe Mode Contactless—Brazil Only 84
Middle East/Africa Region 84
2.1 Acquirer Authorization Requirements 84
2.7 Final Authorizations 85
2.12 Full and Partial Approvals 86
2.21 Merchant Payment Gateway Identifier (MPG ID) 86
United States Region 86

2.1 Acquirer Authorization Requirements....86
2.1.1 Acquirer Host System Requirements....86
2.2 Issuer Authorization Requirements....86
2.2.1 Issuer Host System Requirements....87
2.2.2 Stand-In Processing Service....87
2.4 Performance Standards....89
2.4.2 Performance Standards—Issuer Requirements....89
2.5 Preauthorizations....89
2.5.2 Preauthorizations—Maestro POS Transactions....89
2.11 Full and Partial Reversals....89
2.11.1 Full and Partial Reversals—Acquirer Requirements....89
2.11.2 Full and Partial Reversals—Issuer Requirements....90
2.14 Balance Inquiries....90
Additional U.S. Region and U.S. Territory Rules....90
2.2 Issuer Authorization Requirements....90
2.2.2 Stand-In Processing Service....90
2.5 Preauthorizations....90
2.5.2 Preauthorizations—Maestro POS Transactions....91
2.9 Multiple Authorizations....91
2.10 Multiple Clearing and Multiple Completion Messages....92
2.10.2 Maestro Transactions....93
2.18 Transaction Clearing, Queries, and Disputes....94

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.

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").

Effective 12 April 2024, an Acquirer must support the online authorization of Mastercard®, Debit Mastercard®, and Maestro refund Transactions acquired on the Dual Message System and enable refund Transaction authorization service for a Merchant upon request. The Acquirer must pass the Issuer's refund Transaction authorization response to the Merchant.

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)
- Account Status Inquiry (ASI) requests
- 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

Government Controlled Merchants

Each Authorization Request/0100 and Authorization Advice/0120 message for a Transaction conducted by a Government Controlled Merchant must include the Merchant Country of Origin for that Government Controlled Merchant as defined in Appendix C, whether such country is the same as or different from the country in which the Merchant is located or the Transaction occurs.

Offline Chip Processing

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.

Account Status Inquiry (ASI) Requests

An ASI request is an Authorization Request/0100 or Financial Transaction Request/0200 message initiated by an Acquirer or Merchant to obtain the Issuer's validation that a Cardholder's Account is open and active.

An ASI request is identified with a value of 8 (Account Status Inquiry Service [ASI]) in DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), and when submitted in connection with a purchase, contains a value of 00 (Purchase) in DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code). A Purchase ASI request must have a Transaction amount of zero.

Unless specifically permitted in the Standards, a purchase Transaction authorization request must not contain a Transaction amount value of one major unit of currency or any other nominal test amount that does not represent an actual purchase.

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

Echoing of Transaction Link ID

Effective 17 October 2025, an Acquirer must populate DE 105 (Multi-Use Transaction Identification Data), subelement 001 (Transaction Link Identifier [TLID]) of each incremental Authorization/0100, Authorization Advice/0120, Financial Transaction Request/0200, Financial Transaction Advice/0220, Reversal Request/0400, and Acquirer Reversal Advice/0420 message with the value in the TLID field received in the corresponding Authorization Request Response/0110, Financial Transaction Request Response/0210, or other original message response for the same Transaction.

2.1.1 Acquirer Host System Requirements

NOTE: Rules on this subject appear in the "Asia/Pacific Region", "Canada Region," and "United States Region" sections 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.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region" (relating to China Domestic Transactions), "Europe Region" (including additional provisions), and "United States Region" sections at the end of this chapter.

Offline Chip Processing

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.

Online Authorization of Refund Transactions

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.

If not supported, 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.

Chip Technical Fallback

An Issuer in the Canada Region, Europe Region, Latin America and the Caribbean Region, or Middle East/Africa Region must decline a Transaction authorization request when technical fallback from chip to magnetic stripe occurs and the Merchant is located in any of these Regions.

For all other Transactions, an Issuer may decline a Transaction authorization request when technical fallback from chip to magnetic stripe occurs.

Account Status Inquiry (ASI) Requests

An ASI request is an Authorization Request/0100 or Financial Transaction Request/0200 message initiated by an Acquirer or Merchant to obtain the Issuer's validation that a Cardholder's Account is open and active. An ASI request is identified with the values of 8 (Account Status Inquiry Service [ASI]) in DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status and 00 (Purchase) in DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) and has a Transaction amount of zero.

An Issuer that receives an ASI request must provide a valid and accurate value in DE 39 (Response Code) of the Authorization Request Response/0110 or Financial Transaction Request Response/0210 message. If a Mastercard or Debit Mastercard Account is open and active, the Issuer must provide a value of 00 (Approved) or 85 (Not Declined) in DE 39.

Mastercard will deem an Issuer to be noncompliant with this requirement if the Issuer declines an ASI request involving a Mastercard or Debit Mastercard Account and within 24 hours of such decline, approves a Transaction authorization request for a non-zero Transaction amount involving the same Merchant or Sponsored Merchant and the same Account. A noncompliant Issuer may be subject to fees under the global ASI Transaction Processing Excellence program.

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

Name Validation Requests

An Issuer may receive a request to validate that sender or receiver name data provided in DE 108 (Additional Transaction Reference Data) of a nonfinancial request matches the Cardholder name registered by the Issuer of the Card or Account. If the Issuer chooses to perform name validation themselves, the Issuer must provide a valid value in the Authorization Request Response/0110 or Financial Transaction Request Response/0210 message of match, no match, or partial match response. If name validation is not performed, the Issuer must provide an unverified response. Refer to the applicable Dual Message System or Single Message System technical manuals for name validation message technical specifications.

NOTE: Modifications to this Rule provision appear in the "Canada 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
- Purchase with cash back Transactions for Debit Mastercard (including prepaid) and Maestro (including prepaid) Account ranges
- Refund Transactions (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," "Latin America and the Caribbean 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
- Dynamic AAV Verification in Stand-In must be used for all Mastercard Accounts and all e-commerce-enabled Maestro Accounts that are enrolled in Mastercard Identity Check, unless the Mastercard Identity Check AAV Verification Service is used.

NOTE: Modifications to this Rule appear in the "Europe Region," "United States Region," and "Additional U.S. Region and U.S. Territory Rules" 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 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: Additions to this Rule appear in the "Asia/Pacific Region" and "Europe Region" sections 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.

NOTE: An addition to this Rule appears in the "Asia/Pacific Region" section at the end of this chapter.

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, and Cardholder verification method (including "No CVM" for Contactless Transactions not exceeding the CVM limit).
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. A preauthorization completion is generated from the original preauthorization response and without use of the Card reader or a CVM.
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 or in Rule 2.10.2 Maestro 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," "Latin America and the Caribbean Region," "United States Region," and "Additional U.S. Region and U.S. Territory Rules" sections 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 for China domestic Transactions or in the Asia/Pacific, Europe, or Middle East/Africa Regions. In the United States Region, this Rule applies until 16 June 2025, in the Latin America and the Caribbean Region, this Rule applies until 18 August 2025; and in the Canada Region, this Rule applies until 16 September 2025. Effective 17 June 2025, this Rule only applies in the Latin America and the Caribbean Region and Canada Region. Effective 19 August 2025, this Rule only applies in the Canada Region. Effective 17 September 2025, this Rule will no longer apply in any 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 greater than zero; **and**
2. The final Transaction amount may differ from the authorized amount; **and**
3. The Transaction is not expected to be canceled 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**.

When 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, except upon Cardholder request or when non-completion is unavoidable for technical reasons such as telecommunications failure or POS Terminal failure.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," and "Middle East/Africa Region" sections 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
Undefined authorization (where permitted)	Seven calendar days from the authorization approval date
Final authorization	Seven calendar days from the authorization approval date for purchase and purchase with cash back Transactions and effective 12 April 2024, five calendar days from the authorization approval date for refund Transactions

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.

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

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

2.9 Multiple Authorizations

NOTE: This Rule does not apply for China Domestic Transactions.

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.

[3] 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.

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:
   a. 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 initial approved Authorization Request Response/0110 message; and
   b. Effective 17 October 2025, DE 105 (Multi-Use Transaction Identification Data), subelement 001 (Transaction Link Identifier [TLID]) of each additional authorization request with the same value populated in this field in the initial approved Authorization Request Response/0110 message.

   These unique identifiers 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.

The use of multiple authorizations for the aggregation of separate Cardholder-initiated purchases into a single Transaction must only occur as set forth in Rule 5.10, "Mastercard Micropayment Solution - United States Region Only."

If the additional 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 total authorized 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 incrementally increases, by the amount of the new preauthorization request, the total authorized Transaction amount. 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.

This option is not available to a Single Message System Acquirer.

NOTE: An addition to this Rule appears in the "Europe Region," "Latin America and the Caribbean Region," and "Additional U.S. Region and U.S. Territory Rules" sections at the end of this chapter.

2.10 Clearing, Completion, and Chargeback Message Requirements

2.10.1 Multiple Clearing or Completion Messages

2.10.1.1 Mastercard and Debit Mastercard Transactions

A Mastercard Dual Message System Acquirer has the option of linking multiple presentments with partial amounts to one approved authorization identified as either a preauthorization or final authorization. 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). This value indicates that the original authorization is closed; no subsequent clearing messages may be submitted.

   If the final first presentment message submitted for a preauthorized Transaction contains a value of 1403 in DE 25, and the total authorized amount has not been fully cleared, then the Acquirer or Merchant must initiate an authorization reversal so that the Issuer may release any excess hold on funds in the Cardholder's Account.
2. Effective 17 October 2025, the Acquirer must populate DE 105 (Multi-Use Transaction Identification Data), subelement 001 (Transaction Link Identifier [TLID]) of each First Presentment/1240 message with the same TLID value received in the original Authorization Request Response/0110 message or other original message response.
3. 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;
   b. DE 63 (Network Data), subfield 2 (Banknet Reference Number) and DE 15 (Date, Settlement) of the Authorization Request/0100 message; and
   c. Effective 17 October 2025, DE 105 (Multi-Use Transaction Identification Data), subelement 001 (Transaction Link Identifier [TLID]) of each lifecycle message for the same Transaction.

   NOTE: A Debit Mastercard Issuer may receive the value of 1403 or 1404 in DE 60 (Advice Reason Code), subfield 2 (Advice Reason Detail Code) of a Mastercard Single Message System-generated Financial Transaction Advice/0220 message.
4. 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 Authorization-related or Late Presentment chargeback. Refer to Rule 2.8 regarding Authorization-related chargeback time frames and Rule 3.15.1 regarding Late Presentment chargeback time frames.

2.10.2 Maestro Transactions

NOTE: Rules on this subject appear in the "Latin America and the Caribbean Region" and "Additional U.S. Region and U.S. Territory Rules" sections at the end of this chapter.

2.11 Full and Partial Reversals

An authorization reversal message is used to reduce the original approved Transaction amount. A full reversal (where DE 95 [Replacement Amounts], when present, contains a value of zero) cancels the original authorization request. A partial reversal has a DE 95 value that is less than the original approved Transaction amount, including in the case of a partial approval. For example, if a USD 100 authorization request is partially approved for USD 75, then the DE 95 value in a subsequent reversal must not exceed USD 75.

A reversal message must contain data referencing the original authorization request in DE 48, subelement 63 (Trace ID) and DE 90 (Original Data Elements). If multiple partial reversals are required before the Transaction is cleared, then each partial reversal must reference the original authorization request (and not any subsequent related request or reversal message).

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 the original Transaction authorization request whenever the Acquirer host system is unable to communicate an authorization response to the POS Terminal.

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. Effective 17 October 2025, the Acquirer must populate DE 105 (Multi-Use Transaction Identification Data), subelement 001 (Transaction Link Identifier [TLID]) of each

Reversal Request/0400 and Acquirer Reversal Advice/0420 message with the same TLID value received in the original Authorization Request Response/0110 or other original message response.

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 "Asia/Pacific Region," "Europe Region," and "United States Region" sections at the end of this chapter.

Refund Transactions

A refund Transaction authorized on the Dual Message System that is not reversed by means of an Authorization Reversal Request/0400 message must be submitted for clearing within five (5) days.

A clearing reversal or Single Message System 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.

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.

To match the reversal to the original approved authorization, the Issuer should use:

- The original authorization trace ID, as populated in DE 48, subelement 63 (Trace ID);
- The original switch serial number, as populated in DE 48, subelement 59, subfield 1 (Original Switch Serial Number); or
- Effective 17 October 2025, the original authorization TLID, as populated in DE 105 (Multi-Use Transaction Identification Data), subelement 001 (Transaction Link Identifier [TLID]).

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 section 5.11.1, "Honor All Cards" 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. A Merchant's support of partial approvals is indicated with a value of 1 in DE 48, subelement 61, subfield 1 (Partial Approval Terminal Support Indicator) of the authorization request (0100 or 0200) message.

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.

A Customer must support partial approval as follows:

1. An Issuer must support partial approval for all prepaid Mastercard, all Debit Mastercard (including prepaid), and all Maestro Account ranges.
2. For each Merchant identified with any of the MCCs listed below, an Acquirer must support partial approval on Mastercard and Maestro branded prepaid and debit Account ranges. This requirement applies to Card-present Transactions occurring at attended Terminals and at Cardholder-activated Terminals (CATs) identified with MCC 5542 (Fuel Dispenser, Automated) or MCC 5552 (Electric Vehicle Charging).

MCC	Description
5310	Discount Stores
5311	Department Stores

MCC	Description
5411	Grocery Stores, Supermarkets
5541	Service Stations (with or without Ancillary Services)
5542	Fuel Dispenser, Automated (if authorization occurs prior to fueling)
5552	Electric Vehicle Charging (if authorization occurs prior to charging)
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

3. For an Acquirer in a Region indicated below, the partial approval support requirement in item 2 includes the following additional MCCs.

MCC	Description	Acquirer Region
4111	Transportation: Suburban and Local Commuter Passenger, including Ferries	U.S.
4812	Telecommunication Equipment including Telephone Sales	Canada, U.S.
4814	Telecommunication Services	Canada, U.S.
4816	Computer Network/Information Services	Canada, U.S.
4899	Cable, Satellite, and Other Pay Television and Radio Services	U.S.
5111	Stationery, Office Supplies	U.S.
5200	Home Supply Warehouse Stores	Canada, U.S.
5300	Wholesale Clubs	U.S.
5331	Variety Stores	Canada, U.S.
5399	Miscellaneous General Merchandise Stores	U.S.
5499	Miscellaneous Food Stores: Convenience Stores, Markets, Specialty Stores	Canada, U.S.
5631	Women's Accessory and Specialty Stores	Canada
5641	Children's And Infant's Wear Stores	Canada
5651	Family Clothing Stores	Canada
5661	Shoe Stores	Canada

MCC	Description	Acquirer Region
5734	Computer Software Stores	Canada, U.S.
5735	Record Shops	Canada, U.S.
5921	Package Stores, Beer, Wine, and Liquor	Canada, U.S.
5941	Sporting Goods Stores	Canada, U.S.
5942	Book Stores	Canada, U.S.
5943	Office, School Supply and Stationery Stores	U.S.
5945	Game, Toy, and Hobby Shops	Canada
5947	Gift, Card, Novelty, and Souvenir Shops	Canada
5977	Cosmetic Stores	Canada
7399	Business Services: not elsewhere classified	Canada
7829	Motion Picture and Video Tape Production and Distribution	U.S.
7832	Motion Picture Theaters	U.S.
7841	Video Entertainment Rental Stores	U.S.
7996	Amusement Parks, Carnivals, Circuses, Fortune Tellers	U.S.
7997	Clubs: Country Clubs, Membership (Athletic, Recreation, Sports), Private Golf Courses	U.S.
7999	Recreation Services: not elsewhere classified	U.S.
8011	Doctors: not elsewhere classified	U.S.
8021	Dentists, Orthodontists	U.S.
8041	Chiropractors	U.S.
8042	Optometrists, Ophthalmologists	U.S.
8043	Opticians, Optical Goods, and Eyeglasses	U.S.
8062	Hospitals	U.S.
8099	Health Practitioners, Medical Services: not elsewhere classified	U.S.
8999	Professional Services: not elsewhere classified	Canada, U.S.
9399	Government Services: not elsewhere classified	Canada, U.S.

NOTE: Modifications to this Rule appear in the "Asia/Pacific," "Canada Region," "Europe Region," and "Middle East/Africa 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. 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 refund Transaction must only be reversed for the purchase Transaction amount or adjusted for an amount less than the purchase Transaction amount to correct a clerical error. The reversal or adjustment must occur within one calendar day of the refund Transaction. The Settlement Date of the Financial Transaction Request/0200 or Central Site Business Date of the First Presentment/1240 message of the refund Transaction is counted as day zero. 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.

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.

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

2.13.1 Refund Transactions - Acquirer Requirements

An Acquirer must support the online authorization of Mastercard, Debit Mastercard, and Maestro refund Transactions acquired on the Dual Message System (with the exception of refunds for Contactless transit aggregated Transactions) and enable refund Transaction authorization service for a Merchant upon request. The Acquirer must forward each refund Transaction authorization request to the Issuer at the time of the Transaction, rather than in a batch, so that the Merchant receives the Issuer's response while the Cardholder is at the POS and before offering the Cardholder a refund Transaction receipt.

The Acquirer must identify a refund Transaction authorization request as a final authorization, as described in Rule 2.7.

The First Presentment/1240 message of a refund Transaction must be submitted for clearing within five calendar days of the refund Transaction date, and if authorized, contain refund Transaction authorization data in DE 63, subfield 2 (Trace ID).

An authorized refund Transaction has a message reason code 4808 chargeback protection period of five calendar days from the refund Transaction authorization approval date.

The Acquirer must perform online authorization for refund Transactions acquired through the Dual Message System as follows.

Effective as of:	Dual message-acquired refund Transactions must be online authorized when conducted by a Merchant, Sponsored Merchant, or other Acceptor located in:
18 October 2024	the Asia/Pacific Region (excluding India Domestic Transactions), Europe Region, Latin America and the Caribbean Region (excluding Brazil), or Middle East/Africa Region
9 January 2025	Brazil
1 October 2025	the Canada Region or United States Region

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; and
- Effective 17 April 2026, DE 105 (Multi-Use Transaction Identification Data), subelement 002 (Economically Related Transaction Link Identifier) of the refund Transaction authorization request message and/or clearing message with the DE 105, subelement 001 (TLID) value from the original purchase Transaction.

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.

2.13.2 Refund Transactions - Issuer Requirements

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, the absence of a PIN, or the absence of chip-related data.

Posting of Funds to the Cardholder's Account

Within one 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.

With respect to dual message online authorization requests for refund Transactions, the Issuer is advised:

- to ensure that the refund Transaction amount is treated and displayed to the Cardholder as a pending credit, until the clearing record has been received and matched to the authorization;
- to 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; and
- not to release the funds to the Cardholder until the clearing record is received.

Pending Refund Transaction Information

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 pending refund information must be displayed in a manner similar to that used for a pending purchase Transaction.

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 "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 Clearing, Queries, and Disputes

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

2.18.1 Clearing Requirements

A Dual Message System Customer must:

- Be capable of sending and receiving Transaction clearing messages through the Global Clearing Management System (GCMS);
- Ensure clearing messages contain accurate, valid and complete Transaction data, in compliance with the Standards;

- Monitor and edit Transaction message data as necessary and correct any errors prior to submission to GCMS for processing at the Central Site;
- Keep a log of each file transmitted to GCMS;
- Verify the incoming acknowledgment messages from GCMS against outgoing file data;
- Correct and resubmit any rejected messages as appropriate; and
- Balance clearing data by comparing each daily net settlement advisement against reconciliation messages, reconciliation reports, or both.

Differences between reconciliation messages and reports and the net settlement advisement may occur from time to time due to network edits for risk management purposes. In the event of such differences, the net settlement advisement is deemed to be the definitive record of the movement of funds.

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 chargeback or compliance case (including any cycle within those processes) must be made in good faith and only after careful review of both the Standards and available information pertinent to the dispute. Chargeback and compliance processing requires access to the Mastercom application on Mastercard Connect.

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 Merchant Payment Gateway Identifier (MPG ID)

An Acquirer must populate the MPG ID field (DE 48, subelement 37 [Additional Merchant Data], subfield 5 [Merchant Payment Gateway ID] with the MPG ID assigned by the Corporation at the time of registration of the MPG as a Service Provider, in authorization and advice messages for all Card-not-present Transactions (excluding MO/TO Transactions) identified with a value of 09, 10, or 81 in DE 22, subfield 1 that are received from the particular MPG. The value **999998** must be populated in the MGP ID field if the MPG is wholly owned by the Acquirer and so not

registered as a Service Provider. The value **999997** must be populated in the MPG ID field if the Merchant uses no gateway and connects directly to the Acquirer. This requirement applies to purchase Transactions, refund Transactions, and Payment Transactions initiated by Merchants (for example, Gaming Payment Transactions).

If multiple MPGs are involved, the Acquirer must provide the MPG ID of the MPG that sends to that Acquirer the Transaction data that the Acquirer uses to generate the authorization or advice message.

Population of the MPG ID in authorization and advice messages for Card-present Transactions is recommended but not required.

An Issuer must technically support the population of the MPG ID field in authorization and advice messages for both Card-not-present and Card-present Transactions. No Issuer response to or handling of the MPG ID is required.

NOTE: A modification to this Rule appears in the "Middle East/Africa Region" section at the end of this chapter.

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

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").

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

An Acquirer must be able to transmit a PIN in Preauthorization Request/0100 and Financial Transaction Request/0200 messages for China Domestic Transactions.

2.1.1 Acquirer Host System Requirements

An Acquirer in the Asia/Pacific Region must ensure that its host systems and those of its Service Providers support online PIN:

- For China Domestic Transactions occurring at POS Terminals, including MPOS Terminals; and
- Effective 1 April 2023, for Transactions occurring at contactless-enabled POS Terminals in all other Asia/Pacific Region countries and territories except Japan, Republic of Korea, and Taiwan.

The following Rule applies to China domestic Transactions only.

An Acquirer and each of its Merchants must support POS Transactions, Payment Transactions, Refund Transactions, and full reversals when performed to cancel a POS Transaction that the Acquirer cannot complete due to a technical problem.

The Acquirer may also support the below payment or transfer type transactions:

- China Funds Transfer Transactions
- China Deposit Transactions

An Acquirer must not discriminate.

2.2 Issuer Authorization Requirements

For China Domestic Transactions, the Rule on this subject is modified as follows.

In China, when a Chip Card is used to transact at a Hybrid Terminal, the Transaction must be routed by means of the chip payment application.

2.2.1 Issuer Host System Requirements

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

An Issuer that chooses to enable the purchase with cash back Transaction type for Debit Mastercard (including prepaid) or Maestro (including prepaid) Account ranges must support the purchase with cash back Transaction type on its host system interfaces.

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

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

For China Domestic Transactions, an Issuer's host system interface must support the online processing of:

- POS Transactions
- Payment Transactions
- Refund Transactions
- Full Reversal

- Cash withdrawals at ATM Terminals
- Funds Transfer Transactions; and
- Deposit Transactions.

For China Domestic Transactions, in the event that an Issuer does not 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 not discriminate against or discourage the above transaction types in favor of any other acceptance brand or switch network.

2.3 Authorization Responses

For China Domestic Transactions, the Rule on this subject is modified as follows.

An Acquirer must comply with the authorization response wait time requirements set forth in "Maximum Response Times" in Chapter 2 of the China Switch Specifications.

An Issuer must comply with the authorization response requirements set forth in "Maximum Response Times" in Chapter 2 of the *China Switch Specifications*.

2.5 Preauthorizations

2.5.1 Preauthorizations - Mastercard POS Transactions

For China Domestic POS Transactions, the Rule on this subject is modified as follows.

All preauthorization completion corresponding to a preauthorization must be initiated within **30 calendar days** of the authorization approval date.

The preauthorization completion amount must be less than or equal to the amount approved in the corresponding preauthorization.

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.

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.

2.7 Final Authorization

In China, a domestic final authorization request is identified in the Financial Transaction Request/0200 message when DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains a value of 0 and DE 48 (Additional Data), 61 (POS Data), subfield 5 (Final Authorization Indicator) contains a value of 1.

Effective 3 April 2024 for India Domestic Transactions, the Rule on this subject is modified as follows.

When 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 four calendar days of the authorization approval date; and
2. The presented Transaction amount must equal the authorized amount.

2.8 Message Reason Code 4808 Chargeback Protection Period

Effective 3 April 2024 for India Domestic Transactions, the Rule on this subject is modified as follows.

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
Final authorization	Four calendar days from the authorization approval date

2.11 Full and Partial Reversals

2.11.1 Full and Partial Reversals—Acquirer Requirements

POS Transactions

Effective 3 April 2024 for India Domestic Transactions, the Rule on this subject is modified as follows.

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 four calendar days after the authorization date for any other authorization message.

2.12 Full and Partial Approvals

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

Issuers and Acquirers are not required to support partial approvals.

2.13 Refund Transactions and Corrections

In China, the China Switch allows the Customer to use the China Dispute Resolution Platform to manually initiate a refund for a processed domestic Transaction. The Standards in this manual applicable to a refund Transaction will also apply to a domestic manual refund Transaction.

2.13.1 Refund Transactions - Acquirer Requirements

For **China Domestic Transactions**, the Rule on this subject is modified as follows.

An Acquirer must support the online authorization of Mastercard, Debit Mastercard, and Maestro refund Transactions acquired on the Dual Message System (with the exception of refunds for Contactless transit aggregated Transactions) and enable refund Transaction authorization service for a Merchant upon request. The Acquirer must forward each refund Transaction authorization request to the Issuer at the time of the Transaction, rather than in a batch, so that the Merchant receives the Issuer's response while the Cardholder is at the POS and before offering the Cardholder a refund Transaction receipt.

Original Purchase Identifier

The Acquirer must follow the requirements as per the table below for population of the Original Purchase Identifier. 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.

If the online refund Transaction occurs...	The Acquirer...
Within 180 days from the original Transaction date	The Acquirer must populate DE 48, subelement 59 (Original Network Reference Number) of the refund Transaction authorization request message with unique identifier from the original purchase Transaction, consisting of the values in DE 63 (Network Data), subfield 3 (Network Reference Number); and DE 15 (Date, Settlement) of the purchase of the Transaction authorization approval response message.
After 180 days from the original Transaction date	The Acquirer is strongly recommended to populate DE 48, subelement 59 (Original Network Reference Number) of the refund Transaction authorization request message with unique identifier from the original purchase Transaction, consisting of the values in DE 63 (Network Data), subfield 3 (Network Reference Number); and DE 15 (Date, Settlement) of the purchase of Transaction authorization approval response message.

For **India Domestic Transactions**, the Rule on this subject is modified as follows.

Original Purchase Identifier

The Acquirer must 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.

Canada Region

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

2.1 Acquirer Authorization Requirements

2.1.1 Acquirer Host System Requirements

The Acquirer of a Merchant located in the Canada Region must ensure that its host system and those of its Service Providers:

- Are capable of processing Domestic Debit Mastercard Transactions; and
- Populates the value of Y in DE 48 (Additional Data—Private Use), subelement 18 (Service Parameters), subfield 01 (Canada Domestic Indicator) of the Authorization Request/0100 message for each Mastercard Transaction initiated at Merchants that have provided consent to accept domestically issued Debit Mastercard Cards.

Initiating a Domestic Debit Mastercard Transaction that contains the Y, a Canada Region Acquirer affirms that the Merchant has agreed to accept domestically issued Debit Mastercard Cards.

2.2 Issuer Authorization Requirements

Name Validation Requests

Effective 3 June 2025, a Canada Region Issuer of a Mastercard (including prepaid) or Debit Mastercard Card Program must:

- Validate the sender or receiver name data provided in DE 108 (Additional Transaction Reference Data) of a name validation request by comparing the data to the Cardholder name(s) registered by the Issuer of the Card or Account; and
- Provide a match, no match, or partial match response to each name validation request in the applicable response field, as described in the applicable Dual Message System or Single Message System technical manual.

The name validation service may be performed by the Issuer, the Issuer's Service Provider, or the Mastercard on-behalf Name Match Service. The requirement to support name validation does not apply to Card Programs where no Cardholder name is associated with the Account, including non-reloadable prepaid, vehicle-assigned Mastercard Corporate Fleet, and Central Travel Solutions Card Programs.

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 in Rule 2.12 with a Debit Mastercard or prepaid Mastercard Account range.

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.

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

Strong Customer Authentication (SCA) Requirements

If the Issuer and the Acquirer are located in an SCA Country, but the Merchant is not, EMV 3DS authentication requests must include the Mastercard "Merchant Data" EMV 3DS Message Extension, with Field 3 containing the Acquirer country code. In other cases, it is recommended to provide the Acquirer country code in the Mastercard "Merchant Data" EMV 3DS Message Extension Field 3.

The Issuer and its Access Control Server are advised to use the Acquirer country code in the Mastercard "Merchant Data" EMV 3DS Message Extension 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.

Authentication Outage Exception

The following Rules apply to Intracountry and Cross-border Transactions within and between SCA Countries.

An Acquirer may permit a Merchant to use the Authentication Outage Exception flag in authorization request messages. The Merchant must first attempt use of a suitable exemption (subject to the Acquirer's approval) before resorting to the Authentication Outage Exception. The Acquirer must ensure that the Merchant does not misuse the Authentication Outage Exception as a means to bypass authentication. Authentication failure must persist for at least five minutes, leading all authentications to fail (i.e., no attempt responses provided) before the Authentication Outage Exception is used. Authentication must be resumed as soon as the

outage is resolved. The Acquirer must promptly provide full and clear evidence of the outage upon the Corporation's request.

The Authentication Outage Exception must in no case be used for a Transaction or an Account status inquiry that sets up Merchant-initiated Transactions or recurring payment arrangements. A Transaction completed using the Authentication Outage Exception is not protected from fraud-related chargebacks.

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., alternative technical SCA solution delegation to the Merchant), or exemption under Article 17 of the PSD2 RTS (or corresponding legislation) applied with the Merchant's knowledge.

When SCA by the Issuer is not required, or when it has been delegated, or when SCA has been omitted, the Merchant must provide to the Acquirer the reason for omitting authentication (e.g., exemption or exclusion). The Merchant must not forward a Remote Electronic Transaction without providing the reason for omitting authentication. The Acquirer must indicate the reason for the exemption or exclusion in the appropriate field of the authorization message as specified by the registered switch of its choice. The Acquirer must not submit the authorization request without indicating the reason for omitting authentication.

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.

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 Mastercard "Merchant Data" EMV 3DS Message Extension 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.

An Acquirer of e-commerce Merchants that accept corporate Cards, and an Issuer of such Cards must support the Mastercard "Merchant Data" EMV 3DS Message Extension flag in EMV 3DS authentication requests. This flag indicates if the conditions for the exemption under Article 17 of the PSD2 RTS (or corresponding legislation) are met, so that this exemption can be applied by the Issuer. The flag is in the Mastercard "Merchant Data" EMV 3DS Message Extension Field 4 (Secure Corporate Payment).

Account Status Inquiry (ASI) Requests

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

References to ASI request messages and data fields are replaced by the corresponding message type and data fields of the registered switch of the Customer's choice.

Echoing of Transaction Link ID

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

References to authorization messages and data fields are replaced by the corresponding message types and data fields of the registered switch of the Customer's choice.

2.2 Issuer Authorization Requirements

In the EEA, UK and Gibraltar, 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.

SCA Requirements

The following Rules apply to Intracountry and Cross-border Transactions within and between SCA Countries.

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.

An Issuer that requires authentication for more than 10% of authorization requests which indicate the application of an Acquirer exemption or SCA delegation will be automatically enrolled in the Smart Authentication Direct for Acquirer Exemption (SADAE) service.

Authentication Outage Exception

An Issuer must be able to receive and process the Authentication Outage Exception flag in authorization messages. It is recommended that the Issuer indicate clearly in the authorization response whether or not the Merchant should attempt authentication at a later time when the outage is resolved.

Account Status Inquiry (ASI) Requests

In the EEA, UK and Gibraltar, the Rule on this subject is modified as follows. References to ASI request messages and data fields are replaced by the corresponding message type and data fields of the registered switch of the Customer's choice.

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, does not apply to Maestro Chip-only Cards, as such term is defined in section 6.11, "Maestro Chip-only Card Programs," Chapter 13 of the *Mastercard Rules*.

In the EEA, UK and Gibraltar, 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.

Smart Authentication Stand-In

An Issuer in Armenia, Azerbaijan, Belarus, Israel, Georgia, Kazakhstan, Kyrgyzstan, Tajikistan, Russian Federation (except domestic authentication processed by NSPK), Switzerland, Turkey, Turkmenistan, or Uzbekistan must participate in Smart Authentication Stand-In. Issuers in all other Europe Region countries must participate in Smart Authentication Stand-In or an alternative authentication stand-in solution.

2.2.3 ATM Transaction Requirements for Mastercard Credit Card Issuers

In the EEA, UK and Gibraltar, 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 4.10.1.

Preauthorizations occurring at an electric vehicle charging station and identified with MCC 5552 (Electric Vehicle Charging) must be performed as described in Rule 4.10.2.

In the EEA, UK and Gibraltar 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, electric vehicle charging Transactions, and Contactless transit aggregated Transactions.

As an exception to the preceding Rule, preauthorizations for an estimated maximum amount are permitted for Maestro POS Transactions conducted in a Card-present environment, at vending machines located in the Netherlands and Switzerland that are identified with MCC 5499 (Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores). 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.

Issuers in the Netherlands and Switzerland, respectively, must be able to receive the advice message and must post the Transaction to the Cardholder's Account on the basis of the advice message, rather than the preauthorization response. Support of Maestro preauthorizations at vending machines in the Netherlands and Switzerland is optional for Issuers in other countries.

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 Rule on this subject is modified as follows.

The Acquirer must ensure that when an authorization request for an amount greater than zero is identified as a final authorization:

1. The Transaction may no longer be cancelled and must not be reversed after the authorization request is approved in full by the Issuer, except upon Cardholder request or when non-completion is unavoidable for technical reasons such as telecommunications failure or POS Terminal failure; and
2. The authorization being requested is for the final Transaction amount.

In the EEA, UK and Gibraltar, 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
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

[4] 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.

2.9 Multiple Authorizations

In the Europe Region, the Rule on this subject applies to both Mastercard POS Transactions and Maestro POS Transactions.

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, UK and Gibraltar, 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, UK and Gibraltar, 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:

MCC	Description
5310	Discount Stores

MCC	Description
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 4.10.1.

A Customer must support partial approvals on Mastercard and Maestro if it supports them on other brands, for the same product types and Merchant types as on the other brands. To the extent that support for partial approvals is not required on other brands, then it is not required on Mastercard or Maestro, with the exception of support at Merchants identified with MCC 5542 as set out in the preceding paragraph.

In **Ukraine**, the Rule on this subject is modified as follows:

Effective 1 July 2023, all Issuers must support and participating Acquirers may offer partial approval on Mastercard, Debit Mastercard, and Maestro Account ranges. This requirement applies to Card-present Transactions occurring at attended POS Terminals and Card-not present Transactions.

In **Moldova**, the Rule on this subject is modified as follows:

Effective 1 January 2024, all Issuers must support and participating Acquirers may offer partial approvals on Mastercard, Debit Mastercard, and Maestro Account ranges, for Card-present Transactions occurring at attended POS Terminals and Card-not present (CNP) Transactions.

2.13 Refund Transactions and Corrections

2.13.1 Refund Transactions—Acquirer Requirements

In the EEA, UK, and Gibraltar, 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, UK, and Gibraltar, 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, UK and Gibraltar, 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 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, UK and Gibraltar, 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.

2.22 Co-badged Cards - Acceptance Brand Identifier

The following Rules apply for Intracountry POS Transactions in Serbia, Bosnia and Herzegovina, North Macedonia, Gibraltar, the United Kingdom, and EEA countries and for Cross-border POS Transactions between Serbia, Bosnia and Herzegovina, North Macedonia, Gibraltar, the United Kingdom and an EEA country, and for Intra-EEA POS Transactions 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.

2.2 Issuer Authorization Requirements

2.2.1 Issuer Host System Requirements

In Colombia and Venezuela, an Issuer that chooses to enable the purchase with cash back Transaction type for Debit Mastercard (including prepaid) or Maestro (including prepaid) Account ranges must support the purchase with cash back Transaction type on its host system interfaces.

2.5 Preauthorizations

2.5.2 Preauthorizations - Maestro POS Transactions

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

Each Card-not-present Maestro POS Transaction preauthorization initiated with a debit Card issued in Brazil and used at a Merchant located in Brazil is valid for a period of seven (7) calendar days from the preauthorization approval date. Additional preauthorization requests may be submitted to extend the validity period or increase the authorized amount, as described in Rule 2.9 Multiple Authorizations of this Latin America and the Caribbean Region section.

2.6 Undefined Authorizations

In the Latin America and the Caribbean Region, this Rule applies to Transactions occurring on or before 18 August 2025. As of 19 August 2025, this Rule no longer applies.

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 greater than zero; **and**
2. The final Transaction amount may differ from the authorized amount; **and**
3. The Transaction is not expected to be canceled 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.

2.9 Multiple Authorizations

In Brazil, the Rule on this subject is modified as follows with respect to Card-not-present Maestro POS Transactions initiated with a debit Card issued in Brazil at a Merchant located in Brazil.

Following Issuer approval of the initial preauthorization request, a Merchant may submit one or more additional preauthorization requests for the same Card-not-present Maestro POS Transaction, subject to the following conditions:

1. The original and each additional preauthorization request for the same Transaction is valid for a period of seven (7) calendar days from the authorization approval date.
2. Each additional approved preauthorization:
   a. If submitted for a zero amount, extends the authorization validity period with no change to the total authorized Transaction amount; and
   b. If submitted for a non-zero amount, both extends the authorization validity period and incrementally increases the total authorized Transaction amount.
3. If an additional preauthorization request is declined, then the most recent previously approved preauthorization remains valid. For example, if the Issuer approved the original BRL 100 preauthorization request on June 1 and declined an additional BRL 25 preauthorization request on June 7, then the Transaction must be completed by June 8 (when the original preauthorization expires) for BRL 100 (the original approved amount).
4. If any preauthorization request expires before the Transaction completion message is sent, then the Merchant or Acquirer must initiate a new original preauthorization request for the Transaction.

The processing of multiple preauthorization requests for the same Maestro POS Transaction must occur as follows.

Preauthorization Message (0200/0210)	The Acquirer provides:	The Mastercard Network populates:
Preauth1 (original preauthorization message)	In DE 4 (Amount, Transaction), the original preauthorization request amount	The authorization date in DE 15 (Date, Settlement) and the switch serial number [SSN] in DE 63 (Network Data)
Preauth2 (first additional preauthorization message for the same Transaction)	• In DE 4, the additional amount being authorized, or a zero amount (to extend the authorization validity without increasing the authorized amount) • In DE 15 and DE 63, the same values as received in the **Preauth1** 0210 message	• **Preauth2** authorization date in DE 15 • **Preauth2** SSN in DE 63 • **Preauth1** SSN in DE 48 subelement 59 (Original Switch Serial Number) • In DE 54 (Amounts, Additional), subfield 2 (Amount Type), the value of 92 and in subfield 5 (Amount), the **total cumulative authorized amount**
Preauth3 (second additional preauthorization message for the same Transaction)	• In DE 4, the additional amount being authorized, or a zero amount • In DE 15 and DE 63, the same values as received in the **Preauth2** 0210 message	• **Preauth3** authorization date in DE 15 • **Preauth3** SSN in DE 63 • **Preauth2** SSN in DE 48 subelement 59 • In DE 54, subfield 2, the value of 92 and in subfield 5, the **total cumulative authorized amount**

2.10 Multiple Clearing or Multiple Completion Messages

2.10.2 Maestro Transactions

An Acquirer of a Maestro Merchant located in Brazil that processes a Maestro Card-not-present Transaction involving a debit Card issued in Brazil has the option to submit one or more linked completion messages within a period of seven days from the settlement date.

Acquirer Requirements

1. At the time of the Cardholder's purchase of goods or services, an Acquirer that supports this processing option must populate the following values in the Financial Transaction Request/0200: multiple completion message.

Table 3: Financial Transaction Request/0200 message: multiple completion message

Field	Value
DE 4 (Amount, Transaction)	The total purchase amount
DE 61 (Point of Service [POS] Data), subfield 7 (POS Transaction Status)	4 (Preauthorization Request)
DE 61, subfield 12 (POS Authorization Life Cycle)	07 (Partial completion processing supported)

2. Within seven days of the date contained in DE 15 (Date, Settlement) of the Financial Transaction Request Response/0210: multiple completion message, the Acquirer may submit either one or several Financial Transaction Advice/0220: multiple completion messages. Each completion message must contain the following values.

Table 4: Financial Transaction Advice/0220: multiple completion message

Field	Value
DE 4 (Amount, Transaction)	The Transaction amount being fulfilled with this completion message; which may be all or a portion of the total purchase amount
DE 15 (Date, Settlement)	The same value received in DE 15 of the Financial Transaction Request Response/0210: multiple completion message
DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code)	290 (APS approved transaction; preauthorized by issuer)
DE 60, subfield 2 (Advice Reason Detail Code)	– 1403 (Previously approved authorization: partial amount, multiple completions) – 1404 (Previously approved authorization: partial amount, final completion)
DE 61, subfield 7 (POS Transaction Status)	4 (Preauthorization request)
DE 61, subfield 12 (POS Authorization Life Cycle)	07 (Partial completion processing supported)

Issuer Requirements

Upon receiving a Financial Transaction Advice/0220: multiple completion message containing a value of 1403 or 1404, the Issuer should:

1. Match the completion message to the original Financial Transaction Request/0200 message by comparing the data contained in DE 48, subelement 59 (Original Switch Serial Number)

to the original Switch Serial Number (SSN) in the original 0210: multiple completion message from DE 63 (Network Data); and

2. Adjust any hold on the availability of funds in the Cardholder's Account in accordance with its standard Account management practice. In any event, the Issuer should release any remaining unused amount still held after seven days from the settlement date of the Financial Transaction Request/0200: multiple completion message.

If the completion message contains a value of...	Then the Issuer is advised to...
1403	Reduce the hold placed on the Cardholder's Account in connection with the approved Financial Transaction Advice/0220: multiple completion message by the amount in DE 4 (Amount, Transaction).
1404	Release any unused funds in connection with the approved Financial Transaction Request/0200: multiple completion message.

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.

Middle East/Africa Region

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

2.1 Acquirer Authorization Requirements

In the Middle East/Africa 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 South Africa, the Rule on this subject is modified as follows.

Effective for Debit Mastercard and Maestro Transactions (both Domestic and Cross-border) conducted in South Africa on or after 17 October 2025 and submitted to the Mastercard network for processing, the Acquirer must either (i) follow the Transaction message specifications and processing requirements described in the *Real-time Clearing – Acquirer Product Guide* for the Clear Now product or (ii) use the Mastercard Single Message System (for Maestro Transactions only) and comply with the single message format requirements described in the *Single Message System Specifications*, for all the Transaction types listed below:

- Card-present purchase Transactions and purchase with cash back Transactions, with the exception of Transactions identified with any of the following MCCs:
  - MCCs 3000 through 3350 (Airlines, Air Carriers)
  - MCCs 3351 through 3500 (Car Rental Agencies)
  - MCCs 3501 through 3999 (Lodging: Hotels, Motels, Resorts)
  - MCC 4011 (Railroads; Freight)
  - MCC 4111 (Transportation: Suburban and Local Commuter Passenger, including Ferries)
  - MCC 4112 (Passenger Railways)
  - MCC 4121 (Limousines and Taxicabs)
  - MCC 4131 (Bus Lines)
  - MCC 4411 (Cruise Lines)
  - MCC 4511 (Air Carriers, Airlines: Not Elsewhere Classified)
  - MCC 4722 (Travel Agencies and Tour Operators)
  - MCC 4789 (Transportation Services: not elsewhere classified)
  - MCC 5542 (Fuel Dispenser, Automated)
  - MCC 5552 (Electric Vehicle Charging)
  - MCC 7011 (Lodging: Hotels, Motels, Resorts: not elsewhere classified)
  - MCC 7512 (Automobile Rental Agency: not elsewhere classified)
  - MCC 7513 (Truck Rental)
- Card-not-present purchase Transactions identified with any of the following MCCs:
  - MCC 4814 (Telecommunication Services including but not limited to prepaid phone services and recurring phone services)
  - MCC 4816 (Computer Network/Information Services)
  - MCC 5817 (Digital Goods: Software Applications [Excluding Games])
  - MCC 5818 (Digital Goods: Multi-Category)
  - MCC 6300 (Insurance Sales, Underwriting, and Premiums)
- Manual Cash Disbursement Transactions (MCC 6010)
- ATM Transactions (MCC 6011)
- Payment Transactions (identified with a value of 28 in DE 3, subfield 1)
- Refund Transactions (identified with a value of 20 in DE 3, subfield 1)

2.7 Final Authorizations

In the Middle East/Africa Region, the Acquirer must ensure that any authorization request is identified as a final authorization only if:

- The Transaction may no longer be cancelled and must not be reversed after the authorization request is approved in full by the Issuer, except upon Cardholder request or when non-completion is unavoidable for technical reasons such as telecommunications failure or POS Terminal failure; and
- The authorization being requested is for the final Transaction amount.

2.12 Full and Partial Approvals

In the Middle East/Africa Region, the Rule on this subject is modified as follows.

An Issuer and an Acquirer in Jordan or South Africa is not required to support partial approval.

2.21 Merchant Payment Gateway Identifier (MPG ID)

The Rule on this subject does not apply in the following countries: Jordan, Nigeria and Pakistan.

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 all valid CVM options for Chip Transactions, including but not limited to PIN (both offline and online), 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.

Name Validation Requests

Effective 3 June 2025, a U.S. Region Issuer of a Mastercard, Debit Mastercard (including prepaid), or Maestro (including prepaid) Card Program must:

- Validate the sender or receiver name data provided in DE 108 (Additional Transaction Reference Data) of a name validation request by comparing the data to the Cardholder name(s) registered by the Issuer of the Card or Account; and
- Provide a match, no match, or partial match response to each name validation request in the applicable response field, as described in the applicable Dual Message System or Single Message System technical manual.

The name validation service may be performed by the Issuer, the Issuer's Service Provider, or the Mastercard on-behalf Name Match Service. The requirement to support name validation does not apply to Card Programs where no Cardholder name is associated with the Account, including non-reloadable prepaid, vehicle-assigned Mastercard Corporate Fleet, and Central Travel Solutions Card Programs.

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 BusinessCard 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

Day	Minimum Transaction Count	Recommended Transaction Count	Minimum Transaction Amount
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.

An Acquirer must ensure that a Merchant accepting Debit Mastercard Cards 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. This requirement applies with respect to all MCCs for which the Acquirer is required to support partial approvals, as listed in Rule 2.12.

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.

2.14 Balance Inquiries

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

Acquirers and prepaid Card Issuers must support POS balance inquiries for prepaid Debit Mastercard and prepaid Maestro Account ranges. The Acquirer of a Merchant offering POS balance inquiries must ensure each balance inquiry occurs at a Cardholder-operated Terminal as a magnetic stripe or Chip Transaction with PIN.

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.

2.2 Issuer Authorization Requirements

2.2.2 Stand-In Processing Service

In the U.S. Region and U.S. Territories, the following additional requirements apply.

An Issuer must use the Stand-In Processing Service for all of its debit cards that provide Maestro functionality. The Stand-In Parameters may be set below the Corporation's default TCC limit for Non-Mastercard BIN Maestro card-not-present debit card Transactions.

In the event that fraudulent activity is detected, 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 Non-Mastercard BIN Maestro card-not-present debit card Transactions.

2.5 Preauthorizations

2.5.2 Preauthorizations—Maestro POS Transactions

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

Each Maestro card-not-present (CNP) POS Transaction preauthorization initiated with a Non-Mastercard BIN Maestro card-not-present (CNP) debit card is valid for a period of seven (7) calendar days from the preauthorization approval date, when the preauthorization request message contains a value of 07 in DE 61, subfield 12 (POS Authorization Life Cycle). Additional preauthorization requests may be submitted to extend the validity period or increase the authorized amount, as described in Rule 2.9 Multiple Authorizations of this Additional U.S. Region and U.S. Territories section.

The Authorization-related Chargeback described in Chapter 4 Single Message System Chargebacks for Non-Mastercard BIN Maestro Card-Not-Present (CNP) Debit Transactions of the Chargeback Guide may apply if the Transaction amount in the preauthorization completion message was not fully authorized.

2.9 Multiple Authorizations

In the U.S. Region and U.S. Territories, the Rule on this subject is modified as follows with respect to Maestro card-not-present (CNP) POS Transactions effected with Non-Mastercard BIN Maestro card-not-present (CNP) debit cards.

Following Issuer approval of the initial preauthorization request, a Merchant may submit one or more additional preauthorization requests for the same card-not-present (CNP) Maestro POS Transaction, subject to the following conditions:

1. The original and each additional preauthorization request for the same Transaction is valid for a period of seven (7) calendar days from the authorization approval date, when the preauthorization request message contains a value of 07 in DE 61, subfield 12 (POS Authorization Life Cycle).
2. Each additional approved preauthorization:
   a. If submitted for a zero amount, extends the authorization validity period with no change to the total authorized Transaction amount.
   b. If submitted for a non-zero amount, both extends the authorization validity period and incrementally increases the total authorized Transaction amount.
3. If an additional preauthorization request is declined, then the most recent previously approved preauthorization remains valid. For example, if the Issuer approved the original USD 100 preauthorization request on 1 June and declined an additional USD 25 preauthorization request on 7 June, then the Transaction must be completed by 8 June (when the original preauthorization expires) for USD 100 (the original approved amount).
4. If any preauthorization request expires before the Transaction completion message is sent, then the Merchant or Acquirer must initiate a new original preauthorization request for the Transaction.

The processing of multiple preauthorization requests for the same Maestro POS Transaction must occur as follows.

Preauthorization message (0200/0210)	The Acquirer provides:	The Mastercard Network populates:
Preauth1 (original preauthorization message)	In DE 4 (Amount, Transaction), the original preauthorization request amount	The authorization date in DE 15 (Date, Settlement) and the switch serial number [SSN] in DE 63 (Network Data)
Preauth2 (first additional preauthorization message for the same Transaction)	• In DE 4, the additional amount being authorized, or a zero amount (to extend the authorization validity without increasing the authorized amount) • In DE 15 and DE 63, the same values as received in the **Preauth1** 0210 message • In DE 105 (Multi-Use Transaction Identification Data), subelement 001 (Transaction Link Identifier [TLID]), the same value as received in the **Preauth1** 0210 message	• **Preauth2** authorization date in DE 15 • **Preauth2** SSN in DE 63 • **Preauth1** SSN in DE 48, subelement 59 (Original Switch Serial Number) • In DE 54 (Amounts, Additional), subfield 2 (Amount Type), the value of 92 and in subfield 5 (Amount), the **total cumulative previously authorized and currently requested amount**
Preauth3 (second additional preauthorization message for the same Transaction)	• In DE 4, the additional amount being authorized, or a zero amount • In DE 15 and DE 63, the same values as received in the **Preauth2** 0210 message • In DE 105 (Multi-Use Transaction Identification Data), subelement 001 (Transaction Link Identifier [TLID]), the same value as received in the **Preauth2** 0210 message	• **Preauth3** authorization date in DE 15 • **Preauth3** SSN in DE 63 • **Preauth1** SSN in DE 48, subelement 59 • In DE 54, subfield 2, the value of 92 and in subfield 5, the **total cumulative previously authorized and currently requested amount**

The Authorization-related Chargeback described in Chapter 4 Single Message System Chargebacks for Non-Mastercard BIN Maestro Card-Not-Present (CNP) Debit Transactions of the Chargeback Guide may apply if the Transaction amount in the preauthorization completion message was not fully authorized.

2.10 Multiple Clearing and Multiple Completion Messages

2.10.2 Maestro Transactions

An Acquirer of a Maestro Merchant located in the U.S. Region or U.S. Territories that processes a Maestro "back of card" (non-Mastercard BIN) card-not-present Transaction involving a debit card issued in the U.S. Region or U.S. Territories has the option to submit one or more linked completion messages within a period of seven days from the settlement date.

Acquirer Requirements

1. An Acquirer that supports this processing option must populate the following values in the Financial Transaction Request/0200 message initiated at the time of the Cardholder's purchase of goods or services.

Table 5: Financial Transaction Request/0200 message

Field	Value
DE 4 (Amount, Transaction)	The total purchase amount
DE 61 (Point of Service [POS] Data), subfield 7 (POS Transaction Status)	4 (Preauthorization Request)
DE 61, subfield 12 (POS Authorization Life Cycle)	07

2. Within seven days of the date contained in DE 15 (Date, Settlement) of the Financial Transaction Request Response/0210 message, the Acquirer may submit either one or several Financial Transaction Advice/0220 completion messages. Each completion message must contain the following data.

Table 6: Financial Transaction Advice/0220 completion message(s)

Field	Value
DE 4 (Amount, Transaction)	The Transaction amount being fulfilled with this completion message, which may be all or a portion of the total purchase amount
DE 15 (Date, Settlement)	The same value received in DE 15 of the Financial Transaction Request Response/0210 message
DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code)	290 (APS approved transaction; preauthorized by issuer)
DE 60, subfield 2 (Advice Reason Detail Code)	One of the following: – 1403 (Previously approved authorization - partial amount, multiple completions) – 1404 (Previously approved authorization - partial amount, final completion)

Field	Value
DE 61, subfield 7 (POS Transaction Status)	4 (Preauthorization request)
DE 61, subfield 12 (POS Authorization Life Cycle)	07
DE 105 (Multi-Use Transaction Identification Data), subelement 001 (Transaction Link Identifier [TLID])	Effective 17 October 2025, the same value received in DE 105, subelement 001 of the Financial Transaction Request Response/0210 message

Issuer Requirements

Upon receiving a Financial Transaction Advice/0220 completion message containing a value of 1403 or 1404, the Issuer should:

1. Match the completion message to the original Financial Transaction Request/0200 message by comparing the data contained in DE 48, subelement 59 (Original Switch Serial Number) to the original Switch Serial Number (SSN) in the original 0200 message from DE 63 (Network Data) and effective 17 October 2025, the data contained in DE 105, subelement 001 (Transaction Link Identifier [TLID]) to the DE 105, subelement 001 value in the original 0200 message.
2. Adjust any hold on the availability of funds in the Cardholder's Account in accordance with its standard Account management practice. In any event, the Issuer should release any remaining unused amount still held after seven days from the settlement date of the Financial Transaction Request/0200 message.

If the completion message contains a value of...	Then the Issuer is advised to...
1403	Reduce the hold placed on the Cardholder's Account in connection with the approved Financial Transaction Advice/0220 message by the amount in DE 4 (Amount, Transaction)
1404	Release any unused funds in connection with the approved Financial Transaction Request/0200 message.

2.18 Transaction Clearing, Queries, and Disputes

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

The Acquirer of a U.S. Region Merchant participating in the substantiation of certain tax-qualified purchases (for example, medical-related, prescription drug, and vision care purchases) must be prepared to respond to an Issuer's request for the retrieval of documentation for a Transaction effected with an eligible U.S. Region-issued Card. The Acquirer must provide the

requested documentation within 30 calendar days of the Central Site Business Date of the Issuer's request.

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....99
3.1.1 Mastercard Card Acceptance Procedures....99
Suspicious Cards....99
3.1.2 Maestro Card Acceptance Procedures....100
3.2 Card-Not-Present Transactions....100
3.3 Obtaining an Authorization....100
3.3.1 Mastercard POS Transaction Authorization Procedures....100
Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions....102
Authorization When the Cardholder Adds a Gratuity....102
Card-Not-Present Transaction Declines....103
Use of Card Validation Code (CVC) 2....104
Capture Card Response....104
3.3.2 Maestro POS Transaction Authorization Procedures....104
3.4 Mastercard Cardholder Verification Requirements....104
CVM Not Required for Refund Transactions....105
Use of PIN for Mastercard Magnetic Stripe Transactions....105
3.5 Maestro Cardholder Verification Requirements....106
3.6 Use of a PIN for Transactions at ATM Terminals and Bank Branch Terminals....106
3.7 Use of a Consumer Device CVM....107
3.8 POI Currency Conversion....107
3.8.1 Cardholder Disclosure Requirements....108
3.8.2 Cardholder Disclosure - Transaction Receipt Information....109
3.8.3 Priority Check-Out....110
3.8.4 Transaction Processing Requirements....110
3.9 Multiple Transactions—Mastercard POS Transactions Only....110
3.10 Partial Payment—Mastercard POS Transactions Only....111
3.11 Specific Terms of a Transaction....111
3.11.1 Specific Terms of an E-commerce Transaction....111
3.12 Charges for Loss, Theft, or Damage—Mastercard POS Transactions Only....112
3.13 Transaction Receipts....112
3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements....114
3.13.2 ATM and Bank Branch Terminal Transaction Receipt Requirements....115

3.13.3 Primary Account Number (PAN) Truncation and Expiration Date Omission....116
3.13.4 Prohibited Information....116
3.13.5 Standard Wording for Formsets....116
3.14 Returned Products and Canceled Services....117
3.14.1 Refund Transactions....118
3.15 Transaction Records....119
3.15.1 Transaction Presentment Time Frames....119
3.15.2 Retention of Transaction Records....120
Variations and Additions by Region....120
Asia/Pacific Region....120
3.14 Returned Products and Canceled Services....120
3.14.1 Refund Transactions....120
3.15 Transaction Records....120
3.15.1 Transaction Presentment Time Frames....120
Europe Region....121
3.1 Card-Present Transactions....121
3.1.1 Mastercard Card Acceptance Procedures....121
3.2 Card-Not-Present Transactions....121
3.3 Obtaining an Authorization....121
3.3.1 Mastercard POS Transaction Authorization Procedures....121
Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions....122
Authorization When the Cardholder Adds a Gratuity....122
3.3.2 Maestro POS Transaction Authorization Procedures....122
3.5 Maestro Cardholder Verification Requirements....122
3.8 POI Currency Conversion....123
3.13 Transaction Receipts....123
3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements. 124
3.13.3 Primary Account Number (PAN) Truncation and Expiration Date Omission....124
3.14 Returned Products and Canceled Services....125
3.14.1 Refund Transactions....125
Latin America and the Caribbean Region....126
3.4 Mastercard Cardholder Verification Requirements....126
3.5 Maestro Cardholder Verification Requirements....126
Middle East/Africa Region....126
3.14 Returned Products and Canceled Services....126
3.14.1 Refund Transactions....126
United States Region....127
3.3 Obtaining an Authorization....127
3.3.1 Mastercard POS Transaction Authorization Procedures....127

3.5 Maestro Cardholder Verification Requirements..... 127
Additional U.S. Region and U.S. Territory Rules..... 128
3.14 Returned Products and Canceled Services..... 128
3.14.1 Refund Transactions..... 128

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

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 in a face-to-face environment to determine the validity of a Mastercard Card (but not an Access Device):

- Check for the presence of the Mastercard or Debit Mastercard hologram, as applicable, or the Premium Brand Mark.
- If the POS Terminal displays the PAN encoded on the magnetic stripe and if the PAN is present on the Card, then compare the last four digits of the PAN on the Card with the four-digit truncated PAN displayed on the POS Terminal.

The following steps may be performed 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).
- If a photograph is present on the personal identification, compare the photograph with the person presenting the Card.

The personal identification type and number must not be recorded 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 obtain an online authorization from the Issuer for all Transactions, with the following exceptions:

1. Transactions at a CAT 3 device.
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 (EUR 200 for Europe Region Merchants) or is equal to or less than the applicable EMV mode Contactless Transaction offline chip authorization limit as published in Chapter 5 of the *Quick Reference Booklet*.

3. Refund Transactions. Effective 18 October 2024 in the Asia/Pacific Region, Europe Region, Latin America and the Caribbean Region (9 January 2025 in Brazil), and Middle East/Africa Region and effective 1 October 2025 in the Canada Region and United States Region, this exception is limited to refund Transactions conducted by airline Merchants and contactless transit aggregated Transaction Merchants, India Domestic refund Transactions, and refund Transactions to the following commercial Card types.

Commercial Card Type	**Card Product Identifier**
Mastercard B2B Variable Interchange Program (VIP)	All applicable values
Mastercard Flex Program (MFP)	All applicable values
Mastercard Wholesale Travel Program (MWP)	All applicable values
Bill Pay Commercial	BPC
Commercial Debit Mastercard Card	MDT
Digital Mastercard	DLL
Digital Mastercard Corporate	DCO
Digital Mastercard Central Travel Solutions	DLA
Mastercard BusinessCard Card	MCB
Mastercard Central Travel Solutions Air Card	MLA
Mastercard Central Travel Solutions Land Card	MLL
Mastercard Commercial Payments Account	MAP
Mastercard Corporate Card	MCO
Mastercard Corporate Executive Card	MEO
Mastercard Corporate Fleet Card	MCF
Mastercard Corporate World Card	MWO
Mastercard Government Commercial Card	MGF
Mastercard Micro-Business Card	MLC
Mastercard Professional Card	MPC
Mastercard Purchasing Card	MCP
Mastercard World Elite Corporate Card	MAC
Prepaid Mastercard Business Card (Non-U.S.)	MRW

4. Transit First Ride Risk (FRR) claim Transactions that are less than or equal to the FRR limit amount applicable in the Merchant's country, as described in Rule 5.6.1.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region" section sections at the end of this chapter.

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, undefined authorization (in Regions where supported), or final authorization, and the use of a reversal to convert the Issuer's approval of a Card-not-present Transaction that the Acquirer or Merchant believes in good faith to be fraudulent to a decline.

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.

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

For Mastercard POS Transactions, any gratuity added by the Cardholder must be included in the authorization request amount and must not be added after authorization is obtained, when:

- The authorization is identified as a final authorization; or
- The Transaction is a Card-not-present Transaction, Chip/PIN Transaction, Contactless Transaction, or Mastercard Consumer-Presented Quick Response (QR) Transaction.

For all other Card-present Transactions, including key-entered, magnetic stripe, and Chip Transactions completed with signature CVM (with or without physical signature collection), a gratuity may be added after authorization is obtained, provided:

- The gratuity does not exceed 20 percent of the authorized amount; or
- If the gratuity exceeds 20 percent of the authorized amount, and the original authorization was identified as a preauthorization, then the Merchant obtains an incremental authorization for the amount in excess of the authorized amount.

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

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.

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

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 "United States Region" section 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

Response Code Value	Description
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.

CVC 2 data must not be stored by the Merchant, its Acquirer, or any Service Provider. Refer to section 3.12 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. Signature collection is optional.

If 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 must not 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	The CVM may be any of the following, provided both the Card or Access Device and the POS Terminal support the CVM: • Signature - When signature is selected as the CVM, the Merchant may optionally request the Cardholder's signature • Online PIN • Consumer Device CVM (CDCVM)

With respect to Mastercard POS Transactions conducted by a Merchant using an MPOS Terminal or a Chip-only MPOS Terminal, PIN is not required if:

1. the Merchant has less than USD 100,000 in annual Transaction volume; and
2. 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.

(The use of an MPOS Terminal or Chip-only MPOS Terminal lacking such capabilities confers no chargeback protection. Refer to Rule 7.4 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.

NOTE: Modifications to this Rule appear in the "Latin America and the Caribbean Region" section at the end of this chapter.

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

Each PIN-capable POS Terminal must meet specific requirements for PIN processing wherever an approved implementation of PIN for magnetic stripe Transactions takes place. Refer to chapter 4 of the *Security Rules and Procedures* for more information.

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. Signature collection is optional.

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

1. Ireland
2. Israel
3. United Kingdom

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. 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, as follows:

- On a Contactless Transaction (including any Contactless transit aggregated Transaction) that is equal to or less than the applicable CVM limit. POI currency conversion optionally may be offered on a Contactless Transaction that exceeds the CVM limit.
- On any Card or Account identified in the Mastercard Parameter Extract (MPE) as ineligible for POI currency conversion, including but not limited to:
  - Any ATM or face-to-face Transaction effected with Mastercard and Maestro Prepaid Cards that have single or multi-currency features;
  - 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 Transaction 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.

– On a Virtual Account used to purchase travel services pursuant to the Mastercard Enterprise Solution Wholesale Travel Program.

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. When POI Currency Conversion is offered for an e-commerce Transaction and the currency conversion option is pre-selected, the Cardholder must be informed of the pre-selection and provided with the means to decline the currency conversion;
- 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;
- The offer must be presented in a clear manner and must not use biased or misleading language that may influence the Cardholder's currency selection; and
- In addition to meeting any requirement under applicable local law or regulation, the offer must comply with the following 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 Requirements

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;
  – Any other fee that can be charged in the event the cardholder selects POI currency conversion;
- The Merchant and Terminal must honor Cardholder's currency selection; and

Each Terminal or Merchant Environment identified as a...	Must include the following message to the Cardholder when POI Currency Conversion is offered...
Unattended POS Terminal	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 language, 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.
ATM Terminal	Before the Cardholder is asked to select a currency in which the Transaction is to be completed, the ATM Terminal must clearly disclose the following language, 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."
E-commerce Transaction	Before the Cardholder is asked to select a currency in which the Transaction is to be completed, the Merchant's website must clearly disclose the following language, verbatim, to the Cardholder during the checkout process: "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."

In its sole discretion, the Corporation may approve or reject the presentation or display of cardholder disclosure at the POI.

3.8.2 Cardholder Disclosure - Transaction Receipt Information

Refer to section 3.13 Transaction Receipts, 3.13.1 POS and Mastercard Manual Cash Disbursement Transaction Receipt Requirements, and section 3.13.2 ATM and Bank Branch Terminal Transaction Receipt Requirements regarding provision of Transaction receipts and the information that must be disclosed on a Transaction receipt when the Cardholder has chosen to use the POI currency conversion service to complete the Transaction.

3.8.3 Priority Check-Out

Before initiating POI Currency Conversion for a priority check-out Transaction, a Merchant must complete a written agreement with the Cardholder that specifies all of the following:

- The Cardholder has been offered a choice of currencies for payment, whether a Transaction should be completed in either the local currency or the billing currency;
- The Cardholder has agreed that POI Currency Conversion will take place;
- The specific Transaction currency agreed by the Cardholder;
- That the Cardholder expressly agrees to POI Currency Conversion;
- Any currency conversion commission, fees, or mark-up on the exchange rate; and
- If applicable, that the exchange rate will be determined by the Merchant at a later time, without additional consultation with the Cardholder.

If the Cardholder actively chooses POI Currency Conversion, the Transaction receipt must include the same disclosures previously provided to the Cardholder in addition to all other required information that is described in detail in Rule 3.8.2 Cardholder Disclosure —Transaction Receipt Information.

3.8.4 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 the Model Screen 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 or installment billing Transaction arrangement separately from any other terms (for example, by checking a box or clicking a "Submit" button indicating the acceptance of recurring payment or installment billing 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 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 Transaction Receipts

A Transaction receipt (also called a Transaction Information Document, or TID) must be offered 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 offered for a refund Transaction.

At POS Terminals

At a POS Terminal (including any MPOS or CAT device unless otherwise stated), a paper Transaction receipt must be offered to the Cardholder. A POS Terminal may also offer the Cardholder the option of a receiving a Transaction receipt electronically in digital form, such as through email, text, Merchant website, or other electronic means. The offer of a Transaction receipt may be made verbally by the Merchant or electronically by the POS Terminal (such as a Cardholder-facing screen asking, "Receipt? Press YES or NO" or "Paper receipt? Email receipt? No receipt?").

The following exceptions to the above Standard apply:

- A Transaction receipt is not required to be offered if the Transaction is a Contactless Transaction (including a Contactless transit aggregated Transaction) that is equal to or less than the CVM limit but must be provided (on paper or digitally) upon Cardholder request.
- 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 and clearly displayed the method for such request at the Merchant location:
  - An unattended POS Terminal identified as a CAT 1, CAT 2, or CAT 3 device and using any of the following MCCs:
    - MCC 4111 (Transportation: Suburban and Local Commuter Passenger, including Ferries)
    - MCC 4112 (Passenger Railways)
    - MCC 4131 (Bus Lines)
    - MCC 4784 (Bridge and Road Fees, Tolls)
    - MCC 4789 (Transportation Services: not elsewhere classified)
    - MCC 5499 (Miscellaneous Food Stores - Convenience Stores, Markets, Specialty Stores)
    - MCC 7523 (Automobile Parking Lots and Garages); 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).
- 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 offer a Transaction receipt, as described in Appendix D.

At ATM and Bank Branch Terminals

A Transaction receipt must be offered for a cash withdrawal or other financial Transaction occurring at an ATM or, if technically feasible, a Bank Branch Terminal.

A Transaction receipt may be paper or electronic, such as a digital receipt through email, text, Merchant website, or other electronic means. The offer of a Transaction receipt may be made verbally or electronically (such as a Cardholder-facing screen asking, "Receipt? Press YES or NO" or "Paper receipt? Email receipt? No receipt?").

ATM cash withdrawals without paper receipts are allowed 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 the following information must be included on a Transaction receipt (no other information is required):

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. If the Cardholder has chosen to use a POI currency conversion service to complete the Transaction as described in Section 3.8 POI Currency Conversion, the Transaction receipt must disclose 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.

6. The Transaction date. (For Transaction date requirements, see Appendix C.)
7. 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.
8. For a Chip Transaction, the application identifier (AID) and the application preferred name or application label.
9. 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. A space for the Cardholder's signature must be omitted from the 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 personal identification is requested for a face-to-face unique Transaction or Manual Cash Disbursement Transaction, the personal identification type and number must not be recorded on the Transaction receipt (refer to Rule 3.1.1).

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 (no other information is required):

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). If the Cardholder has chosen to use a POI currency conversion service to complete the Transaction as described in section 3.8 POI Currency Conversion, the Transaction receipt must disclose 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.
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).
- 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).

In the case of involuntary refunds by airlines or other Merchants as required by law, or 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.

Upon Mastercard approval, a Merchant may offer Cardholders the option of a "fast refund" using the MoneySend Payment Transaction, as described in the Mastercard MoneySend and Funding Transactions Program Standards. The fast refund using the MoneySend Payment Transaction may be submitted to the same Account used in the original purchase (as identified on the purchase Transaction receipt) or to a different Account, for example when the Issuer of the Card or Access Device used in the original purchase declines a refund Transaction authorization request. A Merchant enabled for the fast refund using the MoneySend Payment Transaction must continue to support and offer the refund Transaction.

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, canceled services, or a price adjustment related to a prior purchase.

The refund Transaction:

- must be processed in the same currency as used in the related purchase Transaction; and
- must not exceed the authorized amount of the related purchase Transaction, except as may occur due to currency value fluctuations or when the Merchant agrees to credit return shipping costs.

Key entry of Card data is not permitted for Maestro refund Transactions conducted in a Card-present environment. For information about chip-based refund Transactions, refer to the *M/Chip Requirements for Contact and Contactless* manual.

When the original purchase was...	Then the refund Transaction...
A Chip Transaction	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 unless online authorization occurs. Refer to the *M/Chip Requirements for Contact and Contactless* manual for details. Authorization may occur at the Merchant's option but PIN data is not required; an Issuer must not decline a refund Transaction solely because of the absence of PIN data.
A dual message magnetic stripe Transaction	May be completed without CVM or online authorization from the Issuer.
A single message magnetic stripe Transaction	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 must occur but PIN data is not required; an Issuer must not decline a refund Transaction solely because of the absence of PIN data.

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. Upon providing a full or partial refund for returned products or canceled 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.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region" section at the end of this chapter.

3.15.1 Transaction Presentment Time Frames

Upon receiving the Transaction record, the Acquirer must present the Transaction within the applicable presentment time frame in order to avoid an Expired Chargeback Protection Period chargeback.

The Acquirer must present a Transaction to the Issuer within the following presentment time frames:

- For a Mastercard purchase Transaction, no later than 30 calendar days after the latest authorization approval date for a preauthorization or no later than seven calendar days after the authorization approval date for any other authorization, or for an offline chip-approved purchase Transaction or other Transaction not requiring online authorization by the Issuer, seven calendar days after the Transaction date.
- Seven calendar days after the Transaction date of a Maestro purchase Transaction;
- Seven calendar days after the Transaction date of an ATM Transaction;
- Within one calendar day of the authorization date (and no later than 24 hours after the time of authorization approval) of a Payment Transaction;
- Within the aggregation period described in Section 4.5.1 or 4.5.2, as applicable, for a Contactless transit aggregated Transaction; and
- Within five calendar days of the Transaction date of a refund Transaction (the date on the Transaction receipt, or if the refund Transaction was authorized by the Issuer, then the authorization date).

An Issuer must accept Transactions submitted beyond the applicable time frame if the Cardholder's Account is in good standing or the Transaction can be otherwise honored and posted.

3.15.2 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.

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.

3.15 Transaction Records

Effective 3 April 2024 for India Domestic Transactions, the Rule on this subject is modified as follows:

1. A purchase Transaction must be submitted to its Acquirer in accordance with its Merchant Agreement and in compliance with all applicable laws and regulations.
2. Upon providing a full or partial refund for returned products or canceled services, the Merchant must submit the refund Transaction record to its Acquirer in accordance with its Merchant Agreement and in compliance with all applicable laws and regulations.

3.15.1 Transaction Presentment Time Frames

Effective 3 April 2024 for India Domestic Transactions, the Rule on this subject is modified as follows.

The Acquirer must present a Transaction to the Issuer within the following presentment time frames:

- Within one calendar day of the authorization approval date of a Payment Transaction;
- Within four calendar days of the final authorization approval date for all other Transactions.

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

Suspicious Cards

In the EEA, UK and Gibraltar, 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 the Mastercard Identity Check Program, given that the Issuer may use alternative technical solutions for SCA.

The liability shift applies equally to EMV 3DS as to 3DS 1.0.2. Refer to the *Chargeback Guide* for more information.

3.3 Obtaining an Authorization

3.3.1 Mastercard POS Transaction Authorization Procedures

In the EEA, UK and Gibraltar, 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, UK and Gibraltar, 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, UK and Gibraltar, 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.

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, UK and Gibraltar, 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 Transaction Receipts

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

At POS Terminals

The Merchant is not required to **automatically** offer a paper Transaction receipt to the Cardholder. If the Cardholder expressly requests a receipt, one must be provided, either on paper or digitally.

In the following specific cases, a paper Transaction receipt must be automatically offered:

- A Merchant that requires a paper receipt for a refund must offer the Cardholder a paper receipt;
- A Merchant that applies an exchange or return policy must offer a paper receipt on which the policy is stated, in accordance with Rule 3.11 Specific Terms of a Transaction.
- If a paper receipt is otherwise required by applicable law or regulation (e.g., to document a warranty).

If the Merchant provides a paper cash register receipt, tax invoice, or other type of receipt for a Transaction, it is not required to additionally offer a paper POS Terminal receipt.

Provision of the Transaction receipt by digital (non-paper) means is strongly recommended.

When the Merchant offers a Transaction receipt by digital means, it must clearly inform the Cardholder how to access the receipt and whether the Merchant needs to process any additional Personal Data, such as Cardholder contact details, to enable access to the receipt. The Merchant must limit the processing of the Cardholder's additional Personal Data only for the purpose of making the receipt available to the Cardholder. The Merchant must ensure that the digital receipt is promptly available.

The Merchant's copy of the Transaction receipt need not be on paper and may be stored and provided in digital form.

At a POS Terminal in **France**, a paper Transaction receipt must not be automatically provided. A paper Transaction receipt must be provided in the following cases:

- if the Cardholder expressly requests one,
- in case of cancellation of the Transaction,
- if the Transaction is for a refund,
- if the purchase is of durable goods for which a legal guarantee applies, and
- in any other case specified in applicable law, as amended from time to time.

When a paper Transaction receipt is not provided to the Cardholder, the Merchant is permitted to provide a digital receipt.

At ATM Terminals

ATM Terminals that do not have receipt-printing capability may be deployed in the Europe Region.

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 is allowed only if the ATM Terminal does not have receipt-printing capability or is out of paper. The Cardholder must be advised prior to the Transaction that a printed receipt is not available.

As an exception to this Rule, an ATM Terminal in **France** must have receipt-printing capability and must not automatically provide a paper Transaction receipt. A paper Transaction receipt must be provided in the following cases:

- upon Cardholder request,
- in case of cancellation of the Transaction, and
- in any other case specified in applicable law, as amended from time to time.

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.

Effective from the dates shown in the table below, an Acquirer located in one of the applicable countries must attempt to originate all refunds and price adjustments to the original Card used in the purchase Transaction as a "Fast Refund to Original Card" MoneySend Payment Transaction in accordance with the *Mastercard MoneySend and Funding Transactions Program Standards,* except under the following circumstances:

- The Card is not eligible to receive MoneySend Payment Transactions;
- The Issuer has been identified as not supporting MoneySend Payment Transactions; or
- The refund or price adjustment amount exceeds the applicable MoneySend Payment Transaction limit specified in the *Mastercard MoneySend and Funding Transactions Program Standards* or *Mastercard MoneySend and Funding Transactions Program Standards Addendum for Limits*.

Table 7: Applicable countries

Country or Territory	Effective Date for Card-not-present Refunds	Effective Date for Card-present Refunds
Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Israel, Kosovo, Montenegro, North Macedonia, Romania, Serbia	4 November 2025	4 November 2026

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.

3.4 Mastercard Cardholder Verification Requirements

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

A Merchant Terminal located in Peru may be configured so that "No CVM" is the only CVM supported for Chip Transactions conducted with a Chip Card issued in Peru, provided the Transaction amount is equal to or less than PEN 80.

In this Terminal configuration, "No CVM" replaces both signature and PIN in the Terminal's list of supported CVMs. The Acquirer must only use this Terminal configuration for Domestic Peru Transactions.

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, Eswatini, 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 modified as follows.

For Mastercard POS Transactions effected at a U.S. Region Merchant with a Mastercard Card issued in the U.S. Region, any gratuity added by the Cardholder must be included in the authorization request amount and must not be added after authorization is obtained, when:

- The authorization is identified as a final authorization; or
- The Transaction is a Card-not-present Transaction (with the exception below), Chip/PIN Transaction, Contactless Transaction, or Mastercard Consumer-Presented Quick Response (QR) Transaction.

For all other Card-present Transactions, including key-entered, magnetic stripe, and Chip Transactions completed with signature CVM (with or without physical signature collection), and for Card-not-present Transactions identified with MCC 5812 (Eating Places, Restaurants) or MCC 5814 (Fast Food Restaurants), a gratuity may be added after authorization is obtained, provided:

- The gratuity does not exceed 30 percent of the authorized amount; or
- If the gratuity exceeds 30 percent of the authorized amount, and the original authorization was identified as a preauthorization, then the Merchant obtains an incremental authorization for the amount in excess of 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 30 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, or for e-commerce Transactions (including Non-Mastercard BIN Maestro card-not-present debit card Transactions).

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 section 5.12.2, "Charges to Cardholders" 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 133
4.2 Offline Transactions Performed on Board Planes, Trains, and Ships 133
4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions—Europe Region Only 134
4.4 Contactless Transactions at POS Terminals 135
4.5 Contactless Transit Transactions 135
4.5.1 Mastercard Contactless Transit Aggregated Transactions 135
4.5.2 Maestro Contactless Transit Aggregated Transactions 136
4.6 Contactless Transactions at ATM Terminals 137
4.7 Contactless-only Acceptance 137
4.8 Mastercard Consumer-Presented QR Transactions at POS Terminals 138
4.9 Purchase with Cash Back Transactions 139
4.10 Transactions at Unattended POS Terminals 140
4.10.1 Automated Fuel Dispenser Transactions 141
4.10.2 Electric Vehicle Charging Transactions 142
4.11 PIN-based Debit Transactions—United States Region Only 143
4.12 PIN-less Single Message Transactions—United States Region Only 143
4.13 Merchant-approved Maestro POS Transactions 143
4.14 Mastercard Manual Cash Disbursement Transactions 144
4.14.1 Non-discrimination Regarding Cash Disbursement Services 145
4.14.2 Maximum Cash Disbursement Amounts 145
4.14.3 Discount or Service Charges 145
4.14.4 Mastercard Acceptance Mark Must Be Displayed 145
4.15 Encashment of Mastercard Travelers Cheques 146
4.16 ATM Transactions 146
4.16.1 "Chained" Transactions 146
4.16.2 ATM Transaction Branding 146
4.17 ATM Access Fees 146
4.17.1 ATM Access Fees - Domestic Transactions 147
4.17.2 ATM Access Fees - Cross-border Transactions 147
4.17.3 ATM Access Fee Requirements 147
Transaction Field Specifications for ATM Access Fees 147
Non-discrimination Regarding ATM Access Fees 147

Notification of ATM Access Fee....147
Cancellation of Transaction....147
Sponsor Approval of Proposed Signage, Screen Display, and Receipt....148
ATM Terminal Signage....148
ATM Terminal Screen Display....148
ATM Transaction Receipts....149
4.18 Merchandise Transactions at ATM Terminals....149
4.18.1 Approved Merchandise Categories....149
4.18.2 Screen Display Requirement for Merchandise Categories....150
4.19 Shared Deposits—United States Region Only....150
Variations and Additions by Region....151
Asia/Pacific Region....151
4.1 Chip Transactions at Hybrid Terminals....151
4.5 Contactless Transit Transactions....151
4.5.1 Mastercard Contactless Transit Aggregated Transactions....151
4.9 Purchase with Cash Back Transactions....151
4.10 Transactions at Unattended POS Terminals....152
4.10.1 Automated Fuel Dispenser Transactions....152
4.17 ATM Access Fees....152
4.17.1 ATM Access Fees—Domestic Transactions....152
Canada Region....153
4.9 Purchase with Cash Back Transactions....153
4.10 Transactions at Unattended POS Terminals....153
4.10.1 Automated Fuel Dispenser Transactions....153
4.17 ATM Access Fees....153
4.17.1 ATM Access Fees—Domestic Transactions....153
Europe Region....154
4.1 Chip Transactions at Hybrid Terminals....154
4.2 Offline Transactions Performed on Board Planes, Trains, and Ships....154
4.3 No-CVM Magnetic Stripe and Contact Chip Maestro POS Transactions....154
4.4 Contactless Transactions at POS Terminals....155
4.5 Contactless Transit Aggregated Transactions....156
4.5.1 Mastercard Contactless Transit Aggregated Transactions....156
4.5.2 Maestro Contactless Transit Aggregated Transactions....156
4.9 Purchase with Cash Back Transactions....157
4.10 Transactions at Unattended POS Terminals....161
4.10.1 Automated Fuel Dispenser Transactions....162
4.13 Merchant-approved Maestro POS Transactions....162
4.14 Mastercard Manual Cash Disbursement Transactions....162

4.14.2 Maximum Cash Disbursement Amounts....163
4.17 ATM Access Fees....163
4.17.1 ATM Access Fees - Domestic Transactions....163
4.18 Merchandise Transactions at ATM Terminals....163
4.18.1 Approved Merchandise Categories....163
Latin America and the Caribbean Region....164
4.4 Contactless Transactions at POS Terminals....164
4.5 Contactless Transit Aggregated Transactions....164
4.5.2 Maestro Contactless Transit Aggregated Transactions....164
4.9 Purchase with Cash Back Transactions....164
4.17 ATM Access Fees....166
4.17.1 ATM Access Fees—Domestic Transactions....166
Middle East/Africa Region....167
4.9 Purchase with Cash Back Transactions....167
United States Region....167
4.1 Chip Transactions at Hybrid Terminals....168
4.5 Contactless Transit Transactions....168
4.5.1 Mastercard Contactless Transit Aggregated Transactions....168
4.5.2 Maestro Contactless Transit Aggregated Transactions....169
4.9 Purchase with Cash Back Transactions....169
4.10 Transactions at Unattended POS Terminals....170
4.10.1 Automated Fuel Dispenser Transactions....170
4.11 PIN-based Debit Transactions....170
4.12 PIN-less Single Message Transactions....170
4.14 Mastercard Manual Cash Disbursement Transactions....171
4.14.2 Maximum Cash Disbursement Amounts....171
4.14.3 Discount or Service Charges....172
4.17 ATM Access Fees....172
4.17.1 ATM Access Fees—Domestic Transactions....172
4.18 Merchandise Transactions at ATM Terminals....172
4.18.1 Approved Merchandise Categories....172
4.19 Shared Deposits....172
4.19.1 Non-discrimination Regarding Shared Deposits....173
4.19.2 Terminal Signs and Notices....173
4.19.3 Maximum Shared Deposit Amount....173
4.19.4 Deposit Verification....173
4.19.5 ATM Terminal Clearing and Deposit Processing....174
4.19.6 Shared Deposits in Excess of USD 10,000....174
4.19.7 Notice of Return....174

4.19.8 Liability for Shared Deposits.....175

4.1 Chip Transactions at Hybrid Terminals

A Customer must comply with the Standards set forth in the *M/Chip Requirements for Contact and Contactless* 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 support the signature CVM option (signature collection is not required).
- "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 CVM is preferred to signature CVM 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 "Asia/Pacific Region," "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 (or CDCVM was successfully performed on the device).
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 4411 (Cruise Lines)
    d. MCCs 3000 through 3350 and 4511 (Air Carriers, Airlines)
    e. MCC 5811 (Caterers)

    NOTE: Duty-free purchases are not covered by this Rule.

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 Transactions

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

A Merchant offering Mastercard Contactless transit Transactions that utilizes Contactless-only turnstile or at the point of entry acceptance for transportation are not obligated to accept a tap with a non-reloadable prepaid Account provided that other means to make a purchase are located in close proximity to the Contactless-only turnstile or point of entry acceptance device.

4.5.1 Mastercard Contactless Transit Aggregated Transactions

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. An Acquirer submitting an authorization request to start a Contactless transit aggregated Transaction, either deferred or in real-time, must confirm the Issuer's authorization response was approved, in order to submit the First Presentment/1240 message to clear the aggregated transit fare. As an exception to the foregoing Standard, the Acquirer may submit a First Presentment/1240 message to claim transit debt, up to a specified limit in the country for deferred authorizations that were declined and unrecoverable, pursuant to the transit First Ride Risk (FRR) framework. For more information about transit FRR claim Transactions, refer to Rule 5.6.1.

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 Contactless transit aggregated CVM limit amount as described in Appendix E.
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.

Refer to Rule 4.5.1 in the United States Region section at the end of this chapter for the contactless transit aggregated Transaction procedures applicable to all Transactions occurring at U.S. Region transit Merchant locations.

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

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," and "United States Region" sections 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 CVM 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 CVM limit amount as described in Appendix E.

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," "Latin America and the Caribbean Region," and "United States 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 as set forth in this section, an Acquirer may sponsor Merchants that deploy POS Terminals or MPOS Terminals that use 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 use only contactless payment functionality subsequently deploy POS Terminals or MPOS Terminals with contact payment functionality, such POS Terminals or 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. Merchants in the Asia/Pacific Region, Europe Region, Latin America and the Caribbean Region, or Middle East/Africa Region using an MPOS Terminal that employs either of the following PCI-approved EMV-compliant solutions:
   - Mobile Payments on CoTS (MPoC); or
   - Contactless Payments on CoTS (CPoC).

3. 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
4. Merchants located in Hungary, Poland and Romania that use MCC 5994 - News Dealers and Newsstands.
5. Merchants located in Hungary that use MCC 5462 - Bakeries or MCC 5441 - Candy, Nut, Confectionery Stores.
6. Merchants that use MCC 8398 - Organizations, Charitable and Social Service.

Unattended POS Terminals that use 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 *M/Chip Requirements for Contact and Contactless* manual.

4.9 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 (but not any other type of Mastercard) or Maestro Card or Access Device.
2. In a purchase with cash back Transaction, cash may only be provided in combination with a purchase. An Issuer must not approve only the cash back portion of a Transaction containing both a purchase amount and a cash back amount. The cash back service must not be offered in combination with a Manual Cash Disbursement Transaction or the sale of a quasi–cash instrument. Contactless CVM limits do not apply to purchase with cash back Transactions, meaning that such Transactions always require a CVM.
3. In authorization and clearing messages, each purchase with cash back Transaction must contain:
   a. The value of 09 (purchase with cash back) in DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type).
   b. The total Transaction amount (inclusive of the purchase and cash back amounts) in DE 4 (Amount, Transaction).
   c. The cash back amount in DE 54 (Amounts, Additional).

   The purchase amount, cash back amount, and total Transaction amount must all be in the same currency.

The following requirements apply to Acquirers and Merchants:

1. 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.
2. An offer of purchase with cash back that is promoted at the POI must be available to all Cardholders of each Card type for which the service is supported. The Merchant may prompt the Cardholder to use this service.
3. 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, or as applicable in the Merchant's country.
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.

4. The Acquirer must obtain online authorization approval for the full Transaction amount; support for authorization of the purchase amount only is optional.

The following requirements apply to Issuers:

1. An Issuer must properly personalize each Debit Mastercard and Maestro Card and Access Device (including prepaid issuance) to support the purchase with cash back Transaction type. Support is required for both Domestic and Cross-border Transactions, and on both the contact and contactless interfaces of a Dual Interface Card.
2. The Issuer's authorization host must support the purchase with cash back Transaction data fields and values.
3. The Issuer must make an individual authorization decision for each purchase with cash back Transaction. An Issuer that chooses not to offer the cash back service to particular Cardholders must be capable of providing a value of 87 (Purchase Amount Only, No Cash Back Allowed) in DE 39 (Response Code) of the authorization request response message for an Account in good standing and having a sufficient balance, if the POS Terminal indicates support for purchase-amount-only approvals.

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.

4.10 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.

4.10.1 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 or CAT 2 (for Card-present Transactions), CAT 6 (for e-commerce Transactions), or CAT 7 (for transponder Transactions), as described in Appendix D.

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

Authorization Before Fueling

Each automated fuel dispenser Transaction for which authorization is requested prior to the dispensing of fuel is properly processed as follows:

1. The Acquirer's initial authorization request (0100 or 0200) message (dual message Authorization Request/0100 or single message Financial Transaction Request/0200) to the Issuer must be identified as a preauthorization and reflect one of the following:
   a. A maximum fuel dispense amount as determined by the Merchant or Acquirer;
   b. A specific amount selected by the Cardholder; or
   c. In the U.S. Region only, the amount of USD 1. Upon approval, the Issuer is advised to place a temporary authorization hold on the Account of up to USD 500 for Mastercard Corporate Card®, Mastercard Corporate Executive Card®, Mastercard Corporate Fleet Card®, or Mastercard Corporate Purchasing Card™ Transactions and up to USD 175 for all other Mastercard Transactions. Refer to the Authorization-related Chargeback section in the Dual Message System Chargebacks chapter of the *Chargeback Guide* for more information.
2. If the preauthorization request contains the partial approval support indicator, and the Issuer provides a partial approval response, then the final Transaction amount must not exceed the partial approval amount provided by the Issuer in DE 6 (Amount, Cardholder Billing).
3. After the fuel is dispensed, the Acquirer must send an advice message (dual message Authorization Advice/0120 or single message Acquirer Reversal Advice/0420) containing the final Transaction amount (in DE 4 [Amount, Transaction] of the 0120 message or in DE 95 [Replacement Amounts] of the 0420 message) to the Issuer. The advice message must be sent no later than 60 minutes (in the Europe Region, 20 minutes) after the original preauthorization request.
4. If fuel is not dispensed or the Cardholder otherwise cancels the Transaction then within 60 minutes of authorization approval (in the Europe Region, 20 minutes), the Acquirer must

send either an advice message (Authorization Advice/0120 with a value of zero in DE 4 or Acquirer Reversal Advice/0420 with a value of zero in DE 95) or a full reversal (dual message Reversal Request/0400 with a value of zero in DE 95).

5. Within 60 minutes of receiving the advice message, the Issuer must release any hold that the Issuer placed on the Cardholder's available funds or credit in excess of the Transaction amount specified in DE 4 (Amount, Transaction).
   If the Issuer displays pending automated fuel dispenser Transaction information in Cardholder-facing applications, the information must be based on the advice message Transaction amount.
6. The Acquirer must send a First Presentment/1240 or Financial Transaction Advice/0220 message with the final Transaction amount in DE 4 (Amount, Transaction).

As a best practice, the Merchant should inform the Cardholder in advance of any estimated amount for which authorization will be requested (for example, on a screen display or sticker at the Terminal) and obtain the Cardholder's consent to the amount before initiating the authorization request.

NOTE: A modification to the foregoing paragraph applies in the EEA and appears in the "Europe Region" section at the end of this chapter.

Authorization After Fueling

A Merchant that instead chooses to initiate the Transaction authorization request after the fuel is dispensed does so at the risk of a possible decline or partial approval. Such authorizations are properly identified as final authorizations.

4.10.2 Electric Vehicle Charging Transactions

A Transaction occurring at an unattended POS Terminal for the purchase of electric vehicle charging services is identified with MCC 5552 (Electric Vehicle Charging) and a CAT level indicator of CAT 1 or CAT 2 (for Card-present Transactions) or CAT 6 (for e-commerce Transactions) as described in Appendix D. Alternatively, if the primary business of the Merchant is temporary parking services, then MCC 7523 (Automobile Parking Lots and Garages) may be used.

Contactless-only acceptance is permitted (refer to Rules 4.7 and 7.3.2). A contactless-only Terminal supporting a maximum vehicle charging amount that does not exceed the applicable contactless CVM limit is properly identified as CAT 2. The Transaction may be authorized either prior to or after the vehicle charging, as follows.

Authorization Before Charging

Each electric vehicle charging Transaction for which authorization is requested before vehicle charging begins is properly processed as follows:

1. The Merchant must inform the Cardholder of any estimated amount for which authorization will be requested (for example, on a screen display or sticker at the Terminal) and must obtain the Cardholder's consent to the amount before initiating the authorization

request. The estimated amount may be the Terminal's maximum dispense amount or a specific amount requested by the Cardholder.

2. The Acquirer's initial authorization request (0100 or 0200) message to the Issuer must be identified as a preauthorization. If the preauthorization request contains the partial approval support indicator, and the Issuer provides a partial approval response, then the final Transaction amount must not exceed the partial approval amount provided in DE 6 (Amount, Cardholder Billing).
3. If the Transaction is finalized for an amount that:
   a. Exceeds the authorized amount, then the Acquirer must send an additional (incremental) authorization request for the unauthorized amount (refer to section 2.9); or
   b. Is less than the authorized amount, then within 24 hours of finalization, the Acquirer must either send a partial reversal for the excess authorized amount, or submit the Transaction clearing record.
4. In the case of a Transaction cancelled by the Cardholder, then within 24 hours, the Acquirer must send a full reversal request.

Authorization After Charging

If the Merchant initiates authorization after the vehicle charging is completed, then the Acquirer's authorization request must be identified as a final authorization.

4.11 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.

4.12 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.

4.13 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 *M/Chip Requirements for Contact and Contactless* 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.

4.14 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.

4.14.1 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.

4.14.2 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.

4.14.3 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.

4.14.4 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.

4.15 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.

4.16 ATM Transactions

The following Rules relate to ATM Transaction processing.

4.16.1 "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.

4.16.2 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.

4.17 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.

4.17.1 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.

4.17.2 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.

4.17.3 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 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.

4.18 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.

4.18.1 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.

Merchandise Category	Explanation
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.

4.18.2 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.

4.19 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.

4.1 Chip Transactions at Hybrid Terminals

For China Domestic Transactions, the Rule on this subject is modified as follows.

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 PBoC chip data for each Chip Transaction in DE 55 (Integrated Circuit Card [ICC] System-Related Data) of the Preauthorization Request/0100 or Financial Transaction Request/0200 message. For each Chip Transaction, 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 Preauthorization Request/0100 or Financial Transaction Request/0200 message.

4.5 Contactless Transit Transactions

4.5.1 Mastercard Contactless Transit Aggregated Transactions

Effective 3 April 2024 for India Domestic Transactions, the Rule on this subject is modified as follows.

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 Contactless transit aggregated CVM limit amount as described in Appendix E.
4. The maximum time period from the first tap until the First Presentment/1240 message is generated must be four calendar days or less.

4.9 Purchase with Cash Back Transactions

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

Asia/Pacific Region Issuers are not required to support the purchase with cash back Transaction type.

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

For a Debit Mastercard purchase with cash back Transaction, a maximum cash back amount must be established that does not exceed AUD 500.

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.

4.10 Transactions at Unattended POS Terminals

4.10.1 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.

4.17 ATM Access Fees

4.17.1 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.

4.9 Purchase with Cash Back Transactions

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

An Issuer must technically support and properly personalize each Debit Mastercard and prepaid Mastercard Card and Access Device to support the purchase with cash back Transaction type. Support is required for both Domestic and Cross-border Transactions, and on both the contact and contactless interfaces of a Dual Interface Card.

An Acquirer 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.

4.10 Transactions at Unattended POS Terminals

4.10.1 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.

4.17 ATM Access Fees

4.17.1 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, UK and Gibraltar, 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, UK and Gibraltar, 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, UK or Gibraltar. At POS Terminals located in the EEA, UK and Gibraltar, 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, UK or Gibraltar, 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 CVM 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 CVM limit amount as described in Appendix E.
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, UK or Gibraltar, 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.

4.9 Purchase with Cash Back Transactions

In the Europe Region, the following additional Rules apply to all types of Mastercard and Maestro Transactions, unless otherwise specified.

Acquirer and Merchant Requirements

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.

A Merchant located in the **United Kingdom** is permitted to offer a cash back Transaction without an accompanying purchase, upon presentation of a Debit Mastercard Card. All other Standards applicable to purchase with cash back Transactions must be respected. The maximum cash back amount is GBP 100.

An Acquirer in **Montenegro**, **Romania**, or **Serbia** must technically support purchase with cash back Transactions in its host system and on the attended POS Terminals of its Merchants.

An Acquirer in **Armenia**, **Belarus**, **Georgia**, **Kazakhstan**, **Kyrgyzstan**, **Russia**, **Tajikistan**, **Turkmenistan**, **Ukraine**, and **Uzbekistan** that supports purchase with cash back Transactions must technically support **purchase-only approval** in its host system and at all participating POS Terminals.

In **Albania**, **Austria**, **Bulgaria**, **Cyprus**, **Czech Republic**, **Hungary**, **Kosovo**, **Montenegro**, **North Macedonia**, **Poland**, **Romania**, **Serbia**, **Slovakia**, and **Slovenia**, an Acquirer must itself support in its host systems and must ensure that all POS Terminals deployed that support purchase with cash back Transactions on the contact interface, also support purchase with cash back Transactions on the contactless interface, for both Domestic and Cross-border Transactions.

In **Moldova**, the following purchase with cash back Transaction requirements apply:

- an Acquirer that supports purchase with cash back Transactions must technically support purchase-only approval in its host and at all participating POS Terminals;
- POI currency conversion must not be offered on a purchase with cash back Transaction; and
- a Merchant in Moldova that supports purchase with cash back Transactions must show the cash back amount separately on the Transaction receipt.

Maximum Cash Back Amount

The maximum cash back amount of a purchase with cash back Transaction is set out in the following table.

Table 8: Maximum Cash Back Amount

Country	Maximum Cash Back Amount
Armenia	AMD 30,000
Austria	EUR 200 (no maximum on Intracountry Maestro Transactions completed with PIN or CDCVM)
Belarus	BYN 100
Georgia	GEL 150
Germany	EUR 200
Kazakhstan	KZT 50,000
Kyrgyzstan	KGS 5,000
Moldova	MDL 1,000
Poland	PLN 1,000
Russia	RUB 5,000
Switzerland	CHF 300
Tajikistan	TJS 500
Turkmenistan	TKM 400
Ukraine	UAH 6,000
Uzbekistan	UZS 500,000
All other Europe Region countries	EUR 100 or the local currency equivalent

Except as specified elsewhere in this Rule, an Acquirer or Merchant may establish a lower maximum cash back amount, provided that:

- Any such maximum amount is applied uniformly; and
- 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.

CVM Requirements

The following CVMs must be supported by Issuers and Acquirers for purchase with cash back Transactions:

- Online PIN and offline PIN must be supported for Contact Chip Transactions; and
- Online PIN and CDCVM must be supported for Contactless Transactions.

As an exception to this Rule:

- Only online PIN is supported for Contact Chip Transactions and Contactless Transactions on Cards issued under a BIN assigned for **Russia**; and
- Only online PIN is supported for Contact Chip Transactions on Cards issued under a BIN assigned for **Ukraine** or **Switzerland**.

Mastercard Cards, excluding Debit Mastercard Cards

A Merchant located in the Europe Region may, at its option, support purchase with cash back Transactions on Mastercard Cards.

If supported, 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.

Intracountry Transactions

The following Rules apply to Intracountry Transactions under all brands in the country mentioned.

1. For Intracountry Transactions in **Poland**, an Issuer in Poland must not apply a cash back limit lower than PLN 1,000. An Acquirer in Poland that supports purchase with cash back must not apply a cash back limit lower than PLN 1,000. A Merchant in Poland that offers purchase with cash back must not apply a cash back limit lower than PLN 1,000.
2. 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. Intracountry Transactions in **Ukraine** must be processed in UAH only; POI currency conversion must not be offered.
4. In **Switzerland** the purchase amount, cash back amount, and Transaction amount must all be in the same currency. The cash back amount must not be 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.
5. An Issuer in **Armenia**, **Belarus**, **Georgia**, **Kazakhstan**, **Kyrgyzstan**, **Russia**, **Tajikistan**, **Turkmenistan**, **Ukraine**, and **Uzbekistan** must not apply a cash back limit lower than those specified in the above table of maximum cash back amounts.
6. Intracountry Transactions in **Moldova** must be processed in MDL only.

Issuer Requirements

The following requirements apply to Issuers:

1. An Issuer in the Europe Region 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 these Cards.
2. An Issuer must technically support purchase with cash back Transactions on **Mastercard** Cards issued under a BIN or BIN range assigned for the following countries.

Country	Requirement	Effective date
Russia	Technical support in host systems	In effect
Moldova, Ukraine	Technical support in host systems All Cards and MDES Tokens in circulation must have PWCB flag.	In effect
Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan	Technical support in host systems Newly issued and reissued Cards and MDES Tokens must have the PWCB flag.	In effect
	All Cards and MDES Tokens in circulation must have the PWCB flag.	1 December 2025
Italy	Technical support for PWCB Transactions on Prepaid Cards and Tokens in the Issuer's host system Newly issued and reissued Prepaid Cards and Tokens must have the PWCB flag.	In effect

Details of Technical Support Requirements for Issuers

In addition, an Issuer must technically support purchase with cash back Transactions, including in the Issuer authorization host system and with respect to purchase-amount-only approvals as set forth in global Rule 4.9, 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

Country	Mandate applies to Mastercard Cards issued or reissued on or after	With the exception of the following types of Cards
Russia, Ukraine	1 January 2020	No exceptions
Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan	1 January 2023	No exceptions
Moldova	1 April 2023	No exceptions

1. An Issuer that intends to support purchase with cash back Transactions for its Mastercard Cardholders must properly personalize the chip on its Mastercard Cards.
2. An Issuer that supports partial approval 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, UK and Gibraltar, 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.

4.10 Transactions at Unattended POS Terminals

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

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.

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.

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.

4.10.1 Automated Fuel Dispenser Transactions

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

Support for partial amount preauthorization 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.

For more information on Maestro petrol Transaction preauthorizations, refer to "Maestro Preauthorized Transaction Processing" in Chapter 7 of the *Authorization Manual* and "Maestro Pre-authorized Transactions" in Chapter 5 of the *Customer Interface Specification* manual.

In the EEA, UK and Gibraltar, 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 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). The Cardholder may express consent to the amount by continuing with the Transaction.

The preauthorization request amount, advice request amount, and partial approval support indicator must be provided in authorization messages, and the final Transaction amount must be provided in clearing messages, in the fields and with the values specified by the registered switch of the Customer's choice.

4.13 Merchant-approved Maestro POS Transactions

In the EEA, UK and Gibraltar, 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.

4.14 Mastercard Manual Cash Disbursement Transactions

4.14.2 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 are replaced by EUR 5,000 and EUR 1,000, respectively.

4.17 ATM Access Fees

4.17.1 ATM Access Fees - Domestic Transactions

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.

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:

- All countries and territories in the European Economic Area, excluding Poland
- United Kingdom
- Uzbekistan

Subject to complying with the ATM Access Fee notification requirements of the Rules, 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. For example, the amount of the ATM Access Fee must not be greater than that charged on other brands or networks (whether card scheme or other access device or app-based payment method). The ATM Access Fee may vary according to the Card or payment application (whether access device or app-based payment method) category (credit, debit, prepaid, commercial), on condition that corresponding cash withdrawal transactions on other brands and payment applications 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.

4.18 Merchandise Transactions at ATM Terminals

4.18.1 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 CVM limits apply in the Bolivarian Republic of Venezuela, Colombia, and Mexico.

4.9 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 using the highest priority CVM supported by both the Card and the POS Terminal.
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 **Colombia** and **Venezuela**, the Rule on this subject is modified as follows.

Colombia and Venezuela Issuers are not required to support the purchase with cash back Transaction type.

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 using the highest priority CVM supported by both the Card and the POS Terminal.
5. For Mastercard purchase with cash back Transactions, a maximum cash back amount of USD 60 or local currency equivalent applies.
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.

4.17 ATM Access Fees

4.17.1 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.

4.9 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 supports the signature CVM. Signature collection is optional.
- "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 CVM, indicating that a PIN CVM is preferred to the signature CVM 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.

4.5 Contactless Transit Transactions

4.5.1 Mastercard Contactless Transit Aggregated Transactions

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

A contactless transit aggregated Transaction occurs when one or more contactless taps performed with one Mastercard or Maestro Account at one U.S. Region transit Merchant during a 24-hour period (the "tap aggregation period") are combined into a total Transaction amount and subsequently submitted for authorization on a deferred basis. 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.

The following requirements apply.

Account Verification Required

Upon the first use of a Mastercard or Maestro Account at the transit Merchant on a given day (the "initial tap"), the Merchant starts the 24-hour aggregation period. The initial tap must be processed as follows:

- The Merchant sends an Account status inquiry (ASI) Authorization Request/0100 or Financial Transaction Request/0200 message, either deferred or in real-time. An ASI request contains a value of 8 (Account Status Inquiry Service [ASI]) in DE 61, subfield 7 (POS Transaction Status) and a Transaction amount of zero.

- If the Issuer approves or does not decline the ASI request, then the Merchant may proceed with tap aggregation as specified in this Rule.
- If the Issuer declines the ASI request, then the Merchant must not proceed with tap aggregation. The Merchant may submit a transit debt recovery Transaction for the amount of a single ride (if taken).

Aggregation Procedures

The following requirements apply for each tap aggregation period:

1. Following successful account verification as described above, the Merchant or its Acquirer maintains a record of each subsequent tap that occurs within the 24-hour aggregation period.
2. At the end of the aggregation period, the Merchant uses the last tap to initiate an Authorization Request/0100 or Financial Transaction Request/0200 message for the combined total amount of taps (rides taken) during the aggregation period. The total aggregated amount must not exceed the applicable contactless Transaction CVM limit amount (USD 100).
3. The Merchant must receive Issuer authorization for the Transaction. If the Issuer declines, the Merchant may submit a transit debt recovery Transaction. If the transit debt recovery Transaction is declined, the Merchant must not perform tap aggregation involving the Account until debt recovery on the Account is successfully completed and the Issuer approves a new Account verification request.
4. Upon the Cardholder's request, the Merchant must provide a list of the taps that were aggregated (the date, time [if available], and fare for each ride taken).

Multiple aggregation cycles may occur in the same 24-hour period, at the Merchant's discretion.

As described in the "Contactless Transactions" section of Appendix C, Transaction messages for the combined total amount of aggregated taps occurring in an aggregation period must contain:

- A value of 05 (Other) in DE 48, subelement 64, subfield 1 (Transit Transaction Type) of Authorization Request/0100 and Financial Transaction Request/ 0200 messages and in PDS 0210, subfield 1 (Transit Transaction Type) of First Presentment/1240 messages; and
- A value of 1 (Deferred authorization) in DE 61, subfield 7 of the Authorization Request/0100 or Financial Transaction Request/0200 message.

4.5.2 Maestro Contactless Transit Aggregated Transactions

In the U.S. Region, the Rule on this subject is replaced with U.S. Region Rule 4.5.1.

4.9 Purchase with Cash Back Transactions

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

A Merchant located in the United States that has received prior approval from its Acquirer may offer a Cardholder a cash back Transaction with or without an accompanying purchase when a

Debit Mastercard (including prepaid) Card is presented. A maximum cash back amount must be established in an amount that does not exceed USD 200 per Transaction.

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 54 (Amounts, Additional) of the First Presentment/1240 message.

d. Detailed in DE 28 (Amount, Transaction Fee) of the Authorization Request/0100 message or Financial Transaction Request/0200.

e. Included in the total Transaction amount transmitted in DE 4 (Amount, Transaction) of authorization and clearing messages.

4.10 Transactions at Unattended POS Terminals

4.10.1 Automated Fuel Dispenser Transactions

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

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, section 5.11.4, "Additional Cardholder Identification" of the *Mastercard Rules* .

4.11 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).

4.12 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 100; and
- The Transaction is a magnetic stripe Transaction, Contact Chip Transaction, or Contactless Transaction; and

- The Transaction type cannot be performed at an unattended POS Terminal; and
- DE 18 (Merchant Type) does not contain any of the following Merchant category code (MCC) values:
  - MCC 4829 (Money Transfer)
  - MCC 6010 (Manual Cash Disbursements: Customer Financial Institution)
  - MCC 6011 (Automated Cash Disbursements: Customer Financial Institution)
  - MCC 6050 (Quasi Cash: Customer Financial Institution)
  - MCC 6051 (Quasi Cash: Merchant)
  - MCC 6538 (Funding Transactions for MoneySend)
  - MCC 6540 (Funding Transactions)
  - MCC 7800 (Government Owned Lottery [U.S. Region Only])
  - MCC 7801 (Internet Gambling [U.S. Region Only])
  - MCC 7802 (Government Licensed Horse/Dog Racing [U.S. Region Only])
  - MCC 7995 (Gambling Transactions)
  - MCC 9405 (Intra-Government Purchases: Government Only)

If all of the conditions are met, a Corporation-assigned indicator will be populated in DE 48, subelement 81 of the Financial Transaction Request/0200 message, indicating that the Transaction qualifies for processing as a PIN-less Single Message Transaction.

For Transactions qualifying as PIN-less Single Message Transactions:

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.
4. An Issuer may not charge back a PIN-less Single Message Transaction for reason of fraud.

4.14 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.

4.14.2 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.

4.14.3 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.

4.17 ATM Access Fees

4.17.1 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.

4.18 Merchandise Transactions at ATM Terminals

4.18.1 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.

4.19 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.

4.19.1 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.

4.19.2 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.

4.19.3 Maximum Shared Deposit Amount

The maximum Shared Deposit Transaction amount must be limited to USD 99,999.99.

4.19.4 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.

4.19.5 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.

4.19.6 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.

4.19.7 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.

4.19.8 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 179
5.1.1 Acquirer and Merchant Requirements 179
5.1.2 Issuer Requirements 181
5.1.3 Use of Static AAV for Card-not-present Transactions 182
5.1.4 Debit Small-Ticket Digital Transaction Program: Brazil Only 182
5.2 Mail Order and Telephone Order (MO/TO) Transactions 182
5.3 Credential-on-File Transactions 183
5.4 Recurring Payment Transactions 184
5.4.1 Subscription Billing Merchants 186
5.4.1.1 Applicability of Standards 188
5.4.2 Negative Option Billing Merchants 188
5.4.3 China Domestic Recurring Payment Transactions 190
5.5 Installment Billing 190
5.5.1 Single-Authorization Installment Billing 191
5.5.1.1 Definitions 191
5.5.1.2 Transaction Processing Procedures 191
5.5.2 Multiple-Authorization Installment Billing 192
5.6 Transit Transactions Performed for Debt Recovery 194
5.6.1 Transit First Ride Risk Framework 195
5.7 Use of Automatic Billing Updater 198
5.8 Authentication Requirements—Europe Region Only 199
5.9 Merchant-initiated Transactions 199
5.10 Mastercard Micropayment Solution—United States Region Only 200
Variations and Additions by Region 200
Asia/Pacific Region 200
5.1 Electronic Commerce Transactions 200
5.1.1 Acquirer and Merchant Requirements 201
5.1.2 Issuer Requirements 201
5.2 Mail Order and Telephone Order (MO/TO) Transactions 202
5.3 Credential-on-File Transactions 203
5.4 Credential-on-File Transactions 203

5.4.2 China Domestic Recurring Payment Transactions ... 203
5.4.2.1 Transaction Requirements for Acquirers ... 204
5.4.2.2 Transaction Requirement for Issuers ... 206
5.5 Installment Billing ... 206
5.5.1 Single-Authorization Installment Billing ... 206
5.5.1.2 Transaction Processing Procedures ... 206
5.6 Transit Transactions Performed for Debt Recovery ... 206
5.6.1 Transit First Ride Risk Framework ... 207
5.7 Use of Automatic Billing Updater ... 208
5.9 Merchant-initiated Transactions ... 208
Canada Region ... 208
5.7 Use of Automatic Billing Updater ... 208
Europe Region ... 208
5.1 Electronic Commerce Transactions ... 208
5.1.1 Acquirer and Merchant Requirements ... 208
5.1.2 Issuer Requirements ... 210
5.1.3 Use of Static AAV for Card-not-present Transactions ... 211
5.2 Mail Order and Telephone Order (MO/TO) Maestro Transactions ... 211
5.2.1 Definitions ... 211
5.2.2 Intracountry Maestro MO/TO Transactions—Cardholder Authority ... 212
5.2.3 Intracountry Maestro MO/TO Transactions—Transactions Per Cardholder Authority ... 212
5.2.4 Intracountry Maestro MO/TO Transactions—CVC 2/AVS Checks ... 212
5.3 Credential-on-File Transactions ... 213
5.4 Recurring Payment Transactions ... 213
5.5 Installment Billing ... 215
5.5.1 Single-Authorization Installment Billing ... 215
5.5.1.2 Transaction Processing Procedures ... 215
5.5.2 Multiple-Authorization Installment Billing ... 215
5.6 Transit Transactions Performed for Debt Recovery ... 215
5.7 Use of Automatic Billing Updater ... 216
5.7.1 Issuer Requirements ... 216
5.7.2 Acquirer Requirements ... 217
5.8 Authentication Requirements ... 218
5.8.1 Acquirer Requirements ... 218
5.8.2 Issuer Requirements ... 219
5.9 Merchant-initiated Transactions ... 219
Latin America and the Caribbean Region ... 221
5.1 Electronic Commerce Transactions ... 221
5.1.1 Acquirer and Merchant Requirements ... 221

5.1.2 Issuer Requirements....221
5.1.4 Debit Small-Ticket Digital Transaction Program: Brazil Only....221
5.7 Use of Automatic Billing Updater....223
Middle East/Africa Region....223
5.1 Electronic Commerce Transactions....223
5.1.1 Acquirer and Merchant Requirements....223
5.1.2 Issuer Requirements....224
5.7 Use of Automatic Billing Updater....224
United States Region....224
5.7 Use of Automatic Billing Updater....224
5.10 Mastercard Micropayment Solution....224
Additional U.S. Region and U.S. Territory Rules....225
5.1 Electronic Commerce Transactions....225
5.1.1 Acquirer and Merchant Requirements....225
5.1.2 Issuer Requirements....226

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, contactless payment or Mastercard Consumer-Presented QR payment functionality, or as a purchase with cash back Transaction.

NOTE: Additions to this Rule appear in the "Asia/Pacific Region" and "Europe Region," and "Middle East/Africa Region" sections at the end of this chapter.

5.1.1 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 and each 3-D Secure Service Provider (as defined in Chapter 7 of the *Mastercard Rules*) transacting under the Mastercard® Identity Check program, the Acquirer must ensure the Merchant is assigned a Merchant ID and uses the Mastercard Directory Server to complete the authentication if the Transaction is submitted for authorization and clearing (unless such Transaction is submitted via an alternate switch due to regulatory reasons), and ensure that the Merchant correctly populates all UCAF fields with required data elements and complies with the Mastercard Identity Check Standards. Refer to the *Mastercard Identity Check Program* for more information.
5. The Transaction amount used in the authorization message for a CIT must match the value of the products and services in the Cardholder's purchase order, 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. Each subsequent authorization request initiated by the Merchant after the initial CIT must be identified with

the MIT value of M205 (Partial Shipment) in DE 48, subelement 22 (Multi-purpose Merchant Indicator), subfield 5 (Cardholder/Merchant Initiated Transaction Indicator).

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 or digital product or a sample of the physical or digital product provided to a Cardholder by a 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 negative option billing Merchant.
11. If the Merchant is a 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 or digital 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 MMYY 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 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," "Middle East/Africa Region," and the "Additional U.S. Region and U.S. Territory Rules" sections at the end of this chapter.

5.1.2 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 Identity Check.

An Issuer that uses Mastercard Identity Check to verify its Cardholders must:

- Use the Mastercard Secure Payment Application (SPA) algorithm to generate the Accountholder Authentication Value (AAV); and
- Verify the validity of the AAV when present in DE 48, subelement 43 of the authorization request message, or participate in the Mastercard Identity Check AAV Verification Service.

Mastercard 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 MMYY 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 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," "Middle East/Africa Region," and the "Additional U.S. Region and U.S. Territory Rules" sections at the end of this chapter.

5.1.3 Use of Static AAV for Card-not-present Transactions

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

5.1.4 Debit Small-Ticket Digital Transaction Program: Brazil Only

NOTE: A Rule on this subject appears in the "Latin America and the Caribbean 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, India, and the United States Region and U.S. Territories 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 or Identity Check 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).

A Transaction must contain the Credential-on-file indicator (in addition to a CIT or MIT indicator, as applicable) when:

- the Cardholder previously authorized the Merchant to store the Account data for use in future Transactions, and
- the Cardholder agreed to the Merchant's use of the stored Account data to conduct the Transaction being submitted.

Refer to Rule 5.9 for more information about Merchant-initiated Transactions (MITs) and to Appendix C regarding the use of CIT and MIT indicators.

The Acquirer should:

- ensure that the Merchant retains the Cardholder's written agreement to the terms of a Credential-on-file Transaction arrangement; and
- advise the Merchant not to place Account data on file as a Stored Credential if the Issuer provides a Merchant advice code value of 40 (Consumer non-reloadable prepaid card) or 41 (Consumer single use virtual card number) in an authorization response (0110 or 0210) message.

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 Cardholder-initiated 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: • 0 (Attended Terminal) • 1 (Unattended Terminal [Cardholder-activated Terminal {CAT}, home PC, mobile phone, personal digital assistant {PDA}]) • 2 (No Terminal used [voice/audio response unit {ARU} authorization; server])

Data Element	Subfield	Value
61 (Point-of-Service [POS] Data)	4 (POS Cardholder Presence)	One of the following: • 0 (Cardholder present) • 1 (Cardholder not present, unspecified) • 2 (Mail/facsimile order) • 3 (Phone/ARU order) • 5 (Electronic order [home PC, Internet, mobile phone, PDA]) The value of 4 must be used when the first payment in a recurring payment series occurs in a Card-not-present environment.
61 (Point-of-Service [POS] Data)	5 (POS Card Presence)	One of the following: • 0 (Card present) • 1 (Card not present)
48 (Additional Data - Private Use), subelement 22 (Multi-Purpose Merchant Indicator)	5 (Cardholder/Merchant Initiated Transaction Indicator)	One of the following: • C101 (Credential-on-file [ad hoc]) • C102 (Standing Order [variable amount/fixed frequency]) • C103 (Subscription [fixed amount/ fixed frequency])

An Acquirer must identify each subsequent Merchant-initiated recurring payment Transaction with the following values, including when a Stored Credential has been replaced with a Token at the Merchant's request.

Data Element	Subfield	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	• 10 (Credential on File)
61 (Point-of-Service [POS] Data)	1 (POS Terminal Attendance)	One of the following: • 1 (Unattended Terminal [Cardholder-activated Terminal {CAT}, home PC, mobile phone, personal digital assistant {PDA}]) • 2 (No Terminal used [voice/audio response unit {ARU} authorization; server])
61 (Point-of-Service [POS] Data)	4 (POS Cardholder Presence)	4 (Standing order/recurring Transactions)

Data Element	Subfield	Value
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)
48 (Additional Data - Private Use), subelement 22 (Multi-Purpose Merchant Indicator)	5 (Cardholder/Merchant Initiated Transaction Indicator)	One of the following: • M101 (Unscheduled Credential-on-file) • M102 (Standing Order [variable amount/fixed frequency]) • M103 (Subscription [fixed amount/ fixed frequency])

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.

Effective 17 April 2026, an Acquirer is recommended to populate DE 105 (Multi-Use Transaction Identification Data), subelement 002 (Economically Related Transaction Link Identifier) of each subsequent Merchant-initiated recurring payment Transaction with the DE 105, subelement 001 (TLID) value from the original Cardholder-initiated Transaction.

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

5.4.1 Subscription Billing Merchants

The following Standards apply to recurring payment Transactions initiated by a Merchant performing subscription billing in which the Cardholder has agreed for the Merchant to provide ongoing and/or periodic delivery of a service, membership, physical products or Digital Goods. Refer to Rule 5.4.1.1 regarding the applicability of these Standards to certain Merchant categories.

1. The Merchant must disclose the subscription terms simultaneously with a request for Card credentials. The disclosure must include the price that will be billed and the frequency of the

billing (for example, "You will be billed USD 9.95 per month until you cancel the subscription). Merchants that utilize a negative option billing model must also disclose the terms of the trial, including any initial charges, the length of the trial period, and the price and frequency of the subsequent subscription (for example, You will be billed USD 2.99 today for a 30-day trial. Once the trial ends, you will be billed USD 19.99 each month thereafter until you cancel.").
An e-commerce Merchant must:

a. Clearly and prominently display the subscription terms on any payment and order summary webpages; and
b. Capture a Cardholder's affirmative acceptance of the subscription terms before completing the subscription order.

Providing a link to another webpage or requiring the Cardholder to expand a message box or scroll down the webpage to view the subscription terms does not satisfy this requirement.

2. Immediately after the Cardholder completes the subscription order, the Merchant must promptly send a subscription order confirmation to the Cardholder through an email message or other electronic communication method that includes the subscription terms. The confirmation message must include or provide access to instructions for account management capabilities, including instructions for canceling the subscription (and thereby withdrawing permission for any subsequent recurring payment).
3. Each time that the Merchant receives an approved authorization request, it is recommended that the Merchant provide the Cardholder with a Transaction receipt through an e-mail message or other electronic communication method that includes the amount and reason for the billing and includes or provides access to instructions for account management capabilities, including instructions for canceling the subscription (and thereby withdrawing permission for any subsequent recurring payment Transactions). Cardholders may choose to opt-out of receiving these notices.
This Standard becomes a requirement when a Merchant that utilizes a recurring payment plan is identified for four months or more in the Acquirer Chargeback Monitoring Program (ACMP) as an Excessive Chargeback Merchant (ECM), a High Excessive Chargeback Merchant (HECM) and/or an Excessive Fraud Merchant (EFM) within the same audit period (refer to Chapter 8 Acquirer Chargeback Monitoring Program of the Data Integrity Monitoring Program for more information). The Acquirer of a Merchant that has been identified in ACMP for four months or more and has not implemented these requirements may be subject to Category A assessments for each month of noncompliance, in addition to the assessments applicable under the Acquirer Chargeback Monitoring Program.
4. The Merchant must provide an online or electronic cancellation method (similar to unsubscribing from email messages or any other electronic method) or clear instructions on how to cancel that are easily accessible online (such as a "Manage Subscription" or "Cancel Subscription" link on the merchant's home page).
5. For any subscription where the billing frequency is every six months (180 days) or less (i.e., billing occurs every six months, every year, every other year, etc.), the Merchant must send an electronic reminder to the Cardholder at least seven days but no more than 30 days prior to the next billing date that includes the subscription terms and includes or provides access to instructions for account management capabilities, including instructions for canceling the

subscription (and thereby withdrawing permission for any subsequent recurring payment). The communication must clearly reference in the subject line that it relates to upcoming charges to the Cardholder (for example, "Important Information About Upcoming Charges to Your Account") and the message must be distinct from marketing communications that are otherwise sent to the Cardholder.

5.4.1.1 Applicability of Standards

The Standards in this Rule 5.4.1 do not apply to payments for utilities (i.e., gas, electric, sanitation, heating oil, water), telecommunications, insurance policies, or existing debt (for example, vehicle loan or mortgage payments).

The Standards in this Rule 5.4.1 are only best practice recommendations for any not-for-profit/charity Merchant that utilizes a recurring payment plan. However, all five Standards (including, for the avoidance of doubt, item three) become requirements when a not-for-profit/charity Merchant that utilizes a recurring payment plan is identified for four months or more in the Acquirer Chargeback Monitoring Program (ACMP) as an Excessive Chargeback Merchant (ECM), a High Excessive Chargeback Merchant (HECM) and/or an Excessive Fraud Merchant (EFM) within the same audit period (refer to Chapter 8 Acquirer Chargeback Monitoring Program of the Data Integrity Monitoring Program for more information). The Acquirer of a Merchant that has been identified in ACMP for four months or more and has not implemented these requirements may be subject to Category A assessments for each month of noncompliance, in addition to the assessments applicable under the Acquirer Chargeback Monitoring Program.

5.4.2 Negative Option Billing Merchants

A negative option billing Merchant offers a Cardholder the opportunity to purchase a subscription service to automatically receive one or more physical products (such as cosmetics, health-care products, or vitamins), Digital Goods or services on a recurring basis (such as weekly, monthly, semi-annually, or annually). As used in this section, the term "product" means or a physical product or a Digital Good.

The subscription service may be initiated by an agreement between the Cardholder and the Merchant whereby the Cardholder agrees to receive from the Merchant a sample of the product or services (either complimentary or at a nominal price) for a trial period. The sample may be larger, equal to, or smaller than the product provided by the Merchant during the subscription period. For the purposes of this Rule 5.4.2, a trial period means a preset length of time during which the Cardholder may evaluate the characteristics of the product or service such as its quality or usefulness to determine whether the Cardholder wants to either:

- Purchase the product or service on a one-time basis or recurring basis; or
- Return the product (if possible) to the Merchant.

After the trial period has expired, the Merchant may use Account credentials provided to the Merchant by the Cardholder to submit Transactions on a recurring basis each time that the product is shipped, delivered, or otherwise made available to the Cardholder, until either:

- The Cardholder takes action to terminate the agreement with the Merchant (for example, notifying the Merchant to cancel the subscription);
- The Merchant terminates the agreement; or
- The subscription expires.

The following Standards apply to recurring payment Transactions associated with a negative option billing Merchant:

1. For Digital Goods and services offering a trial period longer than seven days: No less than three days and no more than seven days prior to end of trial period, the Merchant must send a reminder notification to the Cardholder that the subscription plan will commence if the Cardholder does not cancel, or whenever terms and conditions will change. This notification must include the basic terms of the subscription and clear instructions on how to cancel. This reminder can be completed by email or any other electronic methods.
2. For physical products:
   a. 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 Transaction.
   b. After the trial period has expired, the 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 for the full-size or regular price product:
      – The date the subscription period begins
      – 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
3. Each time that the Merchant receives an approved authorization request, the Merchant must provide the Cardholder with a Transaction receipt 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 Transaction receipt after a declined authorization request, the Transaction receipt 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 at least seven (7) days in advance when any of the following events occur:

- The Merchant is revising the subscription billing terms
- The recurring payment Transaction cycle has been terminated by either the Merchant or the Cardholder, in which case the notice must be sent no more than seven days after the Cardholder's decision to cancel.

For more information about registration requirements for negative option billing Merchants selling physical goods, refer to Section 9.4.10 of the *Security Rules and Procedures* .

5.4.3 China Domestic Recurring Payment Transactions

NOTE: A Rule on this subject appears in the "Asia/Pacific Region" section at the end of this chapter.

5.5 Installment Billing

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 or other retailer is paid. The amount of each payment is a fixed amount determined by the total number of installments specified and the value 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.

Applicability of Rules

The Standards in Rule 5.5.1 and in message reason code 4850 (Participating Countries-Installment Billing Dispute) in the *Chargeback Guide* apply to an Acquirer-financed and Merchant-financed installment billing where the Acquirer processes a single 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 Issuer approval of the authorization request containing installment information, 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.

Mastercard supports single-authorization installment billing in participating countries only.

The Standards in Rule 5.5.2 apply when a Merchant or Installment Provider offers installment billing to Cardholders, and each installment payment Transaction is submitted individually for authorization by the Issuer, in accordance with the terms agreed by the Cardholder at the POI. Upon Issuer approval, the Acquirer submits a separate clearing record for each installment payment.

For more information about Installment Providers, refer to Chapter 7 of the *Mastercard Rules*.

5.5.1 Single-Authorization Installment Billing

This section applies to installment billing Transactions whereby information about the installment plan agreed between the Merchant and the Cardholder is transmitted in the Merchant's authorization request message for Issuer approval.

5.5.1.1 Definitions

Solely for the purposes of the installment billing Rules set forth herein and in "Installment Billing Dispute-Participating Countries (Reason Code 4850)" in the "Domestic Chargebacks" appendix 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.

5.5.1.2 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/0110 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: Modifications to this Rule appear in the "Asia/Pacific Region" and "Europe Region" sections at the end of this chapter.

5.5.2 Multiple-Authorization Installment Billing

This section describes Transaction processing procedures for Merchants and Installment Providers offering installment billing arrangements to Cardholders in connection with a retail purchase, in which each installment payment is processed as an individually authorized and cleared Transaction. The following requirements apply:

- The installment billing arrangement terms and conditions must be fully and clearly disclosed in advance to the Cardholder. This includes but is not limited to the total number of installment payments, the payment schedule, the amount of each payment, and any fees that may apply;
- The installment billing arrangement must be conducted in accordance with the terms and conditions offered to and agreed by the Cardholder;

- The Acquirer must properly identify each installment payment Transaction as described in the "Installment Payment Information" section; and
- The Transaction receipt for each installment Transaction must include the installment number as it corresponds to the total number of installments (for example, "Payment 2 of 4").

Installment Payment Information

An installment payment Transaction is properly identified as described in the following table.

Table 9: Authorization Request/0100 and Financial Transaction Request/0200 Messages

In This Data Field:	If submitted by a Merchant, each Transaction must contain:	If submitted by an Installment Provider, each Transaction must contain:
DE 43 (Acceptor Name and Address)	The Merchant's name and address	The full or abbreviated name of the Installment Provider in combination with the retailer name, separated by an asterisk (for example, Installment Provider*Retailer)
DE 18 (Merchant Type)	The MCC that best describes the primary business of the Merchant, or the nature of the purchase	The MCC that best describes the primary business of the retailer, or the nature of the purchase
DE 48, subelement 32 (Mastercard-assigned ID)	Optional; if present, the Mastercard-assigned ID of the Merchant	The Mastercard-assigned ID of the Installment Provider
DE 48, subelement 77 (Transaction Type Identifier)	Not Required	P10 (Purchase Repayment)
DE 48, subelement 22 (Multi-Purpose Merchant Indicator), subfield 5 (Cardholder/Merchant Initiated Transaction Indicator)	C104 for the initial CIT and M104 for each subsequent MIT	C104 for the initial CIT and M104 for each subsequent MIT

The following First Presentment/1240 message fields must be populated with the same information as provided in the corresponding Authorization Request/0100 message field:

- DE 43 (Acceptor Name/Location)
- DE 26 (Acceptor Business Code [MCC])
- PDS 0176 (Mastercard-assigned ID)
- PDS 0043 (Transaction Type Identifier)

The Credential-on-file Transaction indicator must be present in authorization and clearing messages as described in Rule 5.3 for each installment payment Transaction subsequent to the

initial payment. The value of C104 or M104, as appropriate, may also be provided in PDS 0218 (Cardholder/Merchant Initiated Transaction Indicator).

If space allows, a message describing the installment being paid may optionally be provided in authorization and clearing messages at the end of DE 43, subfield 1 (Card Acceptor Name); for example, "PYMT 2 of 4".

Effective 17 April 2026, an Acquirer is recommended to populate DE 105 (Multi-Use Transaction Identification Data), subelement 002 (Economically Related Transaction Link Identifier) of each subsequent installment payment Transaction with the DE 105, subelement 001 (TLID) value from the initial installment payment Transaction.

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

Customer Service Information

The Acquirer is recommended to provide the following information in PDS 0170 (Card Acceptor Inquiry Information) of each First Presentment/1240 message:

- A customer service phone number for the retailer in subfield 1 (Customer Service Phone Number);
- A customer service phone number for the Installment Provider in subfield 2 (Card Acceptor Phone Number); and
- The installment number and total number of installments in subfield 3 (Additional Contact Information) (for example, "PAYMENT 2 of 4").

5.6 Transit Transactions Performed for Debt Recovery

A transit Merchant may use the transit debt recovery Transaction to recover a Cardholder's debt resulting from one or more contactless taps for entry to the transit system, if the Issuer has declined the Contactless transit aggregated Transaction authorization request (0100 or 0200) message. A transit debt recovery Transaction is an MIT that is properly identified with:

- A value of 07 (Debt Recovery) in DE 48, subelement 64 (Transit Program), subfield 1 (Transit Transaction Type Indicator) in Authorization Request/0100 and Financial Transaction Request/0200 messages and in PDS 0210 (Transit Program), subfield 1 (Transit Transaction Type Indicator) of First Presentment/1240 messages; and
- An amount in DE 4 (Amount, Transaction) that does not exceed the applicable Mastercard Contactless transit aggregated Transaction CVM limit.

A transit debt recovery Transaction may also contain the MIT value of M208 (Resubmission) in DE 48, subelement 22 (Multi-purpose Merchant Indicator), subfield 5 (Cardholder/Merchant Initiated Transaction Indicator) of Authorization Request/0100 and Financial Transaction Request/0200 messages.

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).

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

5.6.1 Transit First Ride Risk Framework

A transit Merchant that initiates the authorization of Contactless transit aggregated Transactions submitted via the Mastercard Dual Message System and is located in a country implementing the First Ride Risk (FRR) framework may qualify to collect payment for first ride debt incurred by the Cardholder. First ride debt is the amount owed by the Cardholder to the transit Merchant for one or more rides taken upon using a Contactless tap to enter the transit system (such as at a gate or turnstile), if the Issuer declines the Contactless transit aggregated Transaction authorization request. The FRR framework applies solely with respect to the use of a Card or Access Device issued in the Merchant's country, unless otherwise specified.

Under the FRR framework, a Merchant that meets all the FRR framework criteria can collect payment for first ride debt in an amount not exceeding the FRR limit applicable in the Merchant's country, as follows.

Submit this Transaction type:	Under these conditions:
A transit debt recovery Transaction	The Issuer declined the Contactless transit aggregated Transaction using a response code value categorized in Table 7 as "Recoverable" or "Temporarily Recoverable." The transit debt recovery Transaction amount must not exceed the applicable Contactless transit aggregated Transaction CVM limit.
A Transit FRR claim Transaction	1. The Issuer declined the Contactless transit aggregated Transaction or a subsequent transit debt recovery Transaction using a response code value categorized in Table 7 as "Unrecoverable." In such event, the FRR claim Transaction can be submitted immediately; or 2. The Merchant made at least nine transit debt recovery Transaction attempts for a period of 45 calendar days from the date of the original Contactless Transit aggregated Transaction decline, with the last attempt occurring on day 45, and the Issuer declined each attempt for a "Recoverable" or "Temporarily Recoverable" reason. The Merchant must make no more than one attempt per 24-hour period.

An FRR claim Transaction does not require authorization by the Issuer. The FRR claim Transaction is properly identified in the First Presentment/1240 message with:

- A value of 08 (First Ride Risk Claim) in PDS 0210 (Transit Program), subfield 1 (Transit Transaction Type Indicator) for Post Authorized Aggregation (PAA), Authorized Aggregated Split Clearing (AASC) or PAA-Maestro transit model only; and
- An amount in DE 4 (Amount, Transaction) that does not exceed the FRR limit applicable in the Merchant's country, as specified in Chapter 5 of the *Quick Reference Booklet*.

The Acquirer must not submit an FRR claim Transaction if the Issuer used a response code value categorized in this table as "Not Claimable" when declining the original Contactless transit aggregated Transaction or a subsequent transit debt recovery Transaction.

Table 10: Authorization Request Response/0110 Message DE 39 (Response Code) Decline Value Categories

Recoverable	Unrecoverable	Temporarily Recoverable	Not Claimable
51 (Insufficient funds/ over credit limit)	03 (Invalid merchant)	01 (Refer to card issuer)	15 (Invalid issuer)
55 (Invalid PIN)	04 (Capture card)	05 (Do not honor)[5]	30 (Format error)
61 (Exceeds withdrawal amount limit)	12 (Invalid transaction)	70 (Contact card issuer)	54 (Expired card)
65 (Exceeds withdrawal count limit)	13 (Invalid amount)	86 (PIN validation not possible)	57 (Transaction not permitted to issuer/ cardholder)
71 (PIN not changed)	14 (Invalid card number)	87 (Purchase amount only; no cash back allowed)	92 (Unable to route transaction)
75 (Allowable number of PIN tries exceeded)	41 (Lost card)	91 (Authorization system or issuer system inoperative)	94 (Duplicate transmission detected)
76 (Invalid/nonexistent "To Account" specified)	43 (Stolen card)		96 (System error)
77 (Invalid/nonexistent "From Account" specified)	58 (Transaction not permitted to acquirer/ terminal)		

[5] Unrecoverable if DE 48, subelement 84 (Merchant Advice Code) contains a value of 03 (Do not try again).

Recoverable	Unrecoverable	Temporarily Recoverable	Not Claimable
78 (Invalid/Nonexistent account specified)	62 (Restricted card) 63 (Security violation) 79 (Life cycle [Mastercard use only]) 82 (Policy [Mastercard use only]) 83 (Fraud/Security [Mastercard use only]) 88 (Cryptographic failure)		

The terms used in the headings of the preceding table are defined here.

Recoverable

For response codes that are recoverable, the transit acquirer must use the debt recovery Authorization Request/0100 message to attempt debt recovery from the issuer or cardholder.

Unrecoverable

Authorization requests receiving response codes that are deemed unrecoverable will be eligible for unrecoverable debt claims by the merchant's acquirer to the issuer. The claim is submitted as a First Presentment/1240 clearing message without a valid authorization approval.

The transit acquirer submitting a first presentment to make an FRR claim due to reason code 14 (Invalid card number) may be rejected with an error code 2358 (DE2 PRIMARY ACCOUNT NUMBER [PAN] INVALID. THE PAN MAPPING SERVICE CANNOT MAP DE2 TO ANOTHER ACCOUNT NUMBER) from the Global Clearing Message System (GCMS) if the authorization request was initiated from a digitized card associated with a closed account. The transit acquirer may submit a Fee Collection/1740 message to claim the debt for reason code 14 (invalid card number) after the first presentment was rejected with error code 2358 when making an FRR claim.

Temporarily Recoverable

Upon receiving a response code that indicates a temporary situation that the cardholder may potentially be able to resolve by working with the issuer, the transit merchant must make at least nine attempts at debt recovery from the cardholder within 45 calendar days from the date on which the temporarily recoverable decline response code was initially received, until the last attempt occurring no later than day 45.

When all debt recovery attempts are exhausted, the debt becomes unrecoverable, and the transit merchant may submit an FRR claim directly to

the issuer. The claim is submitted as a First Presentment/1240 clearing message without a valid authorization approval.

Not Claimable

Transit merchants must deny access to expired cards and cards that do not support deferred authorization (bit 8 of byte 3 set to 1b) in the transit product data (an extension of third-party data defined in the *M/Chip Requirements for Contact and Contactless* announced in December 2020) at the point of entry, and will be fully liable for declines due to reason codes 54 (Expired card) and 57 (Transaction not permitted to issuer/cardholder).

Merchants cannot claim the debt using the FRR framework or submit a debt recovery authorization upon receiving an expired card decline or card that does not support deferred authorization.

Transit merchants also cannot claim the outstanding debt for response codes that indicate formatting or network issues.

NOTE: Modifications to this Rule appear in the "Asia/Pacific" 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 in the Technical Resource Center on 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 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

A Merchant-initiated Transaction (MIT) is a Card-not-present Transaction that a Merchant initiates based on a prior agreement with the Cardholder, and in which the Cardholder does not actively participate. An MIT is often preceded by an Account Status Inquiry authorization request or CIT.

MITs are classified as follows.

Recurring payment and installment MITs are Credential-on-file Transactions initiated by a Merchant or Installment Provider based on the Cardholder's agreement to be billed on a scheduled or unscheduled basis for goods or services purchased from the Merchant, or for a single purchase to be paid in several installments.

Industry Practice MITs are initiated by the Merchant based on the Cardholder's agreement to the terms and conditions of a single purchase of goods or services. Industry practice MITs may be performed with credentials that the Merchant does not store permanently on file, but only temporarily retains for purposes of completing the purchase. An industry practice MIT may be one of the following:

- "Partial shipment" occurs when items that were out of stock when originally ordered in a CIT are later shipped and billed separately by the Merchant as an MIT.
- "Related/delayed charge" occurs when the Merchant submits an MIT to bill the Cardholder for additional items or fees associated with an initial CIT, in accordance with the original Transaction terms.
- "No-show" is a fee billed by a Merchant in accordance with the Merchant's guaranteed reservation service policy, when the Cardholder fails to cancel a reservation within the time frame disclosed at the time of the booking.
- "Resubmission" occurs when the original CIT authorization request was declined by the Issuer for a reason that does not preclude the Merchant from resubmitting the request after a reasonable period (for example, in 24 hours).

An Acquirer must properly identify in Authorization Request/0100 and Financial Transaction Request/0200 messages:

- All Merchant-initiated Transactions (MITs); and
- Any Cardholder-initiated Transaction (CIT) that occurs in an e-commerce environment and is used to place a credential on file for future MITs.

Refer to Appendix C for MIT and CIT identification requirements.

NOTE: Additions to this Rule appear in the "Europe Region" section and modifications to this Rule appear in the "Asia/Pacific Region" section at the end of this chapter.

5.10 Mastercard Micropayment Solution—United States Region Only

A Rule on this subject appears 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.

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 Identity Check.

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 Identity Check. Cardholders must complete enrollment on the first attempt, and the Issuer must not permit a Cardholder to opt-out of the 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.

A refund for a Maestro Intracountry e-commerce Transaction must be processed as a Payment Transaction.

5.1.1 Acquirer and Merchant Requirements

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.

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.

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

An Acquirer must ensure that each of its Merchants:

- Prominently and clearly discloses to the Cardholder the Merchant's participation in least cost routing prior to the request to capture or for authorization to store the Cardholder's Debit Mastercard Account data. To maintain visual parity, such disclosure must be a least as prominent as, and appear in at least the same size as surrounding content.
- Present Mastercard as a payment option to the Cardholder in accordance with the Standards, irrespective of whether the Transaction is routed or processed through the Interchange System.

5.1.2 Issuer Requirements

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 Identity Check 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.

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 Identity Check must contain a value of 2 (Identity Check 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.
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 (Identity Check 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 Identity Check; 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 Identity Check. Cardholders must complete enrollment on the first attempt, and the Issuer must not permit a Cardholder to opt-out of the 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).

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

An Acquirer must ensure that each of its Merchants:

- Prominently and clearly discloses to the Cardholder the Merchant's participation in least cost routing prior to the request to capture or for authorization to store the Cardholder's Debit Mastercard Account data. To maintain visual parity, such disclosure must be a least as prominent as, and appear in at least the same size as surrounding content.
- Present Mastercard as a payment option to the Cardholder in accordance with the Standards, irrespective of whether the Transaction is routed or processed through the Interchange System.
- Must give at least 7 days notice to the Cardholder to exercise consumer choice in the event that the recurring transaction routing option is different from the Cardholder's last confirmation of checkout choice.

An Acquirer must ensure, within 30 days of when a Merchant begins participating in least cost routing, subsequent to the time of the Merchant's initial request for authorization to store the Cardholder's Debit Mastercard Account data, that the Merchant prominently and clearly discloses to the Cardholder the Merchant's participation in least cost routing as set forth above.

5.4 Credential-on-File Transactions

5.4.2 China Domestic Recurring Payment Transactions

Each Acquirer of China domestic Transactions must comply with all requirements set forth in the Standards applicable to recurring payment Transactions, including the requirements in this manual, in the *China Switch Specifications* for authorization messages, and in the *China Recurring Transaction Program Guide*.

5.4.2.1 Transaction Requirements for Acquirers

Adding a New Recurring Payment Series

The Acquirer must secure approval from Issuer for the recurring payment series prior to the initial recurring payment Transaction via the entrusted relation related messages as described in *China Switch Specifications*.

The Acquirer must include the China Recurring Payment Transaction – Recurring Payment Terms via Data Element 112 (Additional Data [China Use]) Subelement 37 (Delegated Business Information) when requesting to add a new recurring payment series.

The Acquirer may only put a credential on file for recurring payment Transactions if the Issuer approves the request to add a new recurring payment series. The Acquirer must not submit the recurring payment Transaction if the Issuer declines the request to add a new recurring payment series.

The Acquirer must identify each request to add a new recurring payment series with the following values:

Data Elements	Subelement	Value
4 (Amount, Transaction)		0
25 (Point of Service Condition Code)		98 (Entrusted Relation Establishment)
61 (Point-of-Service [POS] Data)	1 (POS Terminal Attendance)	One of the following: • 0 (Attended Terminal) • 1 (Unattended Terminal (Cardholder-activated Terminal [CAT], home PC, mobile phone, personal digital assistant [PDA])) • 2 (No Terminal used (voice/ audio response unit [ARU] authorization); server])
61 (Point-of-Service [POS] Data)	4 (POS Cardholder Presence)	One of the following: • 0 (Cardholder present) • 5 (Cardholder not present (Electronic order [home PC, Internet, mobile phone, PDA]))
61 (Point-of-Service [POS] Data)	5 (POS Card Presence)	One of the following: • 0 (Card present) • 1 (Card not present)
61 (Point-of-Service [POS] Data)	7 (POS Transaction Status)	8 (Account Verification Service)

Data Elements	Subelement	Value
112 (Additional Data [China Use])	37 (Delegated Business Information)	All subfields must appear

Processing of Recurring Payment Transactions

The Acquirer must verify the China Recurring Payment Transaction – Recurring Payment Terms before sending a recurring payment Transaction to the China Switch. If the China Recurring Payment Transaction – Recurring Payment Terms are not consistent with the Cardholder consent, the Acquirer must not submit the Transaction to the China Switch. If the Recurring Payment Terms are consistent with the Cardholder consent, the Acquirer must populate the China Recurring Payment Transaction – Recurring Payment Terms in Data Element 112 (Additional Data [China Use]) Subelement 37 (Delegated Business Information).

The Acquirer must identify each recurring payment Transaction with the following values:

Data Elements	Subfield	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	10 (Credential on File)
61 (Point-of-Service [POS] Data)	1 (POS Terminal Attendance)	One of the following: • (Unattended Terminal (Cardholder-activated Terminal [CAT], home PC, mobile phone, personal digital assistant [PDA])) • 2 (No Terminal used (voice/ audio response unit [ARU] authorization; server))
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)	7 (POS Transaction Status)	0 (Normal Request)
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)
112 (Additional Data [China Use])	37 (Delegated Business Information)	Subfields 01, 02, 03, 04, 05 and 11 must appear

5.4.2.2 Transaction Requirement for Issuers

Adding a New Recurring Payment Series

The Issuer must secure Cardholder consent for the below China Recurring Payment Transaction – Recurring Payment Terms before the completion of the initial recurring payment Transaction:

- Card Acceptor Name
- Merchandise or service
- Payment account
- Recurring frequency or condition
- End date (if applicable)

The Issuer must provide a service to the Cardholder to query and manage the consented recurring payment series.

Processing of Recurring Payment Transactions

The Issuer must verify the China Recurring Payment Transaction – Recurring Payment Terms for each recurring payment Transaction. The Issuer must decline the recurring payment Transaction if the China Recurring Payment Transaction – Recurring Payment Terms is inconsistent with the Cardholder consent.

5.5 Installment Billing

5.5.1 Single-Authorization Installment Billing

5.5.1.2 Transaction Processing Procedures

For India Domestic Transactions completed with electronically recorded Card information (whether Card-read or key-entered) or manually recorded Card information (whether imprinted or handwritten), the first installment must be processed within four days of the Transaction date.

5.6 Transit Transactions Performed for Debt Recovery

5.6.1 Transit First Ride Risk Framework

In Australia, the Rule on this subject is modified to replace Table 10 with Table 11.

Table 11: Authorization Request Response/0110 Message DE 39 (Response Code) Decline Value Categories

Recoverable	Unrecoverable	Temporarily Recoverable	Not Claimable
DE39 Value			
05 (Do not honor)	03 (Invalid merchant)	01 (Refer to card issuer)	14 (Invalid card number)
30 (Format error)	04 (Capture card)	51 (Insufficient funds/ over credit limit)	15 (Invalid issuer)
55 (Invalid PIN)	12 (Invalid transaction)	70 (Contact card issuer)	41 (Lost card)
57 (Transaction not permitted to issuer/ cardholder)	13 (Invalid amount)	86 (PIN validation not possible)	43 (Stolen card)
61 (Exceeds withdrawal amount limit)	58 (Transaction not permitted to acquirer/ terminal)	87 (Purchase amount only; no cash back allowed)	54 (Expired card)
62 (Restricted card)	88 Cryptographic failure)		92 (Unable to route transaction)
63 (Security violation)			94 (Duplicate transmission detected)
65 (Exceeds withdrawal count limit)			
71 (PIN not changed)			
75 (Allowable number of PIN tries exceeded)			
76 (Invalid/nonexistent "To Account" specified)			
77 (Invalid/nonexistent "From Account" specified)			
78 (Invalid/Nonexistent account specified)			
91 (Authorization system or issuer system inoperative)			

Recoverable	Unrecoverable	Temporarily Recoverable	Not Claimable
96 (System error)			

5.7 Use of Automatic Billing Updater

In the Asia/Pacific Region, each Issuer must comply and each Acquirer may comply with the ABU requirements set forth in this chapter.

5.9 Merchant-initiated Transactions

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

For Acquirers in Japan, a Merchant-initiated Transaction may contain the applicable MIT indicator value as described in Appendix C.

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 Acquirer and Merchant Requirements

In the EEA, 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.

In **Hungary**, the following additional Rule applies.

An Acquirer of e-commerce Merchants located in Hungary must ensure that 90% of its e-commerce Intracountry Transactions originate from Merchants that provide Cardholders the option to save Mastercard and Maestro Account data on file, and to use the previously saved Account data to perform a Credential-on-file (COF) Transaction. Tokenized and non-tokenized data storage solutions qualify to show compliance with this requirement.

Compliance is calculated on a quarterly basis and is measured at authorization level. Effective from 1 January 2023, in any given quarter, 65% of an Acquirer's e-commerce Intracountry Transactions must originate from Merchants that are COF-enabled. From 30 June 2023 in any given quarter, 90% of an Acquirer's e-commerce Intracountry Transactions must originate from Merchants that are COF-enabled. A Merchant is COF-enabled if it has at least one Transaction in the corresponding quarter that carries the Credential-on File indicator or a WID of 327.

An Acquirer must ensure that its e-commerce Merchants in Hungary offer to Cardholders a method to provide the initial consent to the Merchant and/or its agent to store the Mastercard or Maestro Account data on file, either in advance of or when carrying out the first Transaction with the Merchant. The Merchant must also provide a process for deleting and updating previously saved credentials.

SCA Requirements

The following Rules apply to Intracountry and Cross-border Transactions within and between SCA Countries.

Authentication Amount

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, in the UK and Gibraltar, 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 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 may apply as provided for in applicable legislation.

This Rule does not apply to recurring payment Transactions.

Attempt to Authenticate Following Soft Decline

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) or use an alternative technical SCA solution. 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.

Secure Corporate Payments

When an authentication or an authorization is flagged as a Secure Corporate Payment, the Acquirer must ensure that the Transaction meets the requirements set out in applicable regulation for application of the Secure Corporate Payment exemption.

5.1.2 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, Montenegro, North Macedonia, Poland, Romania, Serbia, Slovakia, or Slovenia must not participate in the Activation During Shopping (ADS) method of Cardholder enrollment in Mastercard Identity Check 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 Mastercard Identity Check 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 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, UK, and Gibraltar, 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.

SCA Requirements

The following Rule applies for Intracountry and Cross-border Transactions within and between SCA Countries.

An Issuer located in an SCA Country 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."

An Issuer must not challenge more than 5 percent of all authentication requests carrying an Acquirer exemption or exclusion flag unless there is material risk of fraud, and an Issuer that has not opted out of the Authentication Express program must not challenge more than 5 percent of all authentication requests carrying a SCA delegation flag unless there is material risk of fraud.

5.1.3 Use of Static AAV for Card-not-present Transactions

In Belgium, an Issuer of Maestro Cards must technically support Card-not-present Transactions that contain a value of 3 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 Belgium, an Issuer must technically support the DOLM Program coding included in AN 4727 Revised Standards for the Withdrawal of Special Maestro Recurring Payments Programs in Europe Region and Introduction of DOLM in Belgium.

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 8 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 **Ireland** or **France** that acquires intracountry MO/TO transactions under other debit brands must also acquire MO/TO Transactions under the Maestro brand.

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 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, UK and Gibraltar, 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 Belgium, the Rule on this subject is modified as follows.

A Merchant with Transactions processed by an Acquirer located in the EEA, UK, or Gibraltar may submit Maestro recurring payment Transactions on a Card issued under a Maestro BIN assigned for Belgium, using a risk-based authentication approach in accordance with the Debit Online Low Risk Merchant (DOLM) program requirements.

The Acquirer located in the EEA, UK, or Gibraltar must ensure that the Merchant is properly registered for DOLM before using a Mastercard-assigned Merchant ID and static AAV on Transactions completed on Maestro Cards issued in Belgium.

An Acquirer must ensure that a Merchant not registered for DOLM does not use the DOLM Transaction coding set out in DOLM program documentation.

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, UK and Gibraltar, 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.

SCA Requirements

The following Rules apply to Intracountry and Cross-border Transactions within and between SCA Countries.

SCA is required on the initial authorization in a recurring payment arrangement, unless the initial authorization takes place as MO/TO (if allowed by local authorities).

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. As an exception to the preceding Rule, if the initial authorization is a MO/TO transaction, it must be identified as either mail order or telephone order, and not as a recurring payment.

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 MO/TO (if allowed by local authorities), then, whether SCA was carried out or not, the Trace ID of this approved authorization must be used for subsequent authorization requests in the recurring payment arrangement.

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 at least three months before the date of the particular recurring payment Transaction, and that no fraud or Cardholder dispute has been reported in connection with the recurring payment arrangement.

The Trace ID will be considered the reference to the first transaction of that series of recurring transactions mandate that the Cardholder authenticated.

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 transaction.

5.5 Installment Billing

5.5.1 Single-Authorization Installment Billing

Merchant-financed installment billing is in place in Greece. Refer to the Domestic Rules folder on Mastercard Connect® for further information.

5.5.1.2 Transaction Processing Procedures

In the EEA, UK or Gibraltar, 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.

5.5.2 Multiple-Authorization Installment Billing

Installment Payment Information

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

With respect to installment payments submitted by an Installment Provider, the MCC selected by the Acquirer may describe the installment payment service rather than the primary business of the retailer or the nature of the purchase.

5.6 Transit Transactions Performed for Debt Recovery

In the EEA, UK or Gibraltar, 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

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
Ireland	Non-reloadable prepaid Mastercard Cards in the BIN range of 539366 to 539585.
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.
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.
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, Moldova, Montenegro, Netherlands, North Macedonia, 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.
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

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**
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, Malta, Moldova, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Spain, Sweden, Switzerland, Tajikistan, Turkmenistan, Ukraine, United Kingdom, Uzbekistan, and Vatican City	Recurring payment and Credential-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, UK and Gibraltar

In the EEA, UK and Gibraltar, 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").

"SCA Country, SCA Countries" means the countries, islands and territories that have adopted legislation requiring Strong Customer Authentication (e.g., legislation transposing the PSD2 RTS, or similar legislation).

These countries are Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Gibraltar, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain, Sweden, United Kingdom, Ceuta, Melilla, Azores, Madeira, Aland Islands, Jan Mayen, French Guiana, Guadeloupe, Martinique, Réunion, Saint Martin (French Part), and Mayotte.

5.8.1 Acquirer Requirements

EMV 3DS and Identity Check

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.

An Acquirer must ensure, for itself and for its Service Providers (e.g., 3-D Secure Service Providers) the full implementation of EMV 3DS 2.2. In addition, it must ensure that its e-commerce Merchants and Service Providers (e.g., 3DS Service Providers) use the EMV 3DS 2.2 authentication to Merchant app redirection (also called 3DS Requestor App URL). An Acquirer may implement alternative technical authentication solutions that provide equivalent authentication features and performance.

A Merchant that already supports EMV 3DS version 2.1 must continue to support this format to ensure interoperability with Issuers that do not yet support EMV 3DS version 2.2 (for example, those outside of Europe).

In the EEA, Gibraltar, UK, 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 13 (Europe Region) of the *Mastercard Rules* manual.

5.9 Merchant-initiated Transactions

The following Rules apply for Intracountry and Cross-border Transactions within and between SCA Countries.

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).

To set up each individual MIT mandate, 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).

In addition to the Rules set out below, a Merchant with Transactions processed by an Acquirer located in an SCA Country that performs a MIT on a Card issued under a Maestro BIN assigned for Belgium must be registered in the Debit Online Low Risk Merchant Program.

An Acquirer is only allowed to process an MIT when:

- An MIT agreement has been established where the Merchant initiates a Transaction in which the Cardholder (1) is not actively triggering the payment and (2) at the time of Transaction initiation, is not interacting with a Merchant app or website, 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 SCA requirements for Transactions for which Card data has been registered on file with the Merchant and the Cardholder triggers the payment (a Credential-on-File CIT).

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.

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 (e.g., because it was not stored), then the Trace ID of a different authorization that took place at least three months in the past must be populated in the approved authorization request for the MIT, on condition that neither fraud nor a Cardholder dispute has been reported, if the MIT is part of a series of Transactions.

Issuers must be able to process the Trace ID, e.g., 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.

In the case of Transactions in the travel/hospitality sector that are coded as MIT, the Trace ID must be populated with a default value which is different from that which is used in other sectors, when necessary to indicate that proof of authentication is not available, owing to the involvement of a third party sales agent.

If an Acquirer is not able to properly code a Transaction as MIT, the Acquirer, is allowed to code the Transaction as MOTO, provided that SCA was performed as required by the applicable legislation.

An Acquirer is only allowed to submit an authorization for an MIT without proof of authentication - either coded as MOTO or with MIT indicator - if the Merchant indicates to the Acquirer that the Transaction was initiated on the basis of an MIT agreement.

When an authorization is flagged as a Merchant Initiated Transaction without proof of authentication, the Acquirer must ensure that the Transaction meets the requirements set out in applicable legislation.

An Acquirer must identify the specific MIT type, or in the case of a CIT occurring in an e-commerce environment that will be followed by one or more MITs, the specific CIT type in each authorization message in the field specified by the registered switch of its choice.

Travel/hospitality businesses are those identified with following MCCs:

Airlines & Air Carriers	MCCs 3000 through 3350 and 4511
Lodging	MCCs 3501 through 3999 and 7011
Car Rentals	MCCs 3351 through 3500 and 7512
Cruise Lines	MCC 4411
Travel Agencies	MCC 4722
Passenger Railways and Railroads-Freight	MCC 4112 and 4011
Vacation Rentals	MCC 6513

Bus Lines	MCC 4131
Transportation, including Ferries	MCC 4111
Taxi Cabs and Limousines	MCC 4121
Transportation Services - Not elsewhere classified	MCC 4789
Campgrounds and Trailer Parks	MCC 7033
Motor Home and Recreational Vehicle Rentals	MCC 7519
Tourist Attractions and Exhibits	MCC 7991
Aquariums, Dolphinariums, Zoos and Seaquariums	MCC 7998
Insurance Sales, Underwriting and Premiums	MCC 6300
Direct Marketing - Insurance Sales	MCC 5960
Government Services	MCC 9399
Parking Lots & Garages	MCC 7523

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 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 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® Identity Check authentication is highly recommended.

5.1.4 Debit Small-Ticket Digital Transaction Program: Brazil Only

The Debit Small-Ticket Digital Transaction Program (the "Program") allows a Maestro Account issued in Brazil to conduct e-commerce Transactions at a Merchant located in Brazil.

The following Transaction eligibility requirements apply:

- The Transaction is conducted with a Maestro Account (including prepaid Accounts) issued in Brazil;
- The Transaction occurs at a qualifying Merchant located in Brazil, as identified in DE 43, subfield 6 (Card Acceptor Country Code) of the Authorization Request/0100 or Financial Transaction Request/0200 message and the Merchant Country Name field on the Mastercard Analytics Portal. A qualifying Merchant under the Program is defined as one that maintains monthly combined Mastercard and Maestro fraud Transaction volume that does not exceed 40 basis points;
- Transactions must be identified with all required Transaction data;
- At least sixty percent (60%) of the Transactions must involve Maestro Accounts tokenized via the Mastercard Digital Enablement Service for use in Credential-on-File Transactions occurring at the Merchant's website or digital application (in Authorization Request/0100 and Financial Transaction Request/0200 messages, DE 48, subelement 26 [Wallet Program Data], subfield 1 [Wallet ID] contains a value of 327 [Merchant tokenization program]);
- For Transaction amounts up to BRL 300, the Issuer must use its standard authorization parameters when deciding whether to approve or decline a Transaction. For Transaction amounts equal to or exceeding BRL 300, the Issuer may implement appropriate risk-based authorization parameters at its discretion;
- New Merchants have a six-month grace period from the start date of the Merchant's participation in the Program to become compliant with all technical requirements and two more months to be 100% compliant with all additional Program requirements.
- Current participating Merchants have two months to become fully compliant with the new program requirements;
- The Merchant must enable Debit Mastercard and Maestro acceptance, and its Debit Mastercard Transactions must be properly submitted for dual message authorization processing;
- Each Transaction must be identified as either an original Digital Secure Remote Payment Transaction or subsequent Digital Secure Remote Payment Transaction, or involve the sharing of Identity Check Insights; and
- At least sixty percent (60%) of non-recurring Credential-on-File Transactions must involve the sharing of Identity Check Insights.

The Standards set forth in the *Chargeback Guide* apply to Transactions conducted within the Program. The Acquirer retains fraud-related chargeback liability with respect to any Maestro e-commerce Transaction completed without Issuer authentication of the Cardholder pursuant to this Program.

The Acquirer must ensure that e-commerce Transactions submitted by a Merchant participating in the Program are fully compliant with all applicable Transaction data requirements. Failure to comply with such requirements, including but not limited to the provision of valid, accurate and complete Merchant or Sponsored Merchant name, Merchant or Sponsored Merchant ID, and MCC information, will result in the Merchant not being accepted into the Program and its Transactions being blocked from the Program.

5.7 Use of Automatic Billing Updater

An Issuer in the Latin America and the Caribbean Region must comply with the ABU requirements set forth in this chapter, with the exceptions stated below.

In the Latin America and the Caribbean Region, excluding Puerto Rico and the Virgin Islands, U.S., 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 Issuer in Puerto Rico or the Virgin Islands, U.S. is not required to participate in ABU with respect to any prepaid Card Programs the Issuer may have.

An Acquirer in the Latin America and the Caribbean Region must comply with the ABU requirements set forth in this chapter.

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

In Bahrain, Egypt, Ghana, Iraq, Kenya, Kuwait, Lebanon, Morocco, Oman, Pakistan, Qatar, Saudi Arabia, South Africa, and the United Arab Emirates and effective 1 January 2024 in Nigeria, the Rule on this subject is modified as follows.

An Issuer of Accounts in Bahrain, Egypt, Ghana, Iraq, Kenya, Kuwait, Lebanon, Nigeria, Oman, Pakistan, Qatar, Saudi Arabia and the United Arab Emirates that does not meet the Minimum Average Approval Rate (available on Data Integrity Online) for Cross-border Transactions for a covered consumer product type in such country may be assessed for noncompliance and/or incentivized for improved performance as described in the *Data Integrity Monitoring Program* manual. In Nigeria, this requirement applies to Domestic Transactions only.

An Issuer of Accounts in Morocco that does not meet the Minimum Average Approval Rate (available on Data Integrity Online) for Cross-border Card-not-present Transactions for a covered consumer product type in such country may be assessed for noncompliance and/or incentivized for improved performance as described in the *Data Integrity Monitoring Program* manual.

5.1.1 Acquirer and Merchant Requirements

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

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.

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

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 Issuer Requirements

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

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.

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

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

Each Issuer and Acquirer in the Middle East/Africa Region must comply with the ABU requirements set forth in this chapter.

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.

5.10 Mastercard Micropayment Solution

The aggregation of separately authorized Cardholder purchases conducted in a Card-not-present environment into a single aggregated Transaction must only occur pursuant to the Mastercard Micropayment Solution, as set forth in this section.

The Mastercard Micropayment Solution provides for the aggregation of multiple

individual Cardholder-initiated purchases from a single Merchant into a single Transaction clearing record.

Before a Merchant may conduct Card-not-present purchase aggregation Transactions, the Merchant must be registered in the Mastercard Micropayment Solution. To propose a Merchant for registration:

- • The Acquirer must submit the completed Mastercard Micropayment Solution registration form to micropayments@mastercard.com;
- • The Acquirer must provide all information and material required by Mastercard in connection with the proposed registration; and
- • The Acquirer and the Merchant must each satisfy all participation requirements described in the Mastercard Micropayment Solution guidelines.

The Mastercard Micropayment Solution guidelines and registration form are available in the Forms Library on Mastercard Connect®.

Mastercard, in its sole discretion, may approve or reject any application for the registration of a Merchant in the Mastercard Micropayment Solution.

For contactless aggregated transit Transaction requirements, refer to Rule 4.5.

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.

5.1 Electronic Commerce Transactions

5.1.1 Acquirer and Merchant Requirements

In addition, with respect to **Maestro e-commerce Transactions**:

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

2. The Merchant may support EMV 3D Secure (2.0). When supported, the following requirements apply:

a. For the EMV 3D Secure 2.0 specification, the Merchant must support both browser and in-app Transactions.

7. The Acquirer must technically support the data fields and values described in the "Electronic Commerce Transactions" section of Appendix C for Non-Mastercard BIN Maestro CNP debit card Transactions occurring at a Merchant that chooses to route to the Single Message System. Each resulting Non-Mastercard BIN Maestro CNP debit card Transaction (which can be for any amount) must be properly identified in the Financial Transaction Request/0200 message.

8. The Acquirer may submit a Non-Mastercard BIN Maestro CNP debit card Transaction to the Single Message System as an e-commerce Transaction when the e-commerce Merchant is located in the U.S. Region or a U.S. Territory.
9. The Acquirer retains fraud-related chargeback liability with respect to any Non-Mastercard BIN Maestro CNP debit card Transaction.

5.1.2 Issuer Requirements

The following applies with respect to Non-Mastercard BIN Maestro CNP debit card Transactions routed for processing by means of the Single Message System:

An Issuer must be able to receive and respond to a Financial Transaction Request/0200 message when presented by an Acquirer and initiated at an e-commerce Merchant located in the U.S. Region or a U.S. Territory.

Chapter 6 Payment Transactions and Funding Transactions

The following Standards apply with regard to Payment Transactions, including MoneySend Payment Transactions and Gaming Payment Transactions, and Funding 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 228
6.1.1 Payment Transactions - Acquirer and Merchant Requirements 228
6.1.2 Payment Transactions—Issuer Requirements 229
6.2 Gaming Payment Transactions 230
6.3 MoneySend Payment Transactions 230
6.4 China Deposit Transactions – China Only 231
6.5 China Funds Transfer Transactions – China Only 231
6.6 Funding Transactions 231
Variations and Additions by Region 231
Asia/Pacific Region 232
6.4 China Deposit Transactions – China Only 232
6.4.1 Non-discrimination Regarding Maximum Transaction Amount Limit 232
6.4.2 ATM Access Fee 232
6.4.3 Account Verification 232
6.4.4 Failed Transaction 232
6.5 China Funds Transfer Transactions – China Only 232
6.5.1 China Funds Transfer Transaction Terms 233
6.5.2 Non-discrimination Regarding Maximum Amount Limit 233
6.5.3 ATM Access Fee 233
6.5.4 Account Verification 234
6.5.5 Funds Availability 234
Europe Region 234
6.1 Payment Transactions 234
6.1.1 Payment Transactions—Acquirer and Merchant Requirements 234
6.1.2 Payment Transactions—Issuer Requirements 235

6.1 Payment Transactions

A Payment Transaction is a transfer of funds to an Account via the Corporation System.

A Payment Transaction is identified with the following values:

- a value of 28 (Payment Transaction) in DE 3, subfield 1 (Cardholder Transaction Type Code) of authorization request and clearing messages;
- a Transaction Category Code (TCC) of P (Payment Transaction) in DE 48 of authorization request messages;
- the applicable value in DE 18 (Merchant Type) of authorization request messages and DE 26 (Acceptor Business Code [MCC]) of clearing messages; and
- the applicable value in DE 48, subelement 77 (Transaction Type Identifier) of authorization request messages and PDS 0043 (Transaction Type Identifier) of clearing 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 and no later than 24 hours after the time 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 or Gaming 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 or Gaming 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 or Gaming 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 or Gaming Payment Transaction must be in accordance with the *Mastercard MoneySend and Funding Transactions Program Standards* or *Mastercard Gaming and Gambling Payments Program Standards*, as applicable.
9. The Acquirer or Merchant that offers the Payment Transaction service must not request or require that a Cardholder disclose their 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 they must provide their 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 they must provide their 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; and
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

The Gaming Payment Transaction is a transaction that may be used to transfer winnings or value usable for gambling or gaming to a Mastercard or Maestro Account.

NOTE: Refer to the *Mastercard Gaming and Gambling Payments Program Standards* for more information.

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 *Mastercard MoneySend and Funding Transactions Program Standards*.

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 *Mastercard MoneySend and Funding Transactions Program Standards* for a list of Eligible Commercial Card Program types.

6.4 China Deposit Transactions – China Only

NOTE: A Rule on this subject appears in the "Asia/Pacific Region" section at the end of this chapter.

6.5 China Funds Transfer Transactions – China Only

NOTE: A Rule on this subject appears in the "Asia/Pacific Region" section at the end of this chapter.

6.6 Funding Transactions

Each Issuer and Acquirer and each Funding Transaction must comply with all requirements set forth in the Standards applicable to Funding Transactions, including but not limited to those in the *Mastercard MoneySend and Funding Transactions Program Standards*.

As set forth and as from the effective dates set forth in the *Mastercard MoneySend and Funding Transactions Program Standards*, the following requirements apply with respect to Funding Transactions identified with MCC 4829 (Money Transfer), MCC 6538 (Funding Transactions for MoneySend), or MCC 6540 (Funding Transactions):

- Before submitting Funding Transactions using any of these MCCs, an Acquirer must first register itself and each Merchant proposing to initiate such Funding Transactions with Mastercard.
- The Acquirer must use the appropriate Transaction Type Indicator (TTI) value in DE 48, subelement 77 (Transaction Type Identifier) of authorization request messages and in DE 48, PDS 0043 (Transaction Type Identifier) of clearing messages.
- The Acquirer must ensure that each Merchant and each Funding Transaction complies with all applicable legal and operational requirements and that the Funding Transaction includes any required reference data in DE 108 (Additional Transaction Reference Data) of authorization request messages.
- The Issuer must comply with requirements regarding internal controls for AML compliance and information retention for each Funding Transaction received.

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.

6.4 China Deposit Transactions – China Only

This Rule 6.4 and its subsections apply to China domestic Transactions only.

Each Issuer and Acquirer must comply with all requirements set forth in the Standards applicable to China Deposit Transactions, including the technical specifications for authorization messages and the China Interbank ATM Deposit Program Guide.

An Acquirer may choose to participate in China Deposit Transactions; provided that if an Acquirer deploys ATM Terminals that participate in domestic deposit transactions of other scheme brands or networks, such Acquirer's ATM Terminals must participate in China Deposit Transactions.

6.4.1 Non-discrimination Regarding Maximum Transaction Amount Limit

An Acquirer may impose a maximum amount limit on China Deposit Transactions 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 scheme brands or networks. This Rule does not limit the application of other non-discrimination provisions contained in the Standards.

6.4.2 ATM Access Fee

The Acquirer may charge an ATM Access Fee or other fee types imposed, or advised of, at an ATM Terminal, in connection with a Deposit Transaction. The Acquirer must follow the requirements for Rule 4.18.3 ATM Access Fee Requirements in Chapter 4 of this manual.

6.4.3 Account Verification

The Acquirer may submit an account verification message to verify the validation of the deposit account prior to initiating the China Deposit Transaction.

The Issuer must return the deposit account Cardholder name with surname truncated via the account verification response message if the Account is valid.

6.4.4 Failed Transaction

The ATM Terminal must be able to notify the depositor and return the cash if the Deposit Transaction fails.

6.5 China Funds Transfer Transactions – China Only

This Rule 6.5 and its subsections apply to China domestic Transactions only.

Each Issuer and Acquirer must comply with all requirements set forth in the Standards applicable to the China Funds Transfer Transaction, including in the technical specifications for authorization messages, and in the *China Interbank ATM Funds Transfer Program Guide*.

6.5.1 China Funds Transfer Transaction Terms

Key terms used in this section are defined in the following table for purposes of this section only.

Terms	Description
Funding Account	The funding source of the Originating Account Holder, from where funds are acquired by the Originating Institution to initiate a PTA Transaction.
Funding Institution	The issuer of funding account. The Funding Institution and Originating Institution will be the same entity if the funding institution originates the China Funds Transfer Transaction. Funding Institution is also referred as Funding Issuer.
Originating Institution	The Customer that notifies the China Switch to originate a China Funds Transfer Funding Transaction (optional) or a China Funds Transfer Payment Transaction. Also referred to as an Acquirer.
Receiving Account	The Account held by a Receiving Account Holder and to which the Receiving Customer must ensure receipt of a China Domestic Funds Transfer Transaction.
Receiving Institution	The Customer that receives and approves a China Funds Transfer Payment Transaction. Also referred to as the Issuer of Receiving Account in funds transfer transactions.

6.5.2 Non-discrimination Regarding Maximum Amount Limit

A Funding Institution or Receiving Institution may impose a maximum amount limit on China Funds Transfer Transactions provided that the limit imposed on Cardholders is the same or more favorable than the limits imposed on cardholders of other scheme brands or networks. This Rule does not limit the application of other non-discrimination provisions contained in the Standards.

6.5.3 ATM Access Fee

The Originating Institution may charge an ATM Access Fee or other fee types imposed, or advised of, at an ATM Terminal, in connection with a China Funds Transfer Transactions. The Acquirer must follow the requirements in Rule 4.18.3 ATM Access Fee Requirements in Chapter 4 of this manual.

6.5.4 Account Verification

The Originating Institution may submit an account verification message to verify the validation of the receiving account prior to initiating the China Funds Transfer Transaction.

The Receiving Institution must return the receiving account Cardholder name with Surname truncated via the account verification response message if the account is valid.

6.5.5 Funds Availability

For a China Funds Transfer Transaction that occurs at an ATM Terminal, the Receiving Institution must post the funds to the Receiving Account immediately after the approval of the China Funds Transfer Transaction.

Reversal is not allowed for a China Funds Transfer Transaction.

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, UK and Gibraltar, the Rule on this subject is modified as follows.

A Payment Transaction (including Gaming Payment Transactions and MoneySend Payment Transactions) 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, UK and Gibraltar, 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.

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....238
7.2 Terminal Requirements....238
7.2.1 Terminal Function Keys for PIN Entry....239
7.2.2 Terminal Responses....240
7.2.3 Terminal Transaction Log....240
7.2.4 Contactless-enabled Terminals and Contactless Reader Requirements....240
7.3 POS Terminal Requirements....241
7.3.1 Contactless-enabled POS Terminals....241
7.3.2 Contactless-only POS Terminals....242
7.4 Mobile POS (MPOS) Terminal Requirements....243
7.5 ATM Terminal and Bank Branch Terminal Requirements....244
7.5.1 ATM Terminals....245
7.5.2 Bank Branch Terminals....245
7.5.3 Contactless-enabled ATM and Bank Branch Terminals....246
7.6 Hybrid Terminal Requirements....246
7.6.1 Hybrid POS Terminal Requirements....247
Hybrid POS Terminal and Chip-only MPOS Terminal Displays....248
7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements....248
7.7 Mastercard Consumer-Presented QR Functionality....249
Variations and Additions by Region....250
Asia/Pacific Region....250
7.2 Terminal Requirements....250
7.3 POS Terminal Requirements....250
7.3.1 Contactless-enabled POS Terminals....251
7.4 Mobile POS (MPOS) Terminal Requirements....251
7.5 ATM Terminal and Bank Branch Terminal Requirements....252
7.6 Hybrid Terminal Requirements....252
7.6.1 Hybrid POS Terminal Requirements....252
Canada Region....253
7.3 POS Terminal Requirements....253
7.3.1 Contactless-enabled POS Terminals....253
7.4 Mobile POS (MPOS) Terminal Requirements....253

7.5 ATM Terminal and Bank Branch Terminal Requirements....253
7.5.3 Contactless-enabled ATM and Bank Branch Terminals....253
Europe Region....254
7.1 Terminal Eligibility....254
7.2 Terminal Requirements....254
7.2.4 Contactless-enabled Terminals and Contactless Reader Requirements....254
7.3 POS Terminal Requirements....254
7.3.1 Contactless-enabled POS Terminals....255
7.4 Mobile POS (MPOS) Terminal Requirements....256
7.5 ATM Terminal and Bank Branch Terminal Requirements....257
7.5.2 Bank Branch Terminals....257
7.5.3 Contactless-enabled ATM and Bank Branch Terminals....257
7.6 Hybrid Terminal Requirements....258
7.6.1 Hybrid POS Terminal Requirements....258
7.6.2 Hybrid ATM Terminal and Bank Branch Terminal Requirements....258
Latin America and the Caribbean Region....259
7.3 POS Terminal Requirements....259
7.3.1 Contactless-enabled POS Terminals....260
7.6 Hybrid Terminal Requirements....261
Middle East/Africa Region....261
7.3 POS Terminal Requirements....261
7.3.1 Contactless-enabled POS Terminals....261
7.6 Hybrid Terminal Requirements....261
7.6.1 Hybrid POS Terminal Requirements....261
United States Region....261
7.3 POS Terminal Requirements....262
7.3.1 Contactless-enabled POS Terminals....262
7.4 Mobile POS (MPOS) Terminal Requirements....262
7.5 ATM Terminal and Bank Branch Terminal Requirements....262
7.6 Hybrid Terminal Requirements....263
Additional U.S. Region and U.S. Territory Rules....263
7.6 Hybrid Terminal Requirements....263
7.6.1 Hybrid POS Terminal Requirements....263
Hybrid POS Terminal and Chip-only MPOS Terminal Displays....263

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 (including an MPOS Terminal) that is owned, operated or controlled by a Merchant and is in the Merchant's physical possession, 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;
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 that clearly displays to the Cardholder:
   a. The Transaction amount;
   b. Any Transaction data entered into the Terminal by the Cardholder; and
   c. The response received as the result of the Cardholder's Transaction request, including the application labels or preferred names on a multi-application Card.

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: Modifications to this Rule appear in the "Asia/Pacific Region" and "Europe Region" sections 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.

Except as required or permitted by the Standards, 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. As an exception to this Rule, Merchant-approved Maestro POS Transactions 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. Contactless aggregated transit Transaction and single tap and PIN contactless Transaction processing also support temporary logging of chip data for use in a subsequent authorization request after the initial attempt.

When an attempted Transaction is rejected, an indication or reason for the rejection must be included on the Terminal Transaction log.

7.2.4 Contactless-enabled Terminals and Contactless Reader Requirements

For purposes of this chapter, "contactless-enabled" means a Terminal with a contactless reader that is activated and that accepts Cards and Access Devices based on contactless chip technology ("EMV Mode") and optionally magnetic stripe technology "Magnetic Stripe Mode").

All contactless-enabled POS Terminals must transmit the device type indicator when present in the Card or Access Device in DE 48, subelement 23 (Payment Initiation Channel), subfield 1 (Device Type) of Authorization Request/0100 and Financial Transaction Request/0200

messages and in PDS 0198 (Device Type Indicator) of First Presentment/1240 messages. This requirement applies as follows.

Region	Effective Date
Canada and U.S. Regions	Currently in effect
Asia/Pacific, Europe, Latin America and the Caribbean, and Middle East/Africa Regions	Effective for Contactless Transactions occurring on or after 1 January 2026

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 Cardholder Verification Method (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.

Support of CDCVM is required only for Transactions that exceed the CVM limit.

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

7.3 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.

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," and "United States Region" sections at the end of this chapter.

7.3.1 Contactless-enabled POS Terminals

A contactless-enabled POS Terminal must comply with the following.

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	• Must support both online PIN and CDCVM; and • If Mastercard is accepted, must support signature CVM. Signature collection is optional.
Does not support online PIN	Must be configured in accordance with one of the following: 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. 2. A high-value Transaction can occur with signature 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 CVM and CDCVM must be supported. Signature collection is optional.

Mastercard Rule 5.12.3, "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 "Asia/Pacific Region," "Canada Region," "Middle East/Africa Region," "Europe Region," "Latin America and the Caribbean Region," and "United States Region" sections at the end of this chapter.

7.3.2 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 7.3 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.
3. Support online PIN, if required for contactless-enabled POS Terminals in the Merchant's Region or country.

7.4 Mobile POS (MPOS) Terminal Requirements

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.

An MPOS Terminal that cannot print a paper Transaction receipt at the time the Transaction is conducted may be deployed, provided the Merchant has a means by which to provide a receipt to the Cardholder upon request (for example, in an email or text message).

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.

Refer to Section 4.7 regarding the deployment of an MPOS Terminal that uses only contactless payment functionality as a Merchant's sole means of Mastercard and/or Maestro acceptance.

All MPOS Terminals (including Chip-only 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 and excludes contactless-only MPOS Terminals.

NOTE: A modification to this provision of the Rule appears in the "Asia/Pacific Region" section at the end of this chapter.

MPOS Terminal Identification

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*.

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).

Chip-only MPOS Terminal Identification

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.

A software-based Chip-only MPOS Terminal must use the following values:

- In the Authorization Request/0100 or Financial Transaction Request/0200 message, a value of:
  - 2 (Terminal does not have PIN entry capability) or 3 (MPOS Software-based PIN Entry Capability) in DE 22 (Point of Service Data Code), Subfield 2 (POS Terminal PIN Entry Mode)
  - 0 (Dedicated MPOS Terminal with PCI compliant dongle [with or without key pad]) or 1 (Off the Shelf Mobile Device) in DE 48 (Additional Data—Private Use), subelement 21 (Acceptance Data), subfield 1 (MPOS Acceptance Device Type)
- In the First Presentment/1240 message, a value of:
  - 2 (Terminal does not have PIN entry capability) or 3 (MPOS Software-based PIN Entry Capability) in DE 22 (Point of Service Data Code), Subfield 2 (Terminal Data: Card Data Input Capability)
  - 0 (Dedicated MPOS Terminal with PCI compliant dongle [with or without key pad]) or 1 (Off the Shelf Mobile Device) in PDS 0018 (Acceptance Data), subfield 1 (MPOS Acceptance Device Type)

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*.

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.

7.5 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 4.14.4, 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 included 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 4.14.2, 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-enabled ATM and Bank Branch Terminals

Online PIN must be the only CVM supported for Contactless Transactions effected:

- At a contactless-enabled ATM Terminal with a Mastercard, Maestro, or Cirrus Card or Access Device; or
- At a contactless-enabled Bank Branch Terminal with a Maestro or Cirrus Card or Access Device.

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

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. Effective 1 April 2024, this includes when a magnetic stripe is not present on the Chip Card;
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 *M/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 *M/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 3.5.
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 "Asia/Pacific Region," "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.

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.
- Each Mastercard Consumer-Presented QR Transaction must be sent for online authorization by the Issuer.
- Terminal CVM processing is not supported for Mastercard Consumer-Presented QR Transactions.
- 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 must transmit the device type indicator when present in the Card or Access Device used to conduct a Mastercard Consumer-Presented QR Transaction in DE 48, subelement 23 (Payment Initiation Channel), subfield 1 (Device Type) of the Authorization Request/0100 or Financial Transaction Request/0200 message and in PDS 0198 (Device Type Indicator) of the First Presentment/1240 message. This requirement applies as follows.

Region	Effective Date
Canada and U.S. Regions	Currently in effect
Asia/Pacific, Europe, Latin America and the Caribbean, and Middle East/Africa Regions	Effective for Mastercard Consumer-Presented QR Transactions occurring on or after 1 January 2026

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.

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.

7.2 Terminal Requirements

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

For a Debit Mastercard Card Chip Transaction, a Terminal must not display the application label "Credit" or any other term or abbreviation that may be construed to mean or refer to a credit instrument. In accordance with the Standards, the Terminal must display the application preferred name or application label corresponding to the Mastercard-branded Application Identifier (AID).

7.3 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.

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

All newly-deployed POS Terminals must be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality:

- Effective 1 January 2024, with the exception of automated fuel dispenser (AFD) Terminals and integrated POS (iPOS) Terminals deployed at fuel Merchants; and
- Effective 1 July 2026 for AFD Terminals and iPOS Terminals deployed at fuel Merchants, as identified with the following MCCs:
  - MCC 5541 (Service Stations [with or without Ancillary Services])
  - MCC 5542 (Fuel Dispenser, Automated)
  - MCC 5983 (Fuel Dealers: Coal, Fuel Oil, Liquefied Petroleum, Wood)

This requirement excludes contactless-only acceptance as described in Rule 4.7.

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

All POS Terminals, including CATs and MPOS Terminals and excluding contactless-only acceptance as described in Rule 4.7, may be Dual Interface Hybrid Terminals that support and enable:

- both EMV contact and EMV Mode contactless payment functionality; and
- both PBoC contact and PBoC mode contactless payment functionality for China domestic Transactions.

An attended POS Terminal, including any MPOS Terminal, must support online PIN for all China Domestic Transactions, whether conducted using a magnetic stripe reader, a contact chip reader, or a contactless reader. Refer to Rule 3.4 for requirements relating to the use of PIN for Mastercard magnetic stripe Transactions.

In **Indonesia** and **Republic of Korea**, the Rule on this subject is modified as follows.

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.

7.3.1 Contactless-enabled POS Terminals

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

Except as stated below, 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.

Any contactless-enabled POS Terminal submitted to the Corporation for MTIP testing as a new project must only support EMV Mode Contactless Transactions and must not support Magstripe Mode Contactless Transactions.

The following requirements apply to online PIN support on the contact and contactless interface of a Dual Interface POS Terminal and on the contactless interface of a contactless-only POS Terminal:

- In China, all POS Terminals (including MPOS Terminals) that accept China Domestic Transactions must support online PIN. For Cross-border Transactions, online PIN must be enabled in accordance with the below Asia/Pacific Region schedule.
- In all other Asia/Pacific Region countries and territories except Japan, Republic of Korea, and Taiwan:
  - Effective 1 April 2023, all contactless-enabled POS Terminals submitted to the Corporation for MTIP testing as a new project must support online PIN.
  - Effective 1 April 2024, all newly deployed contactless-enabled POS Terminals must support online PIN.

Support of online PIN is optional at MPOS Terminals, except in China, as stated above.

7.4 Mobile POS (MPOS) Terminal Requirements

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 **Japan**, the Rule on this subject is modified as follows.

Effective 1 January 2024, 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 **Indonesia** and **Republic of Korea**, the Rule on this subject is modified as follows.

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.

For China domestic Transactions, the Rule on this subject is modified as follows.

For a Transaction that occurs at a Hybrid Terminal, if the Card also supports Mastercard chip technology, the Transaction must be completed using the chip. Technical fallback to magnetic stripe is not permitted.

7.6.1 Hybrid POS Terminal Requirements

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

For a Debit Mastercard Card Chip Transaction, a Hybrid POS and Chip-only MPOS Terminal must not display the application label "Credit" or any other term or abbreviation that may be construed to mean or refer to a credit instrument. In accordance with the Standards, the Terminal must display the application preferred name or application label corresponding to the Mastercard-branded Application Identifier (AID).

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 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.

7.3.1 Contactless-enabled POS Terminals

In the Canada Region, the Rule on this subject is modified to add the following:

All contactless-enabled POS Terminals, including any contactless-enabled Terminal submitted to the Corporation for MTIP testing as a new project, must only support EMV Mode Contactless Transactions and must not support Magnetic Stripe Mode Contactless Transactions.

7.4 Mobile POS (MPOS) Terminal Requirements

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

All MPOS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

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.

7.5.3 Contactless-enabled ATM and Bank Branch Terminals

All contactless-enabled ATM and Bank Branch Terminals, including any contactless-enabled Terminal submitted to the Corporation for MTIP testing as a new project, must only support

EMV Mode Contactless Transactions and must not support Magnetic Stripe Mode Contactless Transactions.

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, UK and Gibraltar, 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, UK and Gibraltar, 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.

7.2.4 Contactless-enabled Terminals and 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, UK and Gibraltar, 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.

7.3 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.

7.3.1 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 must ensure that all POS Terminals (including MPOS Terminals) are contactless-enabled.

All contactless-enabled POS Terminals must support EMV Mode Contactless Transactions.

All newly deployed contactless-enabled POS Terminals, including any contactless-enabled Terminal submitted to the Corporation for MTIP testing as a new project, must only support EMV Mode Contactless Transactions and must not support Magnetic Stripe Mode Contactless Transactions.

Effective 1 January 2024, all contactless-enabled POS Terminals must only support EMV Mode Contactless Transactions and must not support Magnetic Stripe Mode Contactless Transactions.

The Acquirer of a Merchant located in **Italy** and identified with one of the following Card acceptor business codes (MCCs) must ensure that all POS Terminals at the Merchant's locations are contactless-enabled.

MCC	Description
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

MCC	Description
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

Online PIN Support

POS Terminals deployed in Ireland and the United Kingdom may either support or not support online PIN on the contactless interface.

In Ireland and the United Kingdom, all new POS Terminals that are submitted to the Corporation for M-TIP testing on or after 1 April 2023 must support online PIN on the contactless interface if they support online PIN on the contact interface.

All newly deployed POS Terminals in France must support online PIN on the contactless interface.

Prior to 31 December 2023, POS Terminals deployed in Finland may either support or not support online PIN on the contactless interface.

Effective 1 May 2024, POS Terminals deployed in Israel may either support or not support online PIN on the contactless interface.

In Israel, it is strongly recommended that all new POS Terminals submitted to the Corporation for M-TIP testing on or after 1 May 2024 support online PIN on the contactless interface if the POS Terminal supports online PIN on the contact interface.

7.4 Mobile POS (MPOS) Terminal Requirements

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, UK and Gibraltar:

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.

7.5 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. Transfers from one account to another and account selection are not currently supported in the Europe Region.
3. 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).
4. 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.

7.5.3 Contactless-enabled ATM and Bank Branch Terminals

All contactless-enabled ATM and Bank Branch Terminals must support EMV Mode Contactless Transactions.

All newly-deployed contactless-enabled ATM and Bank Branch Terminals, including any contactless-enabled Terminal submitted to the Corporation for MTIP testing as a new project, must only support EMV Mode Contactless Transactions and must not support Magnetic Stripe Mode Contactless Transactions.

Effective 1 January 2024, all contactless-enabled ATM and Bank Branch Terminals must only support EMV Mode Contactless Transactions and must not support Magnetic Stripe Mode Contactless Transactions.

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, Moldova, Montenegro, North Macedonia, 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 CVM to signature CVM 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, Moldova, Montenegro, North Macedonia, and Serbia** must support the use of PIN as the CVM for Chip Transactions conducted with a Mastercard Card.

In the EEA, UK and Gibraltar, 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.

ATM Terminals must be contactless-enabled in the following countries by the dates specified.

Countries	Effective date
Bosnia and Herzegovina	Requirement already in effect for newly deployed ATM Terminals
Czech Republic Montenegro Poland Serbia	19 January 2024 for all ATM Terminals in Czech Republic and Poland

Countries	Effective date
Albania	19 July 2024 for newly deployed ATM Terminals and for ATM Terminals that are already contactless-enabled for another acceptance brand 19 July 2028 for all ATM Terminals
Austria	
Bulgaria	
Croatia	
Cyprus	
Germany	
Greece	
Hungary	
Kosovo	
Liechtenstein	
Malta	
North Macedonia	
Romania	
Slovakia	
Slovenia	
Switzerland	

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 POS Terminal Requirements

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

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.

7.3.1 Contactless-enabled POS Terminals

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

All contactless-enabled Terminals, including a contactless-enabled Terminal submitted to the Corporation for MTIP testing as a new project, must only support EMV Mode Contactless Transactions and must not support Magnetic Stripe Mode Contactless Transactions.

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.

Online PIN Support

The following requirements apply to online PIN support on the contact and contactless interfaces of a Dual Interface POS Terminal and on the contactless interface of a contactless-only POS Terminal.

Online PIN support is required for:	Effective as of:
All contactless-enabled POS Terminals submitted to Mastercard for M-TIP testing, except MPOS and integrated POS (iPOS) Terminals	In effect
All newly deployed contactless-enabled POS Terminals	In effect
All contactless-enabled POS Terminals	• 1 January 2024 except in Mexico • 1 December 2025 in Mexico

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.

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.

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 POS Terminal Requirements

7.3.1 Contactless-enabled POS Terminals

In the Middle East/Africa Region, the Rule on this subject is modified as follows.

All contactless-enabled Terminals, including a contactless-enabled Terminal submitted to the Corporation for MTIP testing as a new project, must only support EMV Mode Contactless Transactions and must not support Magnetic Stripe Mode Contactless Transactions.

All contactless-enabled POS Terminals deployed in the Region must support online PIN. This requirement applies to the contact and contactless interfaces of a Dual Interface POS Terminal and the contactless interface of a contactless-only POS Terminal. MPOS Terminals are excluded from this requirement.

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 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.
- 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.
- A newly-deployed POS Terminal that supports contactless acceptance must support only EMV mode contactless. Magstripe mode contactless must not be supported.
- Effective 1 April 2023, all POS Terminals that support contactless acceptance must support only EMV mode contactless. Magstripe mode contactless must not be supported.

7.3.1 Contactless-enabled POS Terminals

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

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.

7.4 Mobile POS (MPOS) Terminal Requirements

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

All MPOS Terminals may be Dual Interface Hybrid Terminals that support and enable both EMV contact and EMV Mode contactless payment functionality.

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 connected to the Mastercard Single Message System 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....266
Canada Region....267
Europe Region....267
Single European Payments Area (SEPA)....268
Non-Single European Payments Area (Non-SEPA)....268
Latin America and the Caribbean Region....269
Middle East/Africa Region....270
United States Region....271

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 SAR	Solomon Islands
India	Sri Lanka
Indonesia	Taiwan
Japan	Thailand
Kiribati	Timor-Leste
Korea, Republic of	Tokelau
Lao People's Democratic Republic	Tonga
Macao SAR	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	Guernsey	Norway[6]
Andorra	Hungary	Poland
Antarctica	Iceland	Portugal[7]
Armenia	Ireland	Romania
Austria	Isle of Man	Russian Federation
Azerbaijan	Israel	Saint Helena, Ascension and Tristan Da Cunha
Belarus	Italy	Saint Pierre and Miquelon
Belgium	Jersey	San Marino
Bosnia and Herzegovina	Kazakhstan	Serbia
Bulgaria	Kosovo	Slovakia
Croatia	Kyrgyzstan	Slovenia
Cyprus	Latvia	Spain[8]
Czech Republic	Liechtenstein	Sweden
Denmark[9]	Lithuania	Switzerland
Estonia	Luxembourg	Tajikistan
Finland[10]	Malta	Turkey
France[11]	Moldova	Turkmenistan
Georgia	Monaco	Ukraine
Germany	Montenegro	United Kingdom[12]

6 Includes Svalbard and Jan Mayen.
7 Includes Azores and Madeira.
8 Includes Canary Islands, Ceuta and Melilla.
9 Includes Faroe Islands and Greenland.
10 Includes Aland Islands.
11 Includes Mayotte, Guadeloupe, Martinique, French Guiana, St. Martin (French Part), Réunion, and St. Barthélemy.
12 Includes Falkland Islands, South Georgia and South Sandwich Islands.

Gibraltar	Netherlands	Uzbekistan
Greece	North Macedonia	Vatican City

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	Greece	Netherlands
Antarctica	Guernsey	Norway[13]
Austria	Hungary	Poland
Belgium	Iceland	Portugal
Bulgaria	Ireland	Romania
Croatia	Isle of Man	Saint Helena, Ascension and Tristan da Cunha
Cyprus	Italy	San Marino
Czech Republic	Jersey	Slovakia
Denmark[14]	Latvia	Slovenia
Estonia	Liechtenstein	Spain
Finland[15]	Lithuania	Sweden
France[16]	Luxembourg	Switzerland
Germany	Malta	United Kingdom[17]
Gibraltar	Monaco	Vatican City

Non-Single European Payments Area (Non-SEPA)

The Non-Single European Payments Area includes the following countries or territories.

Albania	Moldova
Armenia	Montenegro

[13] Includes Svalbard and Jan Mayen.
[14] Includes Faroe Islands and Greenland.
[15] Includes Aland Islands.
[16] Includes Mayotte, Guadeloupe, Martinique, French Guiana, St. Martin (French Part), Réunion, and St. Barthélemy.
[17] Includes Falkland Islands, South Georgia and South Sandwich Islands.

Azerbaijan	North Macedonia
Belarus	Russian Federation
Bosnia and Herzegovina	Serbia
Georgia	Tajikistan
Israel	Turkey
Kazakhstan	Turkmenistan
Kosovo	Ukraine
Kyrgyzstan	Uzbekistan

Latin America and the Caribbean Region

The Latin America and the Caribbean Region includes the following countries or territories.

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[18]	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.

[18] Bonaire, St. Eustatius and Saba.

Middle East/Africa Region

The Middle East/Africa Region includes the following countries or territories.

Afghanistan	French Southern Territories	Oman
Algeria	Gabon	Pakistan
Angola	Gambia	Palestine
Bahrain	Ghana	Qatar
Benin	Guinea	Rwanda
Botswana	Guinea-Bissau	Sao Tome and Principe
Bouvet Island	Iraq	Saudi Arabia
British Indian Ocean Territory	Jordan	Senegal
Burkina Faso	Kenya	Seychelles
Burundi	Kuwait	Sierra Leone
Cameroon	Lebanon	Somalia
Cape Verde	Lesotho	South Africa
Central African Republic	Liberia	South Sudan
Chad	Libyan Arab Jamahiriya	Sudan (excluding Darfur)
Comoros	Madagascar	Tanzania
Congo	Malawi	Togo
Côte D'Ivoire	Mali	Tunisia
Democratic Republic of the Congo	Mauritania	Uganda
Djibouti	Mauritius	United Arab Emirates
Egypt	Morocco	Western Sahara
Equatorial Guinea	Mozambique	Yemen
Eritrea	Namibia	Zambia
Eswatini (formerly Swaziland)	Niger	Zimbabwe
Ethiopia	Nigeria	

West African Economic and Monetary Union (UEMOA)

The West African Economic and Monetary Union includes the following countries or territories.

Benin	Mali	Togo
Burkina Faso	Niger	Guinea-Bissau
Cote d'Ivoire	Senegal	

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..... 273

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 Section 2.1.4 Noncompliance Assessments 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	
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 or Completion Messages	A
2.11	Full and Partial Reversals	A
2.12	Full and Partial Approvals	A
2.13	Refund Transactions and Corrections	A
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

Compliance Zones

Rule Number	Rule Title	Category
2.17	Euro Conversion - Europe Region Only	C
2.18	Transaction Clearing, Queries, and Disputes	A
2.19	Chargebacks for Reissued Cards	C
2.20	Correction of Errors	A
2.21	Merchant Payment Gateway Identifier (MPG ID)	A
2.22	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
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

Compliance Zones

Rule Number	Rule Title	Category
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	Purchase with Cash Back Transactions	A
4.10	Transactions at Unattended POS Terminals	A
4.10.1	Automated Fuel Dispenser Transactions	A
4.11	PIN-based Debit Transactions - United States Region Only	A
4.12	PIN-less Single Message Transactions - United States Region Only	A
4.13	Merchant-approved Maestro POS Transactions	A
4.14	Mastercard Manual Cash Disbursement Transactions	A
4.14.1	Non-discrimination Regarding Cash Disbursement Services	A
4.14.2	Maximum Cash Disbursement Amounts	B
4.14.3	Discount or Service Charges	B
4.1	Mastercard Acceptance Mark Must Be Displayed	B
4.15	Encashment of Mastercard Travelers Cheques	B
4.16	ATM Transactions	A
4.17	ATM Access Fees	B
4.18	Merchandise Transactions at ATM Terminals	A
4.19	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

Compliance Zones

Rule Number	Rule Title	Category
5.4	Recurring Payment Transactions	A
5.5	Installment Billing	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, United Kingdom, and Gibraltar 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
7.2.2	Terminal Responses	B
7.2.3	Terminal Transaction Log	A
7.2.4	Contactless-enabled Terminals and Contactless Reader Requirements	A
7.3	POS Terminal Requirements	A
7.4	Mobile POS (MPOS) 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....278
Account Status Inquiry (ASI) Requests....278
Contactless Transactions....279
Contactless Transit Aggregated Transactions....281
Contactless-only Transactions....283
Electronic Commerce Transactions....285
Digital Secure Remote Payment Transactions....287
Digital Secure Remote Payment Transactions Containing Chip Data....287
Digital Secure Remote Payment Transactions Containing Digital Payment Data....289
Merchant-initiated Transactions following Digital Secure Remote Payment Transactions....291
Mastercard Biometric Card Program Transactions....292
Transaction Type Identifier (TTI)....293
Merchant Country of Origin....293
China Deposit Transactions....293
China Funds Transfer Transactions....294
Cardholder-initiated Transactions (CITs)....296
Merchant-initiated Transactions (MITs)....297

Transaction Date

The Transaction date appearing in DE 12 (Date and Time, Local Transaction) is specified as follows.

For the following Transaction...	The Transaction date is the date on which...
Face-to-Face	The products or services are exchanged.
Non–Face-to-Face	The products are shipped or services performed.
Vehicle Rental	The vehicle is returned, or, if applicable, the prepayment date.
Lodging	Checkout occurred, or if applicable, the prepayment date.
No-show	The Cardholder was expected to arrive at the lodging merchant and failed to appear.
Airline/Railway	The airline or railway ticket was issued.
Cruise Line	The transportation documents were issued.
On-board Cruise Line	The passenger disembarks.
Refund	The Merchant grants a credit or price adjustment.
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.
Card-not-present purchase aggregation (U.S. Region only)	The Cardholder's multiple individual purchases involving one Mastercard Account that occurred at a Merchant registered in the Mastercard Micropayment Solution are aggregated by the Merchant into a total Transaction amount and submitted to the Acquirer.

Account Status Inquiry (ASI) Requests

An ASI request is an Authorization Request/0100 or Financial Transaction Request/0200 message initiated by an Acquirer or Merchant to obtain the Issuer's validation that a Cardholder's Account is open and active, subject to ASI service requirements.

An ASI request is identified with a value of 8 (Account Status Inquiry Service [ASI]) in DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), and when submitted in connection with a purchase, contains a value of 00 (Purchase) in DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code). A Purchase ASI request must have a Transaction amount of zero.

The ASI service is Activity subject to the Standards and includes the production and delivery of deliverables (herein, "the Deliverables"), including the ASI Probability Indicator. The Deliverables are only an input to and should not be used in isolation or as the sole method for the Customer's and Merchant's retry or other related decisioning. In particular, the Customer acknowledges and agrees that its acceptance and use of the Deliverables is only one aspect of the Customer's banking activities. The Customer will have sole responsibility for ensuring that the Customer's and Merchant's use of the Deliverables is compliant with applicable law or governing authority. In addition, Mastercard is not providing the ASI service as investment, legal or financial advice, and is not making any representation or warranty about Mastercard's business operations. The Customer agrees to indemnify Mastercard for any loss to Mastercard caused by the Customer's failure to comply with applicable law or regulation when using the ASI service.

The ASI service includes the Name Validation Service, a related service that may be used by Originating Institutions to allow Senders or Transaction Initiators to validate that the Recipient or Sender is the intended person, through a process of matching the name information in the ASI request with the name associated with the Card issued by the Receiving Institution or Funding Issuer.

The Originating Institution acknowledges and agrees when using Name Validation Service that:

- The Name Validation Service does not provide a guarantee against fraud and there is a risk of fraud regardless of the name match result received.
- Mastercard does not accept liability for any loss or claims made against an Originating Institution relating to a Payment Transaction or Funding Transaction that has been made based on the name match result received using the Name Validation Service.
- Any decision to proceed with a Payment Transaction or Funding Transaction after receiving a name match result is at the discretion of the Sender or Transaction Initiator and is not solely based on the name match result received through the Name Validation Service.
- The Name Validation Service is an optional service and Mastercard makes no representation as to whether the Originating Institution is, or is not, under a legal or regulatory obligation to use it.

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").

Table 12: 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: • **07** (PAN auto-entry via contactless M/Chip) • **91** (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)
61 (Point-of-Service [POS] Data)	11 (POS Card Data Terminal Input Capabilities)	One of the following: • **3** (Contactless M/Chip) • **4** (Contactless Magnetic Stripe)

Table 13: 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: • **A** (Contactless Magnetic Stripe [Proximity Chip]) • **M** (Contactless EMV/Chip [Proximity Chip])
	7 (Card Data: Input Mode)	One of the following: • **A** (PAN auto-entry via contactless magnetic stripe) • **M** (PAN auto-entry via contactless M/Chip)

Contactless Transit Aggregated Transactions

The Acquirer must identify each Contactless transit aggregated Transaction with the following values.

Table 14: 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: • **4111** (Transportation - Suburban and Local Commuter Passenger, including Ferries) • **4131** (Bus Lines) • **4784** (Bridge and Road Fees, Tolls)
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." **NOTE: Additionally, the value of 82 appears in Contactless debt repayment Transactions.**
48 (Additional Data - Private Use)	1 (Transaction Category Code [TCC])	**X** (Airline and Other Transportation Services)
48 (Additional Data - Private Use), subelement 64 (Transit Program)	1 (Transit Transaction Type)	One of the following: • **03** (Post-authorized Aggregated) • **05** (Other) **NOTE: This value is only for contactless transit aggregated Transactions occurring at U.S. Region Merchant locations.** • **06** (Post-authorized Aggregated Maestro)
61 (Point-of-Service [POS] Data	1 (POS Terminal Attendance)	**1** (Unattended terminal)
	3 (POS Terminal Location)	**0** (On premises of merchant facility)
	4 (POS Cardholder Presence)	**0** (Cardholder present)
	5 (POS Card Presence)	**0** (Card present)
	6 (POS Card Capture Capabilities)	**0** (Terminal/Operator has no card capture capability)

Data Element	Subfield	Value
	7 (POS Transaction Status)	One of the following: • **0** (Normal request) • **1** (Deferred authorization) **NOTE: This value is only for contactless transit aggregated Transactions occurring at U.S. Region Merchant locations.** • **4** (Pre-authorized request)
	10 (Cardholder-Activated Terminal Level)	**0** (Not a CAT transaction)
	11 (POS Card Data Terminal Input Capability)	One of the following: • **3** (Contactless M/Chip) • **4** (Contactless Magnetic Stripe)

Table 15: 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: • **A** (PAN auto-entry via contactless magnetic stripe) • **M** (PAN auto-entry via contactless M/Chip)
	3 (Terminal Data: Card Capture Capability)	**0** (No capture capability)
	4 (Terminal Operating Environment)	**2** (On merchant premises; unattended terminal)
	5 (Card Present Data)	**0** (Cardholder present)
	6 (Card Present Data)	**1** (Card present)
	7 (Card Data: Input Mode)	One of the following: • **A** (PAN auto-entry via contactless magnetic stripe) • **M** (PAN auto-entry via contactless M/Chip)
26 (Merchant Business Code [MCC])		One of the following: • **4111** (Transportation-Suburban and Local Commuter Passenger, including Ferries) • **4131** (Bus Lines) • **4784** (Bridge and Road Fees, Tolls)

Data Element/PDS	Subfield	Value
PDS 0210 (Transit Transaction Program)	1 (Transit Transaction Type)	One of the following: • **03** (Post-authorized Aggregated) • **05** (Other) - effective 15 August 2022, applies to contactless transit aggregated Transactions occurring at U.S. Region Merchant locations • **06** (Post-authorized Aggregated Maestro)

Contactless-only Transactions

The Acquirer must identify each Contactless-only Transaction with the following values.

Table 16: 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 by Mastercard from time to time.
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)	**1** (Unattended terminal)
	3 (POS Terminal Location)	One of the following: • **0** (On premises of merchant facility) • **1** (Off premises of merchant facility [merchant terminal - remote location])
	4 (POS Cardholder Presence)	**0** (Cardholder present)
	5 (POS Card Presence)	**0** (Card present)
	7 (POS Transaction Status)	**0** (Normal request)
	10 (Cardholder-Activated Terminal Level)	One of the following: • **1** (Authorized Level 1 CAT: Automated dispensing machine with PIN) • **2** (Authorized Level 2 CAT: Self-service terminal) • **3** (Authorized Level 3 CAT: Limited-amount terminal)

Data Element	Subfield	Value
	11 (POS Card Data Terminal Input Capability)	One of the following: • **3** (Contactless M/Chip) • **4** (Contactless Magnetic Stripe)

Table 17: 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: • **A** (PAN auto-entry via contactless magnetic stripe) • **M** (PAN auto-entry via contactless M/Chip)
	4 (Terminal Operating Environment)	One of the following: • **2** (On merchant premises; unattended terminal) • **4** (Off merchant premises; unattended) • **6** (Off cardholder premises; unattended)
	5 (Card Present Data)	**0** (Cardholder present)
	6 (Card Present Data)	**1** (Card present)
	7 (Card Data: Input Mode)	One of the following: • **A** (PAN auto-entry via contactless magnetic stripe) • **M** (PAN auto-entry via contactless M/Chip)
26 (Merchant Business Code [MCC])		An MCC approved to be contactless-only as published by Mastercard from time to time.

Electronic Commerce Transactions

The Acquirer must identify each electronic commerce Transaction with the following values.

Table 18: Authorization Request/0100, Authorization Advice/0120, Acquirer Reversal Advice/0420, and Financial Transaction Request/0200 Messages

Data Element	Subfield or Subelement	Field	Value	Description
22	01	POS Terminal PAN Entry Mode	**09**, **10**, or **81**	**09** = PAN/Token entry via electronic commerce containing DSRP cryptogram in DE 55 (Integrated Circuit Card [ICC] System-Related Data) **10** = Credential on File **81** = PAN/Token entry via electronic commerce with optional Identity Check-AAV or DSRP cryptogram in UCAF
	02	POS Terminal PIN Entry Mode	**2**	Terminal does not have PIN entry capability
48	01	Transaction Category Code	**T**	Phone, Mail, or Electronic Commerce Order
	42/SF 1	Electronic Commerce Security Level Indicator and UCAF Collection Indicator	**As appropriate**	
61	1	POS Terminal Attendance	**1**	Unattended terminal (Cardholder-Activated Terminal [CAT], home PC, mobile phone, PDA)
	3	POS Terminal Location	**4**	On premises of Card acceptor facility (Cardholder terminal including home PC, mobile phone, PDA)
	4	POS Cardholder Presence	**4** or **5**	**4** (Cardholder not present (standing order/recurring transactions) [If the Transaction is the first payment in a recurring payment arrangement] **5** (Cardholder not present [electronic order])
	5	POS Card Presence	**1**	Card not present

Data Element	Subfield or Subelement	Field	Value	Description
	6	POS Card Capture Capabilities	**0**	Terminal/operator does not have card capture capability
	7	POS Transaction Status	**0** or **4**	**0** = Normal request **4** = Preauthorized request
	8	POS Transaction Security	**0**	No security concern
	10	Cardholder-Activated Terminal Level	**6**	Authorized Level 6 CAT: Electronic Commerce
	11	POS Card Data Terminal Input Capability Indicator	**6**	Terminal supports key entry input only

Table 19: First Presentment/1240 Message

Data Element	Subfield or Subelement	Field	Value	Description
22	1	Terminal Data: Card Data Input Capability	**6**	Terminal supports key entry input only
	2	Terminal Data: Cardholder Authentication Capability	**0**	No electronic authentication capability
	3	Terminal Data: Card Capture Capability	**0**	No capture capability
	4	Terminal Operating Environment	**2**	On acceptor premises; unattended terminal
	5	Cardholder Present Data	**4** or **5**	**4** (Cardholder not present (standing order/recurring transactions) [If the Transaction is the first payment in a recurring payment arrangement] **5** (Cardholder not present [electronic order])
	6	Card Present Data	**0**	Card not present

Data Element	Subfield or Subelement	Field	Value	Description
	7	Card Data: Input Mode	**7**, **R**, or **S**	**7** = Credential on File **R** = PAN/Token entry via Electronic commerce containing DSRP cryptogram in DE 55 (Integrated Circuit Card [ICC] System-Related Data) **S** = Electronic commerce
	12	PIN Capture Capability	**0**	No PIN capture capability
PDS	0023	Terminal Type	**CT6**	CAT Level 6 (Electronic commerce transaction)
PDS	0052	Electronic Commerce Security Level Indicator	**As appropriate**	

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 Digital Payment Data field. 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

Table 20: Authorization Request/0100 and Financial Transaction Request/0200 Messages

Data Element	Subfield or Subelement	Value
22 (Point-of-Service [POS] Entry Mode)	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])

Data Element	Subfield or Subelement	Value
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) = **50** (Mastercard Digital Enablement Service PAN Mapping); and • Subfield 2 (On-behalf [OB] Result 1) = **C** (Conversion of Token to PAN completed successfully)
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs cryptographic validation: • Subfield 1 = **51** (Mastercard Digital Enablement Service Chip Pre-Validation); and • Subfield 2 = **V** (Valid)
55 (Integrated Circuit Card [ICC] System-Related Data)		Contains chip data formatted in accordance with EMV specifications.
61 (Point-of-Service [POS] Data)	3 (POS Terminal Location)	One of the following: • **2** (Off premises of card acceptor facility [cardholder terminal including home PC, mobile phone, PDA]); or • **4** (On premises of card acceptor facility [cardholder terminal including home PC, mobile phone, PDA])
	4 (POS Cardholder Presence)	**5** (Electronic order [home PC, Internet, mobile phone, PDA])
	10 (Cardholder-Activated Terminal Level)	**6** (Authorized Level 6 CAT: Electronic commerce)

Table 21: First Presentment/1240 Messages

Data Element	Subfield or PDS	Value
22 (Point-of-Service [POS] Data Code)	4 (Terminal Operating Environment)	One of the following: • **2** (On card acceptor premises; unattended terminal); or • **4** (Off card acceptor premises; unattended)
	5 (Cardholder Present Data)	**5** (Cardholder not present [electronic order (PC, Internet, mobile phone, or PDA)])
	7 (Card Data: Input Mode)	**R** (PAN Entry via electronic commerce, including remote chip)
48 (Additional Data)	PDS 0023 (Terminal Type)	**CT 6** (CAT level 6 [electronic commerce transaction])
55 (Integrated Circuit Card [ICC] System-Related Data)		Contains chip data formatted in accordance with EMV specifications.

Digital Secure Remote Payment Transactions Containing Digital Payment Data

Table 22: Authorization Request/0100 and Financial Transaction Request/0200 Messages

Data Element	Subfield or Subelement	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	One of the following: • **10** (Credential-on-file) • **81** (PAN/Token entry via electronic commerce with optional Identity Check AAV or DSRP cryptogram in UCAF)

Data Element	Subfield or Subelement	Value
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 = **2** • Position 2 = **4** • Position 3 = **2** or **6**
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs token mapping: • Subfield 1 (On-behalf [OB] Result 1) = **50** (Mastercard Digital Enablement Service PAN Mapping); and • Subfield 2 (On-behalf [OB] Service) = **C** (Conversion of Token to PAN completed successfully)
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs cryptographic validation: • Subfield 1 = **51** (Mastercard Digital Enablement Service Chip Pre-Validation); and • Subfield 2 = **V** (Valid)
61 (Point-of-Service [POS] Data)	3 (POS Terminal Location)	One of the following: • **2** (Off premises of card acceptor facility [cardholder terminal including home PC, mobile phone, PDA]); or • **4** (On premises of card acceptor facility [cardholder terminal including home PC, mobile phone, PDA])
	4 (POS Cardholder Presence)	**5** (Electronic order [home PC, Internet, mobile phone, PDA])
	10 (Cardholder-Activated Terminal Level)	**6** (Authorized Level 6 CAT: Electronic commerce)
DE 104 (Digital Payment Data)	001 (Digital Payment Cryptogram)	Contains the DSRP cryptogram

Table 23: First Presentment/1240 Messages

Data Element	Subfield or PDS	Value
22 (Point-of-Service [POS] Data Code)	4 (Terminal Operating Environment)	One of the following: • **2** (On card acceptor premises; unattended terminal); or • **4** (Off card acceptor premises; unattended)
	5 (Cardholder Present Data)	**5** (Cardholder not present [electronic order (PC, Internet, mobile phone, or PDA)])
	7 (Card Data: Input Mode)	**S** (Electronic commerce)
48 (Additional Data)	PDS 0023 (Terminal Type)	**CT 6** (CAT level 6 [electronic commerce transaction])
	PDS 0052 (Electronic Commerce Security Level Indicator)	All of the following: • Position 1 = **2** • Position 2 = **4** • Position 3 = **2** or **6**

Merchant-initiated Transactions following Digital Secure Remote Payment Transactions

Table 24: Authorization Request/0100 and Financial Transaction Request/0200 Messages

Data Element	Subfield or Subelement	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	**10** (Credential-on-file) or **81** (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 = **2** • Position 2 = **4** • Position 3 = **7** **NOTE: Liability will depend on whether cryptographic data was present matching initial DSRP transaction.**

Data Element	Subfield or Subelement	Value
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs token mapping: • Subfield 1 (On-behalf [OB] Service) = **50** (Mastercard Digital Enablement Service PAN Mapping); and • Subfield 2 (On-behalf [OB] Result 1) = **C** (Conversion of Token to PAN completed successfully) **NOTE: Value 51 (Mastercard Digital Enablement Service Chip Pre-Validation) does not appear in a partial shipment or recurring payment.**

Table 25: First Presentment/1240 Messages

Data Element	Subfield or PDS	Value
22 (Point-of-Service [POS] Data Code)	4 (Terminal Operating Environment)	One of the following: • **2** (On card acceptor premises; unattended terminal); or • **4** (Off card acceptor premises; unattended)
	5 (Cardholder Present Data)	**5** (Cardholder not present [electronic order (PC, Internet, mobile phone, or PDA)])
	7 (Card Data: Input Mode)	**S** (Electronic commerce)
48 (Additional Data)	PDS 0023 (Terminal Type)	**CT 6** (CAT level 6 [electronic commerce transaction])
	PDS 0052 (Electronic Commerce Security Level Indicator	All of the following: • Position 1 = **2** • Position 2 = **4** • Position 3 = **7**

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.

Transaction Type Identifier (TTI)

The Transaction Type Identifier (TTI), when present in a Transaction message, must contain a value that is valid and that most accurately describes the purpose for which the Transaction is being conducted. A TTI value must not be used for any purpose other than as set forth in the applicable Standards, including but not limited to the following:

- *Customer Interface Specification*
- *Single Message System Specifications*
- *IPM Clearing Formats*
- *Mastercard Gaming and Gambling Payments Program Standards*
- *Mastercard MoneySend and Funding Transactions Program Standards*

The TTI value is populated in DE 48, subelement 77 of Authorization Request/0100 messages and Financial Transaction Request/0200 messages and in PDS 0043 of First Presentment/1240 messages.

The following TTI values are no longer valid and must not appear in Transaction messages:

- C01 = Person-to-Person
- C05 = Payment Transaction for a reason other than those defined in values C01–C04
- C09 = Card Activation

Merchant Country of Origin

The Acquirer must populate the Merchant Country of Origin in each Transaction conducted by a Government Controlled Merchant, whether such country is the same as or different from the country in which the Merchant is located or the Transaction occurs, (a) in DE 48 (Additional Data—Private Use), subelement 37 (Additional Merchant Data), subfield 4 (Home Country ID) of Authorization Request/0100 and Authorization Advice/0120 messages, and (b) in PDS 0213 (Home Country ID) in First Presentment/1240 messages.

China Deposit Transactions

In China, the following Transaction Identification Requirements apply.

The Acquirer must identify each China Domestic Deposit Transaction with the following values.

Table 26: China Domestic Deposit Transaction Values for Financial Transaction Request/0200 Messages

Data Element	Subfield	Value
3 (Processing Code)	1 (Cardholder Transaction Type)	**21** (Deposit)
61 (Point of Service [POS] Data)	7 (POS Transaction Status)	**0** (Normal Request)

China Funds Transfer Transactions

In China, the following Transaction identification requirements apply.

The Originating Institution (Acquirer) must identify each China Funds Transfer Request with the following values.

Table 27: China Funds Transfer Request Values for Financial Transaction Request/0200 Messages

Data Element	Subfield	Value
3 (Processing Code)	1 (Cardholder Transaction Type)	**10** (Funds Transfer - Funding)
25 (Point of Service Condition Code)		**00** (Used for Payer Paid Funds Transfer) **66** (Used for Payee Paid Funds Transfer)
48 (Additional Data)	77 (Transaction Type Identifier)	**D01** (Person to Person)
61 (Point of Service [POS] Data)	7 (POS Transaction Status)	**0** (Normal Request)
102 (Account Identification-1)		Account Number of the Sending Account
103 (Account Identification-2)		Account Number of the Receiving Account
112 (Additional Data, China Use)	050 (Cardholder Identification Information)	If DE 25 equals 00, the Institution Region Code for the Receiving Institution (subfield 06) is mandatory

China Switch identifies each China Funds Transfer Funding Transaction with the following values.

Table 28: China Funds Transfer Funding Transaction Values for Financial Transaction Request/0200 Messages

Data Element	Subfield	Value
3 (Processing Code)	1 (Cardholder Transaction Type)	**10** (Funds Transfer - Funding)
25 (Point of Service Condition Code)		**00** (Used for Payer Paid Funds Transfer) **66** (Used for Payee Paid Funds Transfer)
48 (Additional Data)	77 (Transaction Type Identifier)	**D01** (Person to Person)
61 (Point of Service [POS] Data)	7 (POS Transaction Status)	**0** (Normal Request)
102 (Account Identification-1)		Account Number of the Sending Account
103 (Account Identification-2)		Account Number of the Receiving Account
112 (Additional Data, China Use)	050 (Cardholder Identification Information)	If DE 25 equals 00, the Institution Region Code for the Receiving Institution (subfield 06) is mandatory

China Switch identifies each China Funds Transfer Payment Transaction with the following values.

Table 29: China Funds Transfer Payment Transaction for Financial Transaction Request/0200

Data Element	Subfield	Value
3 (Processing Code)	1 (Cardholder Transaction Type)	**28** (Funds Transfer – Payment Transaction)
25 (Point of Service Condition Code)		**00** (Used for Payer Paid Funds Transfer) **66** (Used for Payee Paid Funds Transfer)
48 (Additional Data)	77 (Transaction Type Identifier)	**D01** (Person to Person)
102 (Account Identification-1)		Account Number of the Sending Account
103 (Account Identification-2)		Account Number of the Receiving Account

Data Element	Subfield	Value
112 (Additional Data, China Use)	050 (Cardholder Identification Information)	If DE 25 equals 00, the Institution Region Code for the Receiving Institution (subfield 06) is mandatory

Cardholder-initiated Transactions (CITs)

The Acquirer must provide a Cardholder-initiated Transaction (CIT) value in Authorization Request/0100 and Financial Transaction Request/0200 messages, in addition to populating all other required data, when the Transaction occurs in an e-commerce environment and the Cardholder is authorizing the Merchant to store the credential for subsequent use.

These values may optionally be used in CITs occurring in other acceptance environments. When populated in an Authorization Request/0100 message, the same value may also be provided in the First Presentment/1240 message.

Table 30: Authorization Request/0100 and Financial Transaction Request/0200 Messages

Data Element/ Subelement	Value	Use this value when...	Examples
DE 48, subelement 22 (Multi-purpose Merchant Indicator) subfield 5 (Cardholder/Merchant Initiated Transaction Indicator)	C101 (Credential-on-file [ad hoc])	The Cardholder is authorizing the Merchant to store the Cardholder's Account data for subsequent use in connection with one or more later Transaction(s) with that Merchant (a "COF arrangement").	The Cardholder initiates a purchase and agrees that the Merchant may store the credential for future purchases.
	C102 (Standing Order [variable amount/fixed frequency])	The Cardholder is agreeing to a COF arrangement with the Merchant for a series of recurring payments of **variable amount and fixed frequency** and is initiating the first payment.	The Cardholder initiates the first in a series of monthly utility payments, where the amounts will vary based on electricity consumption.

Data Element/ Subelement	Value	Use this value when...	Examples
	C103 (Subscription [fixed amount/fixed frequency])	The Cardholder is agreeing to a COF arrangement with the Merchant for a series of recurring payments **fixed amount and fixed frequency** and is initiating the first payment. The subscription arrangement may include an allowance for price changes to occur from time to time.	The Cardholder initiates the first in a series of quarterly newspaper subscription payments of fixed amounts.
	C104 (Installment)	The Cardholder has expressly authorized a COF arrangement with the Merchant for an installment billing plan and is initiating the first payment. The installment billing must be for a single purchase of goods or services with a known amount and set frequency over a specified duration.	The Cardholder agrees to enter into an installment billing plan for the purchase of a television and to make the first payment.

Table 31: First Presentment/1240 Messages

Data Element/PDS	Value
PDS 0218 (Cardholder/Merchant Initiated Transaction Indicator)	One of the following: • C101 (Credential-on-file [ad hoc]) • C102 (Standing Order [variable amount/fixed frequency]) • C103 (Subscription [fixed amount/fixed frequency]) • C104 (Installment) Refer to Table 28 for usage information.

Merchant-initiated Transactions (MITs)

The Acquirer must identify each Merchant-initiated Transaction (MIT) in Authorization Request/0100 and Financial Transaction Request/0200 messages with one of the following values as

applicable, in addition to populating all other required data. The value of M1XX means "Merchant-initiated recurring payment or installment" and the value of M2XX means "Merchant-initiated industry practice." When populated in an Authorization Request/0100 message, the same value may also be provided in the First Presentment/1240 message.

Table 32: Authorization Request/0100 and Financial Transaction Request/0200 Messages

Data Element/ Subelement	Value	Use this value when...	Examples
DE 48, subelement 22 (Multi-purpose Merchant Indicator), subfield 5 (Cardholder/Merchant Initiated Transaction Indicator)	M101 (Unscheduled Credential-on-file)	The Cardholder has expressly authorized the Merchant to store the Cardholder's Account data for subsequent use in connection with one or more later Transaction(s) with that Merchant (a "COF arrangement").	The Merchant initiates a Transaction to "topup" the Cardholder's tollway account based on a prearranged reload schedule.
	M102 (Standing Order [variable amount/fixed frequency])	The Cardholder has expressly authorized a COF arrangement with the Merchant for a series of recurring payments of **variable amount and fixed frequency**.	The Merchant initiates a Transaction for the Cardholder's next monthly utility payment.
	M103 (Subscription [fixed amount/fixed frequency])	The Cardholder has expressly authorized a COF arrangement with the Merchant for a series of recurring payments of **fixed amount and fixed frequency**, which may include an allowance for price changes to occur from time to time.	The Merchant initiates a Transaction for the Cardholder's next quarterly newspaper subscription payment.

Data Element/ Subelement	Value	Use this value when...	Examples
	M104 (Installment)	The Cardholder has expressly authorized a COF arrangement for an installment billing plan relating to a single purchase of goods or services with a known amount and set frequency over a specified duration.	The Merchant initiates a Transaction for the Cardholder's next biweekly installment payment for the purchase of a television.
	M205 (Partial Shipment)	One or more items in the Cardholder's purchase order was out of stock at the time that the Cardholder initiated payment. The Merchant initiates a separate Transaction for the remaining items when ready to be shipped.	The Cardholder originally ordered a hat and sunglasses, but the hat was out of stock. The Cardholder completes the purchase of the sunglasses and agrees to wait for the hat to be restocked. The Merchant initiates a partial shipment Transaction for the hat when back in stock.
	M206 (Related/Delayed Charge)	After completing a payment, the Cardholder owes an additional amount to the Merchant based on the original Transaction terms.	The Merchant initiates a related/delayed charge Transaction for mini-bar charges after the Cardholder has checked out of the hotel.
	M207 (No-show)	Under the Merchant's guaranteed reservation service policy, the Cardholder owes a no-show fee.	The Merchant initiates a Transaction to collect a no-show fee when the Cardholder does not cancel a guaranteed reservation within the previously disclosed cancellation time frame.

Data Element/ Subelement	Value	Use this value when...	Examples
	M208 (Resubmission)	The Merchant's previous attempt to obtain authorization for a Transaction was declined but the Issuer's response does not prohibit the Merchant from trying again later.	• The Merchant initiates an authorization request after receiving a previous "insufficient funds/ over credit limit" response. • The Merchant initiates a transit debt recovery Transaction.

Table 33: First Presentment/1240 Message

Data Element/PDS	Value
PDS 0218 (Cardholder/Merchant Initiated Transaction Indicator)	One of the following: • M101 (Unscheduled Credential-on-file) • M102 (Standing Order [variable amount/fixed frequency]) • M103 (Subscription [fixed amount/fixed frequency]) • M104 (Installment) • M205 (Partial Shipment) • M206 (Related/Delayed Charge) • M207 (No-show) • M208 (Resubmission) Refer to Table 30 for usage information.

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....302
CAT Level Requirements....302
Dual Capability for CAT 1 and CAT 2....303
CAT Level 1: Automated Dispensing Machines (CAT 1)....303
CAT Level 2: Self-Service Terminal (CAT 2)....304
CAT Level 3: Limited Amount Terminals (CAT 3)....305
CAT Level 4: In-Flight Commerce (IFC) Terminals (CAT 4)....306
CAT Level 6: Electronic Commerce Transactions (CAT 6)....309
CAT Level 7: Transponder Transactions (CAT 7)....309
CAT Level 9: Mobile POS (MPOS) Acceptance Device Transactions (CAT 9)....310

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)
- **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) that has dual capability as a CAT 1 and CAT 2 device should:

- For Mastercard, Debit Mastercard, and Maestro Transactions, 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 Mastercard or Debit Mastercard magnetic stripe Card is used or a Mastercard, Debit Mastercard, or Maestro Contactless Transaction occurs for an amount equal to or less than the applicable contactless CVM limit.

For Mastercard and Debit Mastercard Transactions, a PIN-capable Hybrid POS Terminal identified with MCC 5542 that is located outside of the U.S. Region and:

- Supports offline PIN but not online PIN, may function as a CAT 2 device when a U.S. Region-issued Chip Card that supports online PIN but not offline PIN is used; or
- If online PIN is supported, may function as a CAT 1 device without dual capability as a CAT 2 device.

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. When PIN is present, 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 support "No CVM" as the CVM.
2. CAT 3 devices may support offline PIN CVM for Contact Chip Transactions, in accordance with the security requirements for PIN and key management.

3. CAT 3 devices must not support 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 SAR and Macao SAR 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.

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 22210000 to 27209999 or 51000000 to 55999999.
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 or electronic 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 Appendix C 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 support "No CVM" as the CVM.
2. CAT 7 devices must not support signature CVM or PIN CVM (online or offline).

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 and Transit Limits

This appendix specifies Contactless Transaction and Contactless transit aggregated Transaction CVM limit amounts and transit First Ride Risk limits.

Overview 312
CVM and Transit Limits 312

Overview

This appendix presents information on Contactless and Contactless transit aggregated Transaction Cardholder Verification Method (CVM) limit Amounts and transit First Ride Risk limits. See Chapters 3 and 4 of the *Transaction Processing Rules* for more information.

CVM and Transit Limits

Prerequisite

These instructions are for the online version of *Transaction Processing Rules*. If you are reading this in the PDF version, go to the Technical Resource Center on Mastercard Connect® and open the document from there.

Procedure

To access the CVM and Transit Limits Microsoft® Excel® spreadsheet, following the steps in this section.

IMPORTANT: The CVM and Transit Limits spreadsheet is large. So before you print it, be aware that depending on your printer settings and paper selection, the printed spreadsheet may exceed 250 pages.

To download the spreadsheet only, follow these steps.

1. In the icon group to the right of the section title, select **Download Attachments** (the paperclip icon).
2. In the **Attachments** window, select the `cvm_and_transit_limits_month_year.xlsx` file.

   The file is downloaded to your local computer.

To download the spreadsheet as part of a zip file, follow these steps.

1. In the icon group to the right of the section title, select **Download PDF** (the PDF page icon).
2. Select **Save all topics and attachments**.

   A zip file that contains the spreadsheet and the English and translated versions of the *Transaction Processing Rules* document is downloaded to your local computer.
3. To access the spreadsheet, unzip the file.

Appendix F Digital Goods and Lodging Merchant Services

This appendix contains best practices for Merchants conducting sales of Digital Goods and information about the Mastercard Guaranteed Reservation Program for lodging Merchants.

Digital Goods Purchases....314
Guaranteed Reservations....315
Advance Resort Deposit....316

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.

Guaranteed Reservations

All lodging Merchants who accept Mastercard are automatically enrolled in the Guaranteed Reservation Program. Lodging Merchants are not required to process Guaranteed Reservation transactions; however, each Merchant has the ability to create Guaranteed Reservation (No-Show) transactions.

When a Cardholder guarantees their reservation with a Mastercard, the Merchant is ensuring that a room will be available for the Cardholder when the Cardholder arrives at the property. Merchants have the following responsibilities when accepting a Guaranteed Reservation:

- The Merchant must keep a room available until check-out time on the day following the reservation.
- When accepting the Card as a guarantee, the Merchant will provide the Cardholder with a confirmation number for the reservation.
- The Merchant must inform the Cardholder of the cancellation time and conditions. Merchants may set cancellation limits up to 72 hours prior to the stay. When the Cardholder makes a reservation within the Merchant's cancellation period (for example, the Cardholder makes a reservation 24 hours in advance when the Merchant has a 48-hour cancellation requirement) the Merchant agrees the default time of cancellation for that reservation will be 18:00 Merchant local time.
- Merchants must accept a cancellation from the Cardholder when provided prior to the agreed upon time frames. Upon acceptance of the cancellation, the Merchant will provide a cancellation number.
- Cardholders who cancel beyond the cancellation policy may be billed for one night of room and tax only.
- No-show transactions must be authorized prior to billing. A no-show Transaction authorization request must be identified with a Merchant-initiated Transaction (MIT) value of M207 (No Show Charge) in DE 48 (Additional Data: Private Use), subelement 22 (Multi-Purpose Merchant Indicator), subfield 5 (Cardholder/Merchant Initiated Transaction Indicator).

In the event the Merchant is unable to provide a room to a Cardholder who guaranteed the stay with a Mastercard, the Merchant must do all the following:

- Not bill the Cardholder a no-show charge
- Provide the Cardholder with an option to take accommodations at a lodging establishment rated equal to, or better than, the reserved property
- Ensure the Cardholder is not charged more than the rate of the guaranteed stay
- Receive complimentary transportation to the new location, and
- A complimentary call when necessary for the Cardholder to inform others of the new location.

Merchants billing no-show Transactions are advised to keep notation that the Transaction was a no-show in the event of a chargeback.

Should a Cardholder dispute a no-show charge for any reason other than as an unauthorized Transaction, the Merchant may support their cancellation policy and no-show billing only with documentation verifying the Cardholder received the cancellation policy and failed to adhere to it.

Advance Resort Deposit

A Merchant participating in the Advance Resort Deposit service must follow these procedures:

1. Explain the terms of the advance resort deposit reservation to the Cardholder, including the cancellation and refunds policies. **A "no refund" policy must be clearly disclosed to the Cardholder.**
2. Request the card account and Cardholder address information and confirm the room rate and location.
3. Obtain authorization from the Issuer and include on the TID the reservation confirmation number and the words "advance deposit" in place of the Cardholder's signature. The Merchant is recommended to note on the TID any special terms and conditions regarding its cancellation and refund policy.
4. Provide confirmation, a copy of the TID (including the reservation confirmation number), and information concerning its cancellation and refund policies (including a "no refund" policy, when applicable) to the Cardholder. This information must be provided by letter, email, fax, or other message.
5. If a Cardholder cancels his or her reservation in accordance with the agreed upon procedures, the Merchant must follow the cancellation and refund policy previously disclosed to the Cardholder.

Appendix G 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 319
Models for ATM Access Fee Notification at ATM Terminals 320
Models for Standard Signage Notification of an ATM Access Fee 320
Asia/Pacific Region 320
Australia 321
Canada Region 321
Europe Region 322
United Kingdom 323
Latin America and the Caribbean Region 323
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela 324
Middle East/Africa Region 325
United States Region 326
Models for Generic Terminal Signage Notification of an ATM Access Fee 327
Asia/Pacific Region 327
Australia 327
Canada Region 328
Europe Region 329
United Kingdom 329
Latin America and the Caribbean Region 330
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela 331
Middle East/Africa Region 332
United States Region 332
Models for Screen Display Notification of an ATM Access Fee 333
Asia/Pacific Region 333
Australia 334
Canada Region 335
Europe Region 335
United Kingdom 336
Latin America and the Caribbean Region 337
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela 337

Middle East/Africa Region....338
United States Region....339
Model for an ATM Access Fee Transaction Receipt....340
Model Screen Offering POI Currency Conversion....340
Model Receipt for Withdrawal Completed with POI Currency Conversion....341
Model Screen Displays for Offering Installment Payments....342
Model Receipt Texts for Installments....352

Screen and Receipt Text Standards

Response Code	Recommended Screen Text	Recommended Receipt Text
• Format error • Invalid acquirer • Cardholder not on file • Do not honor/Restricted card • Unable to process/System error • ATM processor inoperative • Cardholder processor inoperative/Not found	"I am sorry. I am unable to process your request. Please contact your financial institution."	"Denied Unable to Process"
• Invalid transaction • Invalid transaction selection	"I am sorry. You have selected an invalid transaction. Do you want to try another transaction?"	"Denied Invalid Transaction"
• Invalid amount	"You have selected an invalid amount. Please select an amount in multiples of _____."	"Denied Invalid Amount"
• Insufficient funds	"I am unable to process for insufficient funds. Please contact your financial institution."	"Denied Insufficient Funds"
• Invalid PIN	"You have entered your PIN incorrectly. Do you want to try again?"	"Denied Invalid PIN"
• PIN tries exceed permitted number of attempts	"You have exceeded the number of attempts permitted to enter your PIN. Please contact your financial institution."	"Denied Invalid PIN"
• Exceeds withdrawal limit	"You have exceeded the withdrawal limit. Do you want to select another amount?"	"Denied Invalid Amount"
• Denied—Capture card	"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.

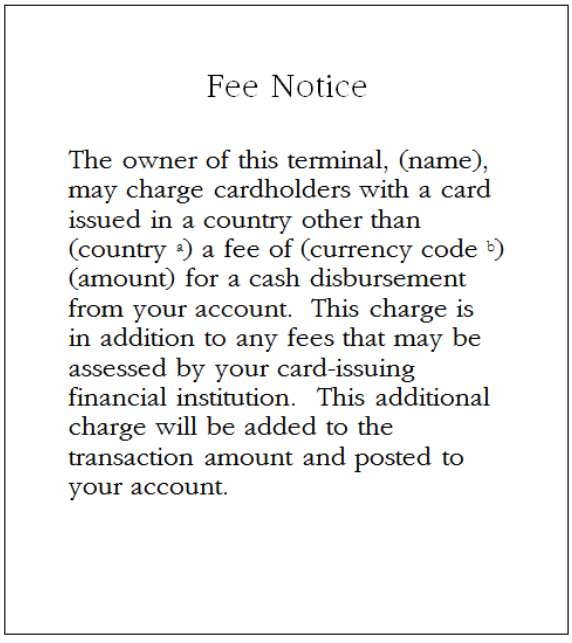
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type
Body text	Must be at least 14 point type

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

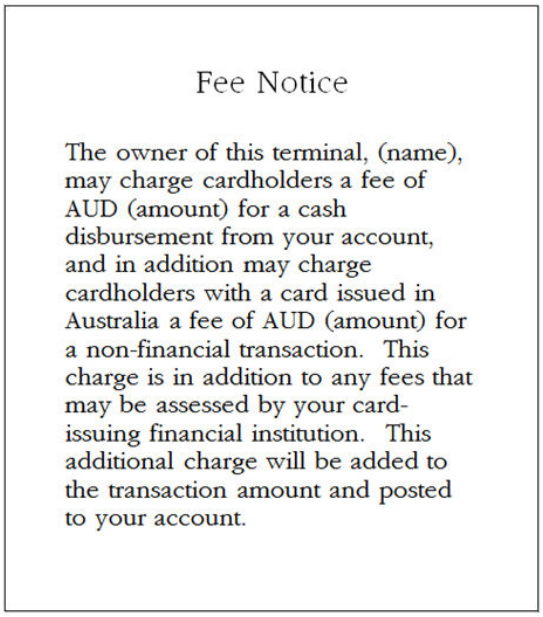
The owner of this terminal, (name), may charge cardholders with a card issued in a country other than (country [a]) a fee of (currency code [b]) (amount) for a cash disbursement from your account. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. 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.

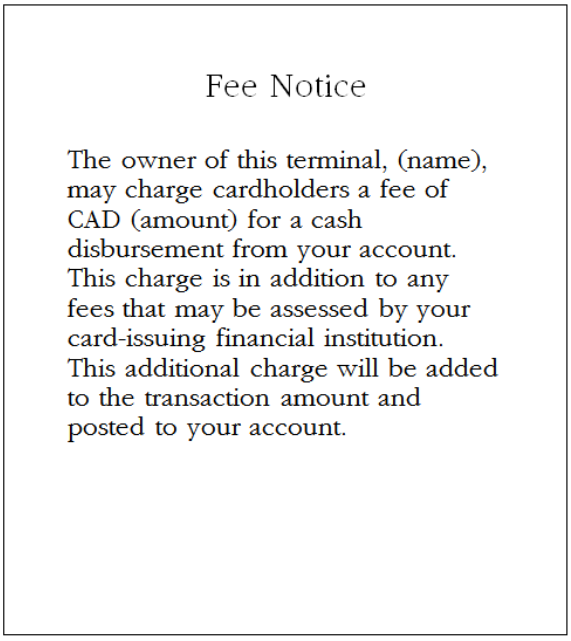
Australia

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for Australia only.



Canada Region

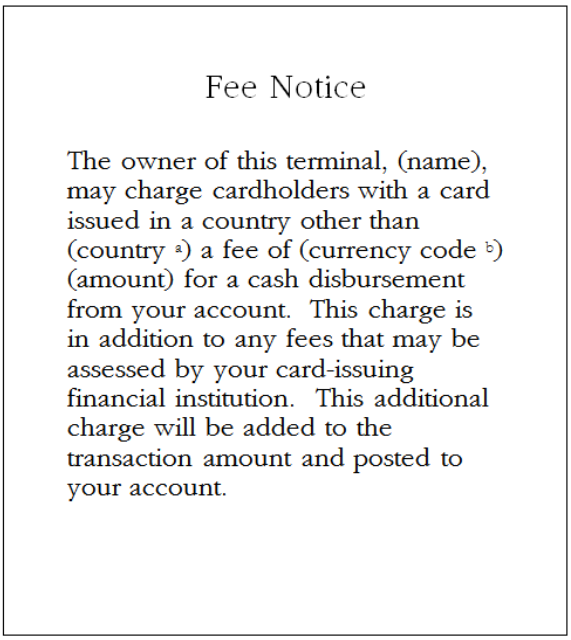
The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Canada Region only.


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

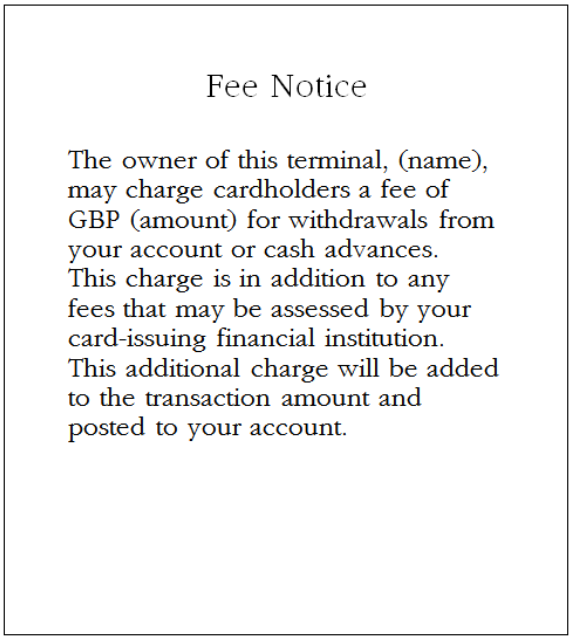
The owner of this terminal, (name), may charge cardholders with a card issued in a country other than (country [a]) a fee of (currency code [b]) (amount) for a cash disbursement from your account. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. 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.

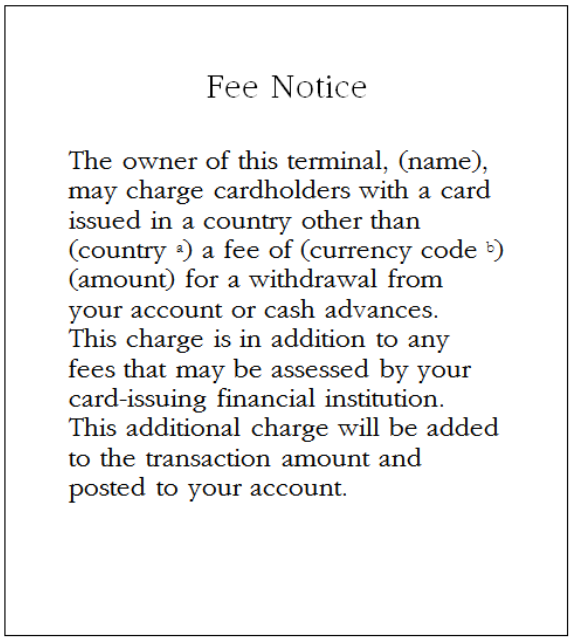
United Kingdom

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the United Kingdom only.



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.

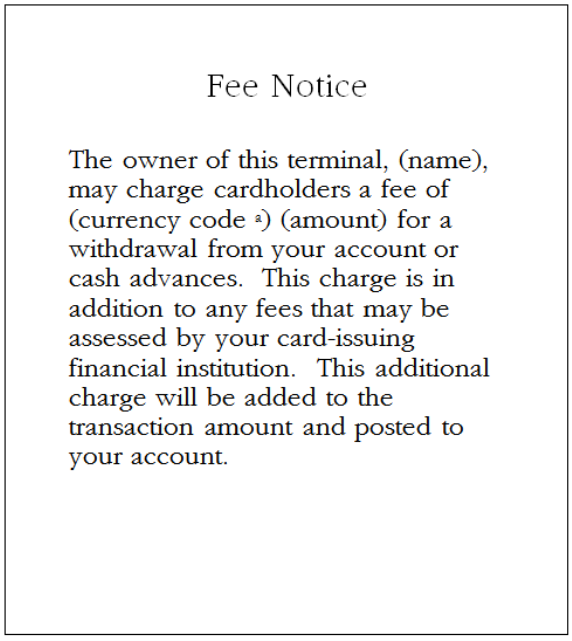


a Insert country where ATM is located.

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.

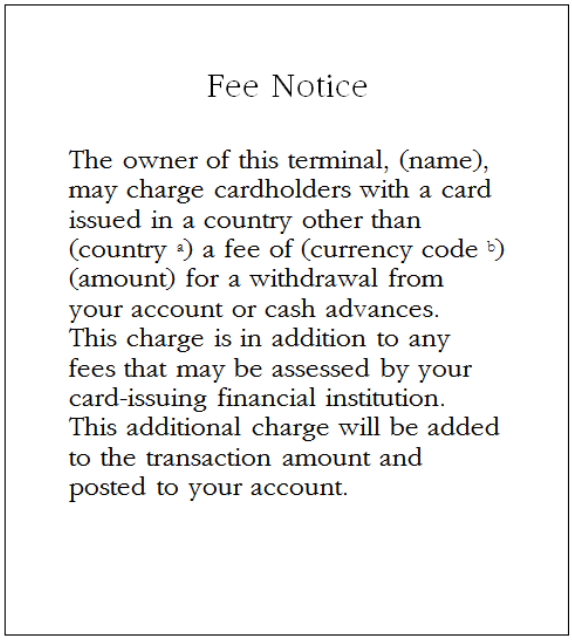

Fee Notice

The owner of this terminal, (name), may charge cardholders a fee of (currency code [a]) (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 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

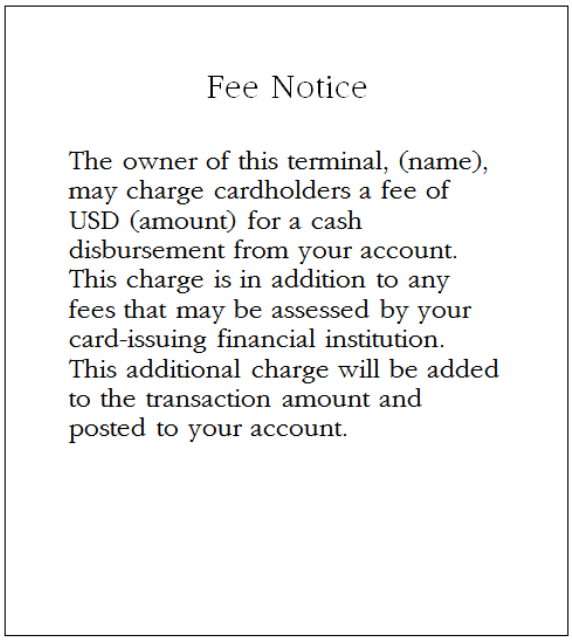
The owner of this terminal, (name), may charge cardholders with a card issued in a country other than (country [a]) a fee of (currency code [b]) (amount) for a withdrawal from your account or cash advances. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. 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.

United States Region

The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the United States only.


Fee Notice

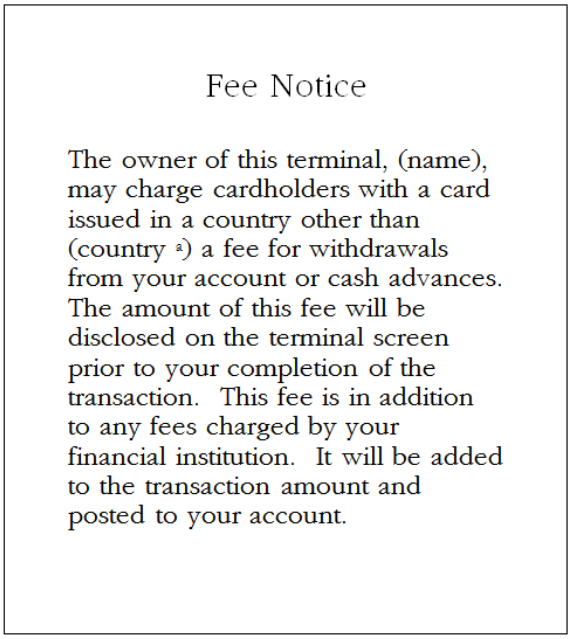
The owner of this terminal, (name), may charge cardholders a fee of USD (amount) for a cash disbursement from your account. This charge is in addition to any fees that may be assessed by your card-issuing financial institution. This additional charge will be added to the transaction amount and posted 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

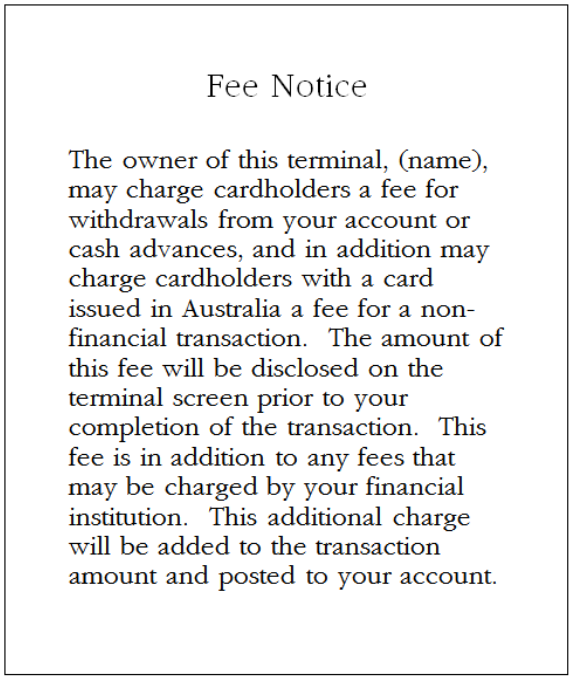
The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Asia/Pacific Region, except Australia.



a Insert country where ATM is located.

Australia

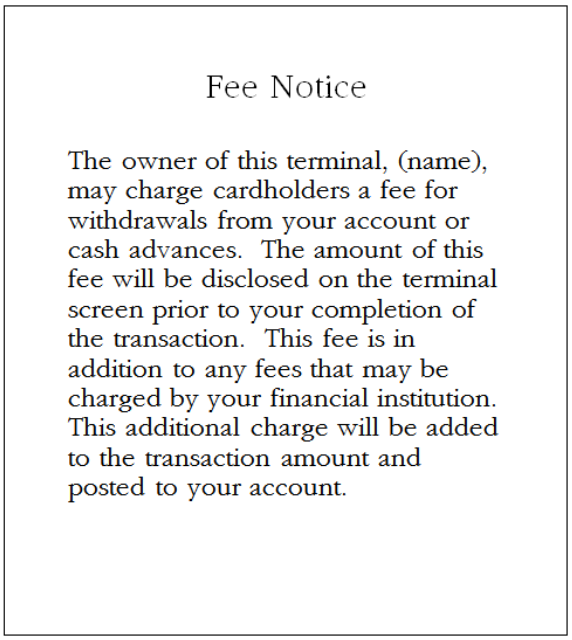
The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for Australia only.


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

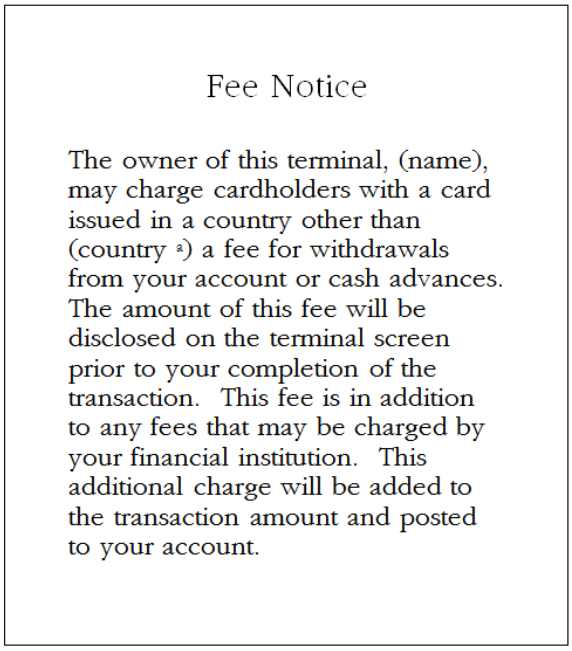
The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Canada Region only.


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

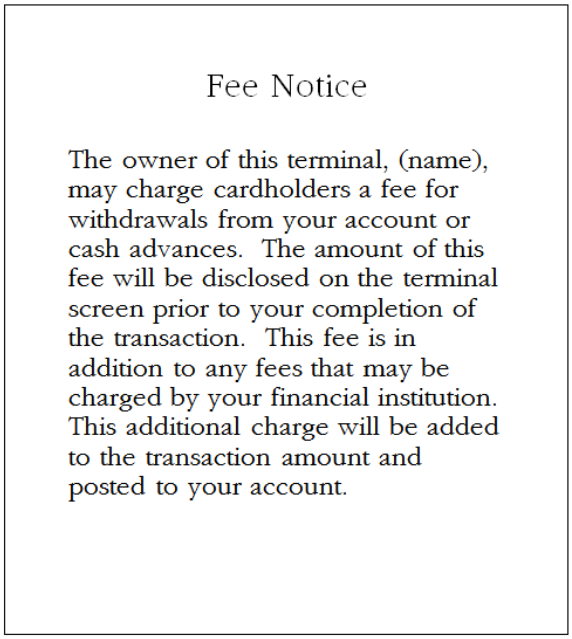
The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Europe Region only, except the United Kingdom.



a Insert country where ATM is located.

United Kingdom

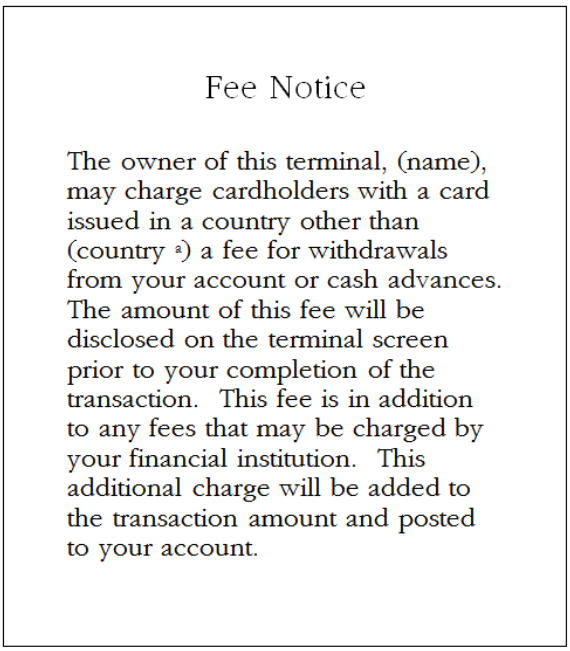
The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the United Kingdom only.



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.

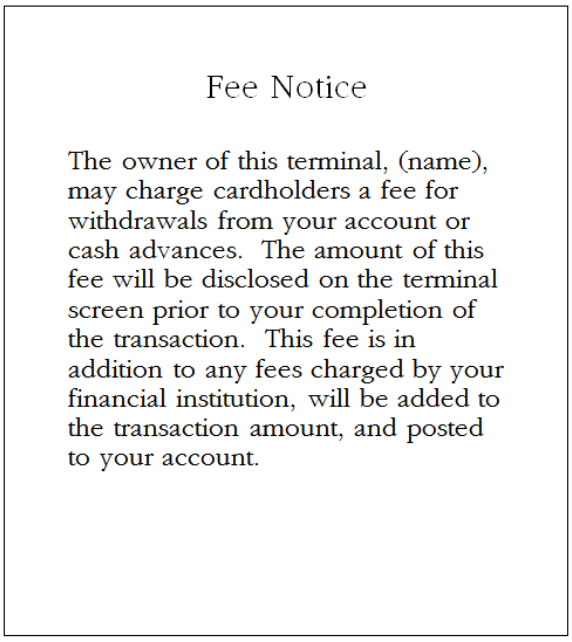
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



a Insert country where ATM is located.

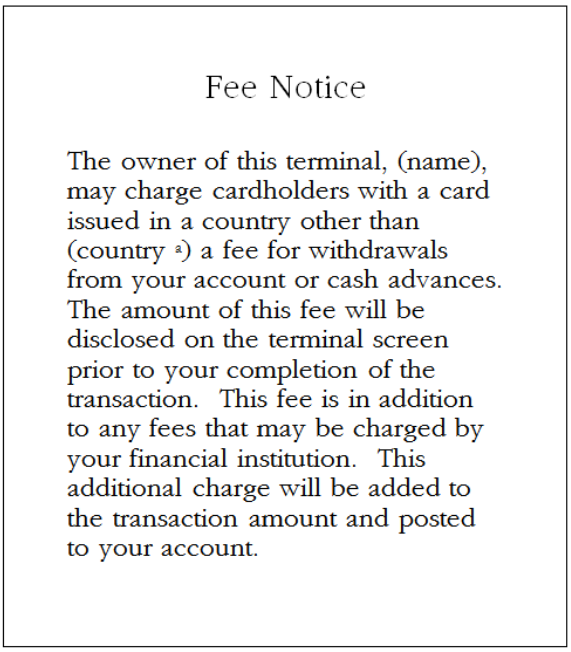
Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela

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.



Middle East/Africa Region

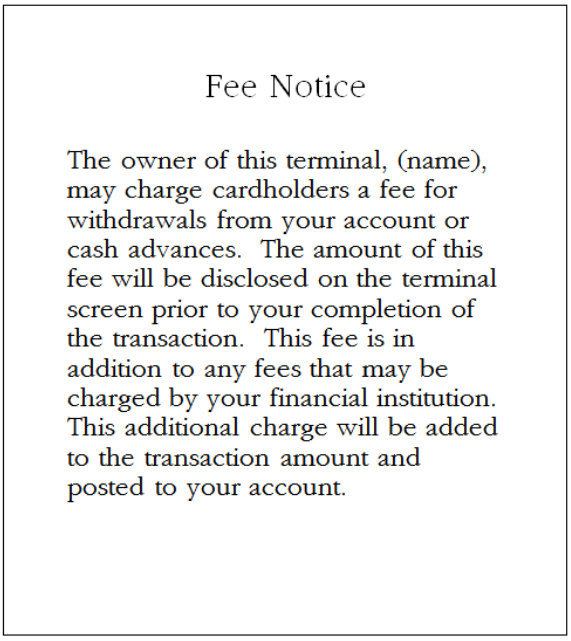
The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for the Middle East/Africa Region.



a 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.



a Insert country where ATM is located.

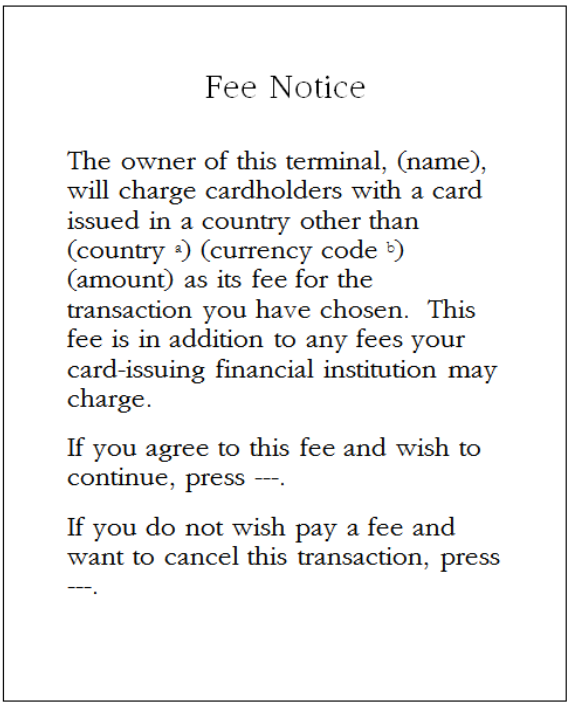
b Insert currency code for the country where the ATM is located.

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 [a]) (currency code [b]) (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 ---.

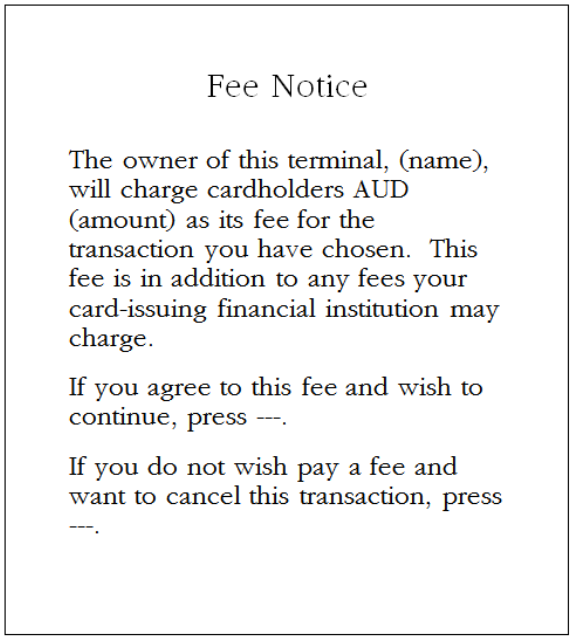
If you do not wish pay a fee and want to cancel this transaction, press ---.

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

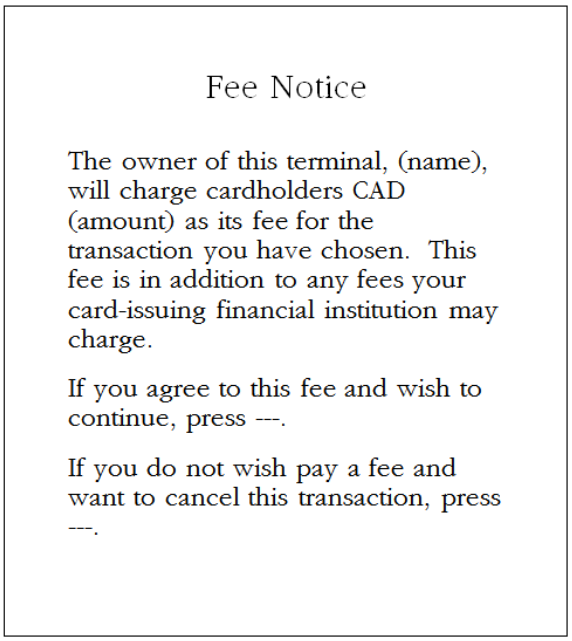
The owner of this terminal, (name), will charge cardholders AUD (amount) as its fee for the transaction you have chosen. This fee is in addition to any fees your card-issuing financial institution may charge.

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

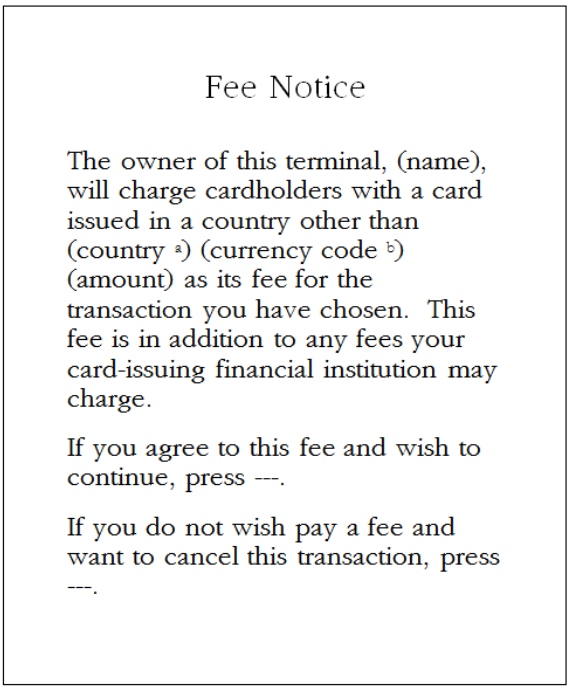
The owner of this terminal, (name), will charge cardholders CAD (amount) as its fee for the transaction you have chosen. This fee is in addition to any fees your card-issuing financial institution may charge.

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 [a]) (currency code [b]) (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 ---.

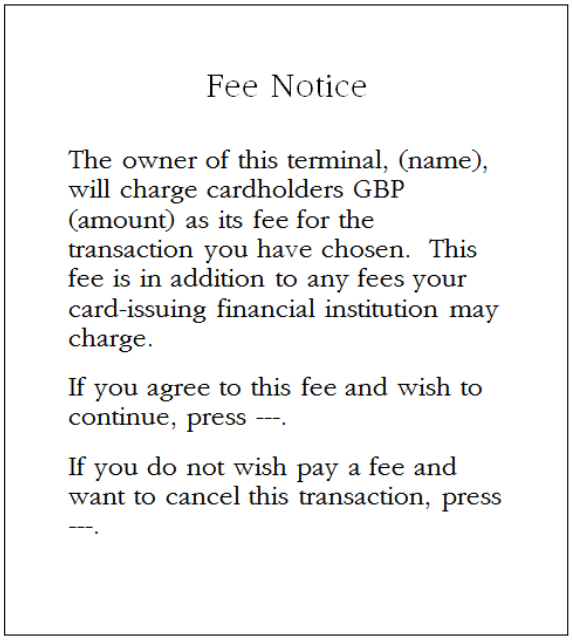
If you do not wish pay a fee and want to cancel this transaction, press ---.

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

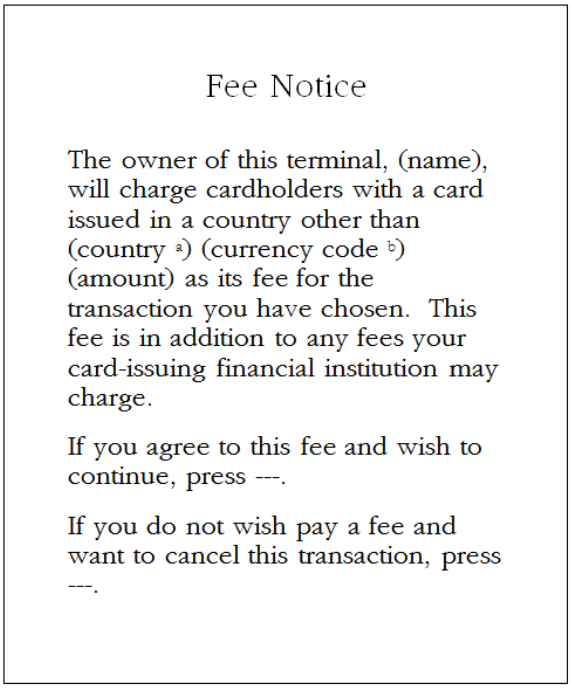
The owner of this terminal, (name), will charge cardholders GBP (amount) as its fee for the transaction you have chosen. This fee is in addition to any fees your card-issuing financial institution may charge.

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 [a]) (currency code [b]) (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 ---.

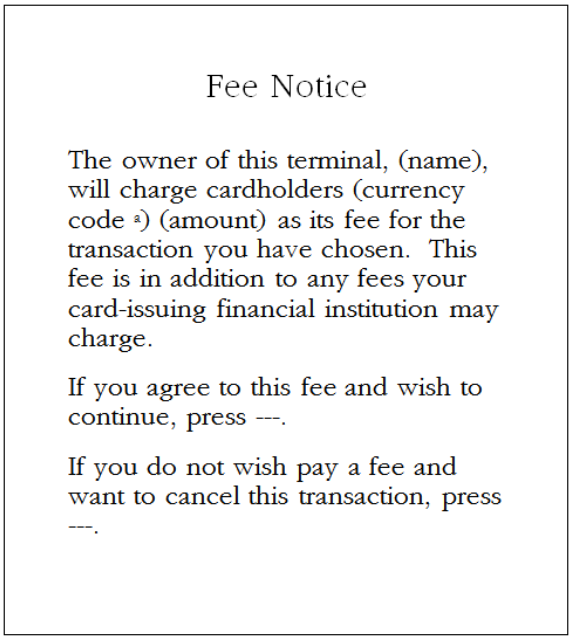
If you do not wish pay a fee and want to cancel this transaction, press ---.

a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela

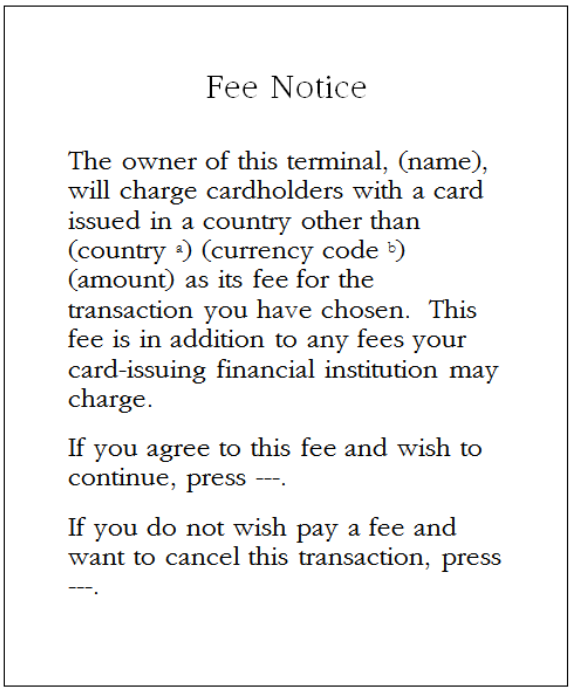
The following model form illustrates ATM Terminal signage notification of an ATM Access Fee for only the following countries in the Latin America and the Caribbean Region: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela.



a 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 Veñezuela (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 [a]) (currency code [b]) (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 ---.

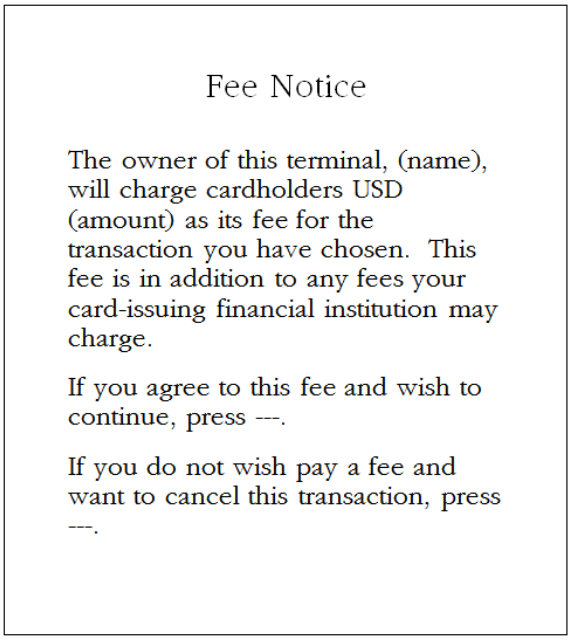
If you do not wish pay a fee and want to cancel this transaction, press ---.

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 Screen Offering POI Currency Conversion

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	EUR 64.38

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.

CHARGE MY ACCOUNT GBP 51.50 >>>
CHARGE MY ACCOUNT EUR 64.38 >>>

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

Figure 1: POS Terminal Displays in Hungarian

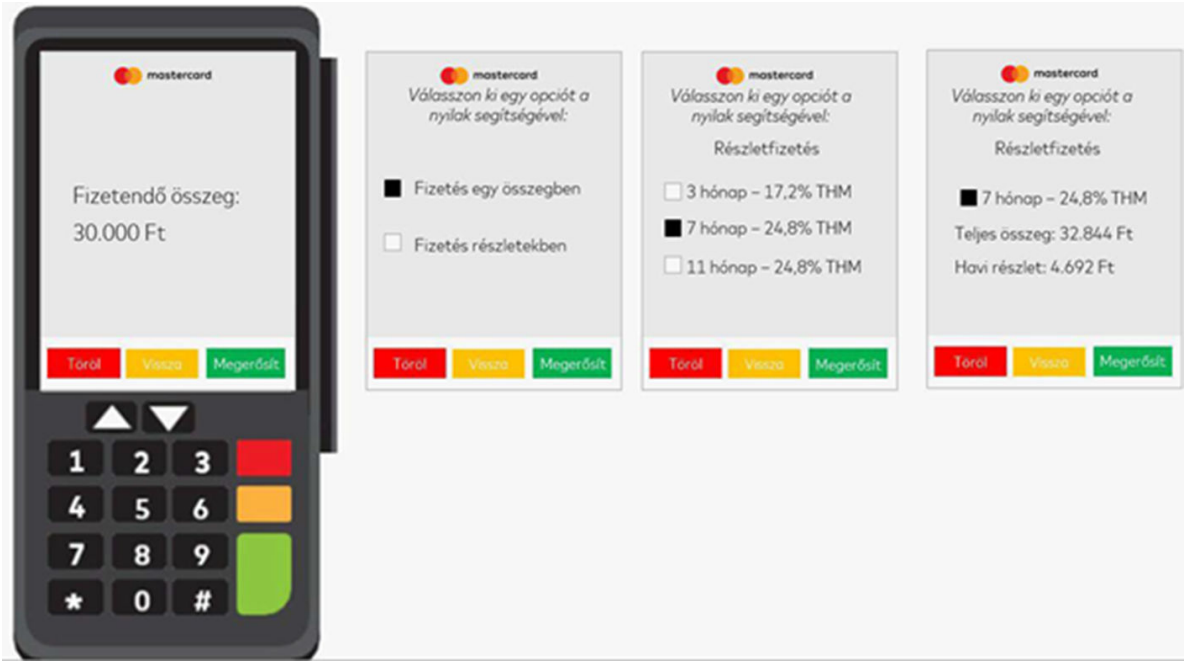
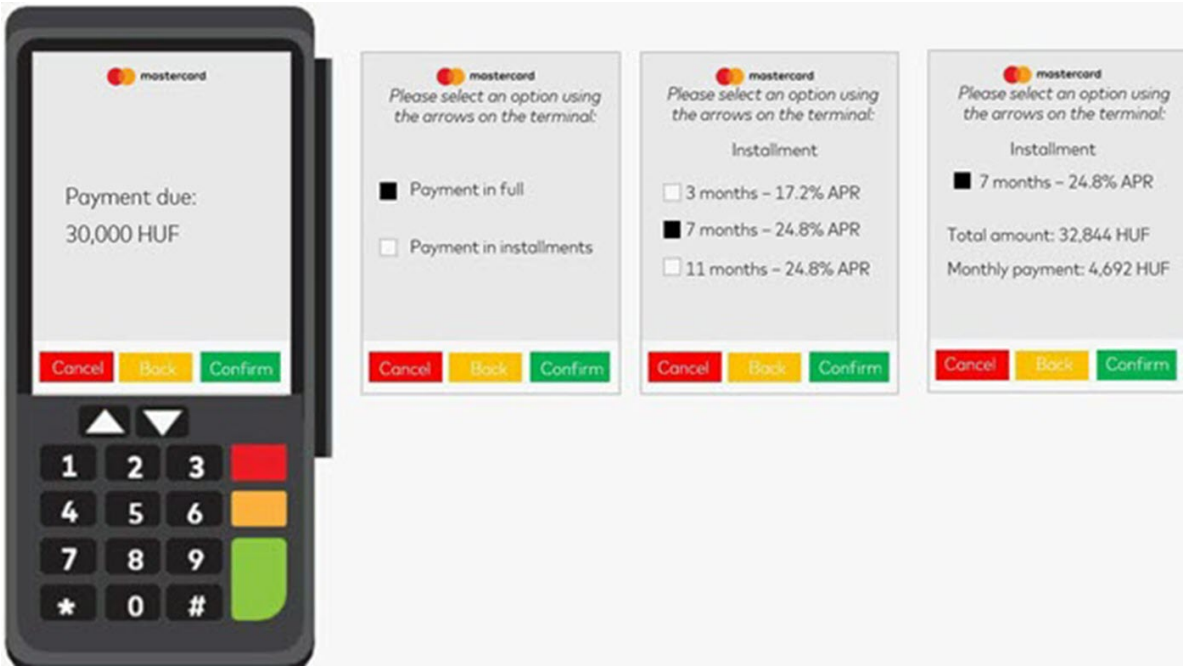


Figure 2: POS Terminal Displays in English



Poland

Figure 3: POS Terminal Display One in Polish

Figure 4: POS Terminal Display One in English

Figure 5: POS Terminal Display Two in Polish

Figure 6: POS Terminal Display Two in English

Figure 7: E-commerce Display One in Polish

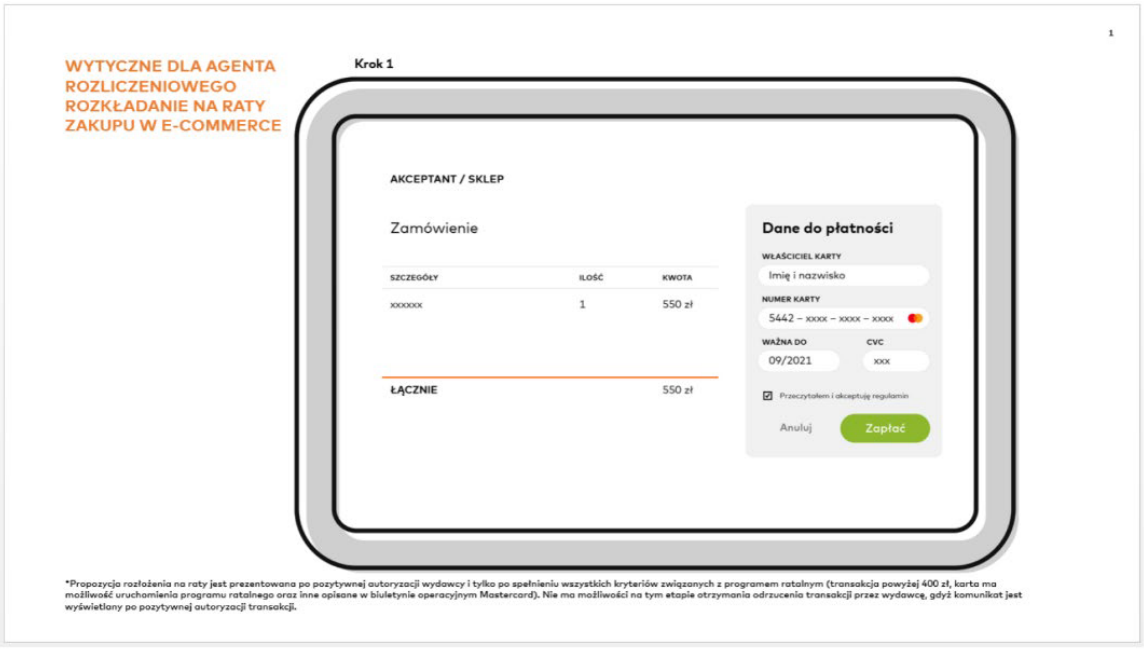


Figure 8: E-commerce Display Two in Polish

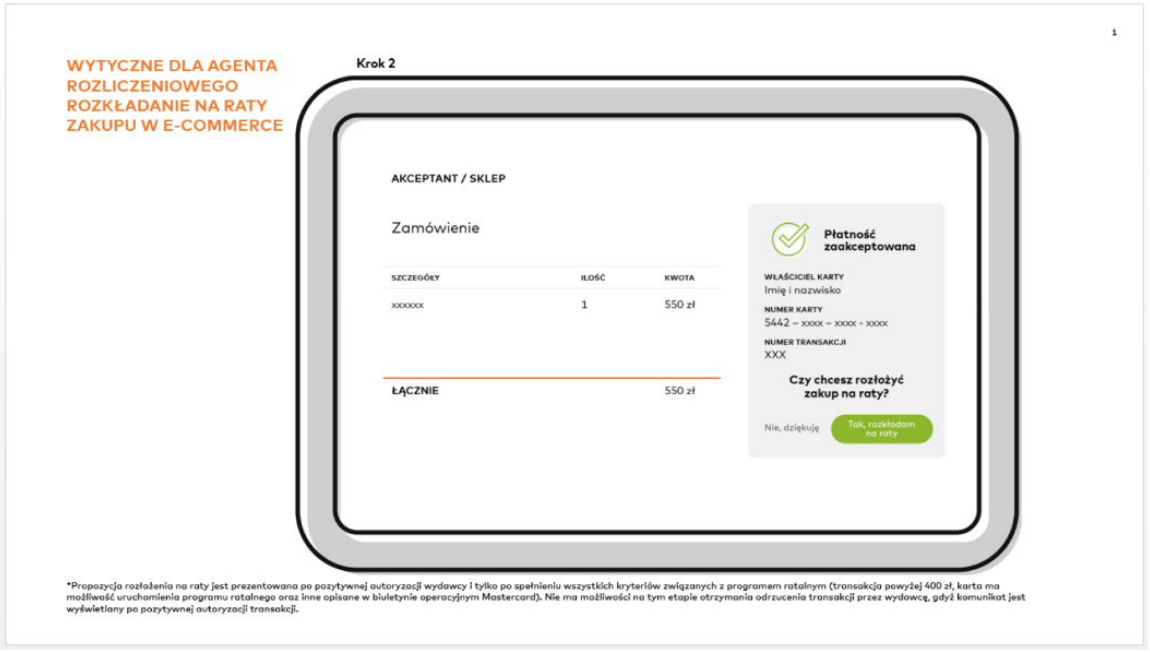


Figure 9: E-commerce Display Three in Polish

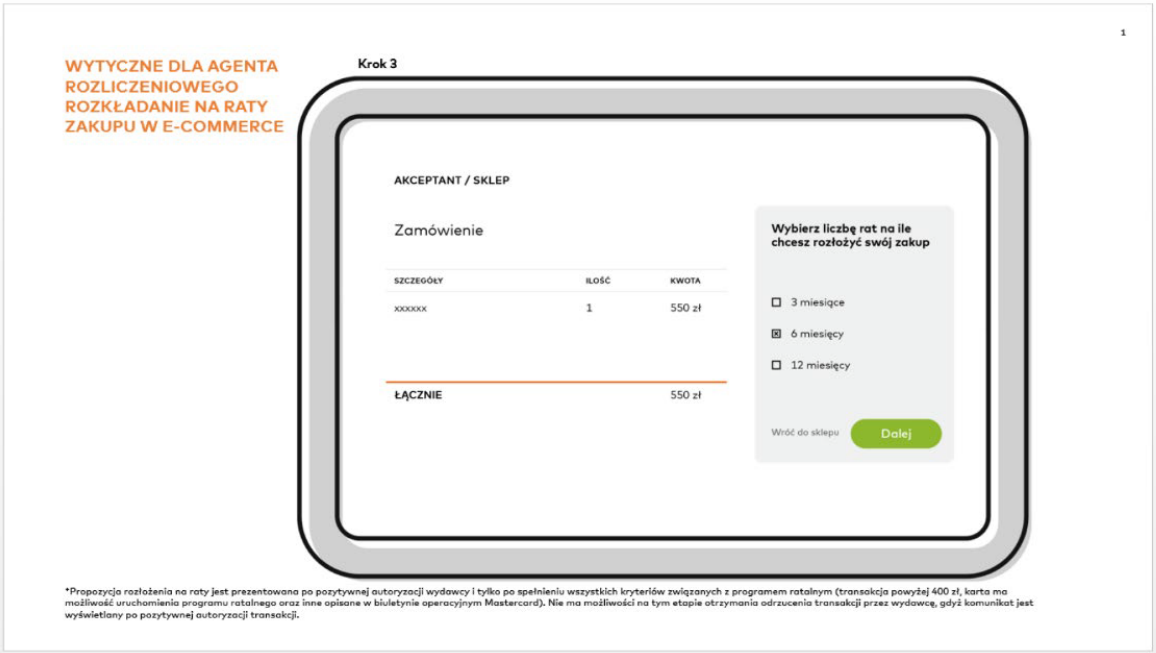


Figure 10: E-commerce Display Four in Polish

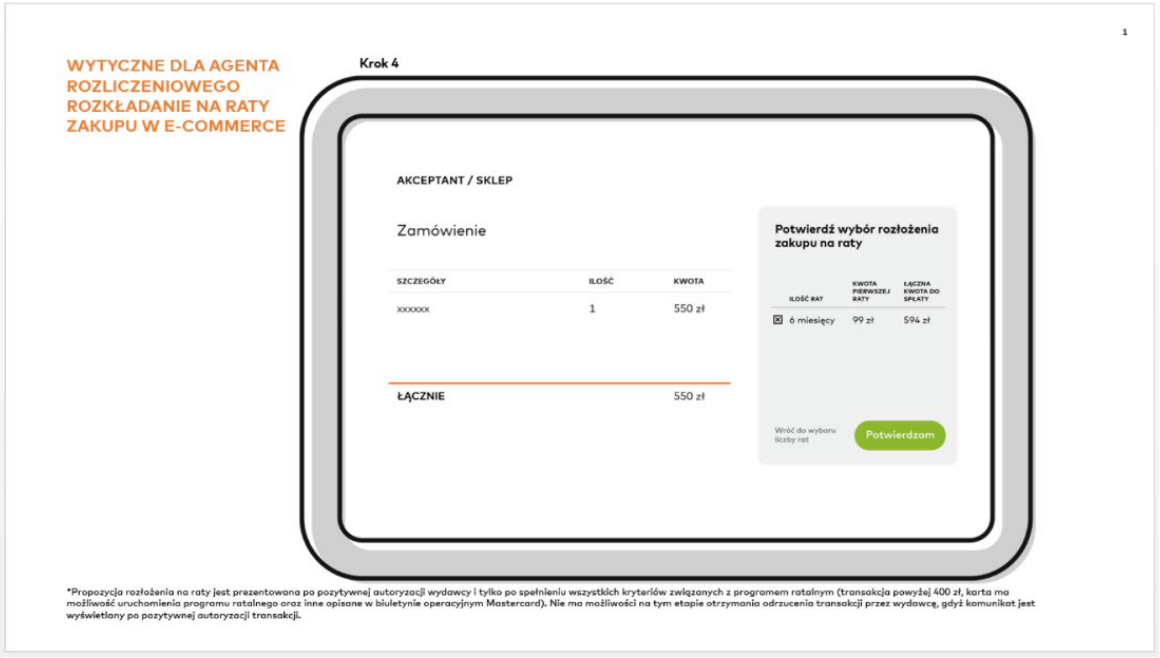


Figure 11: E-commerce Display Five in Polish

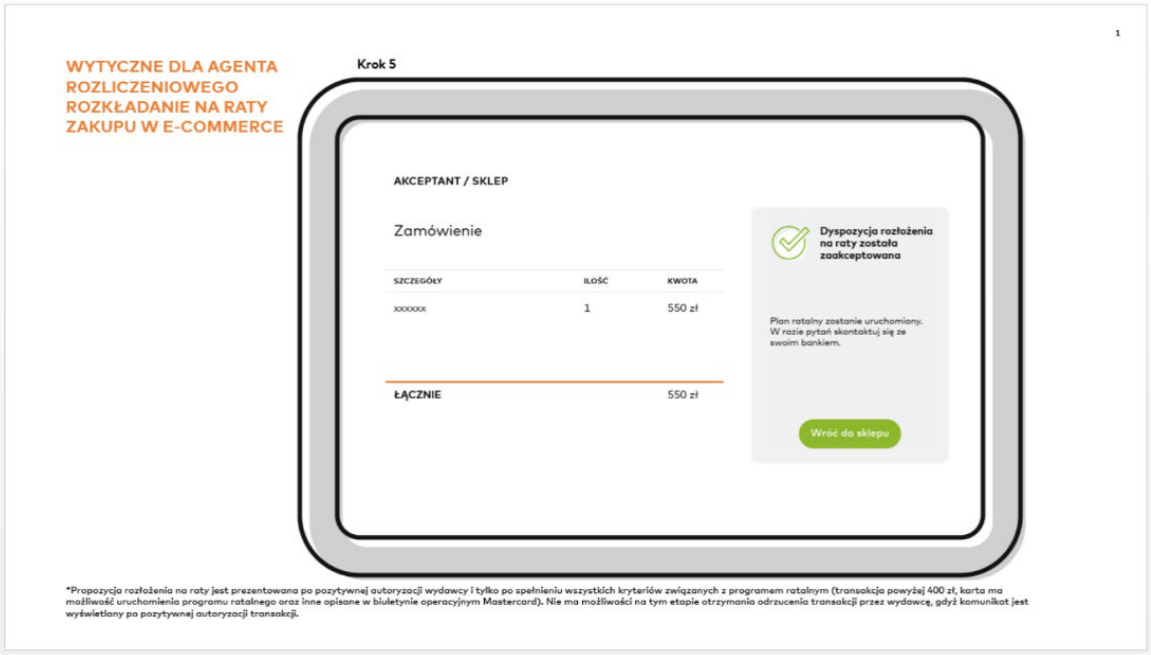


Figure 12: E-commerce Display One in English

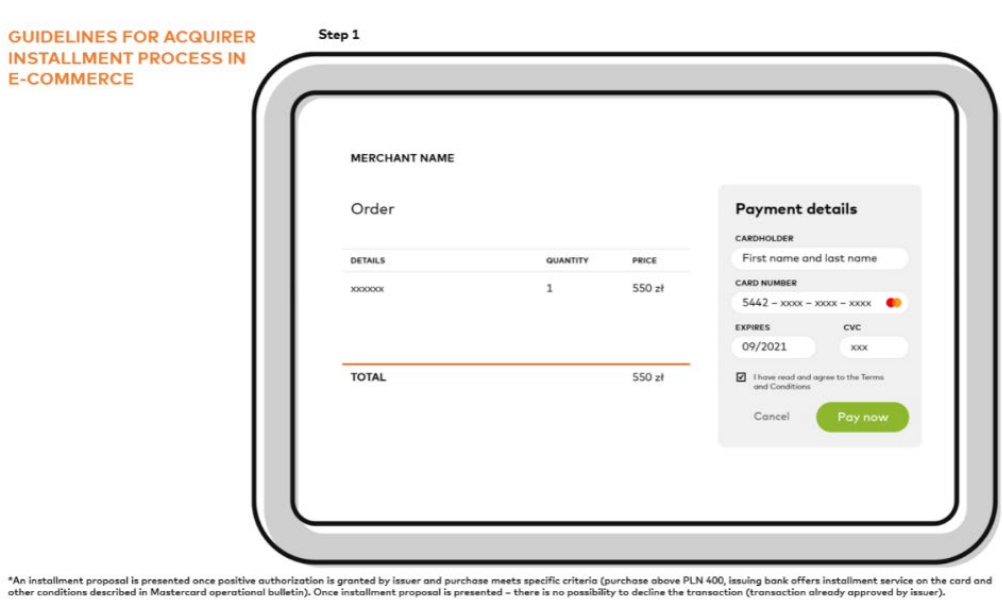


Figure 13: E-commerce Display Two in English

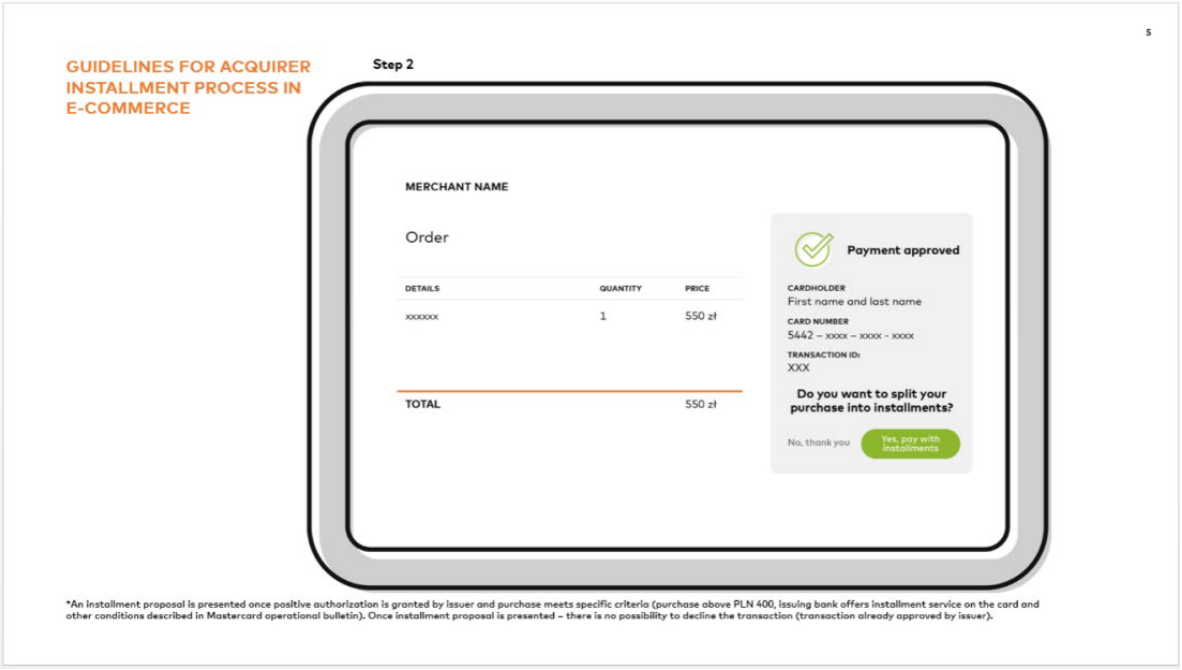


Figure 14: E-commerce Display Three in English

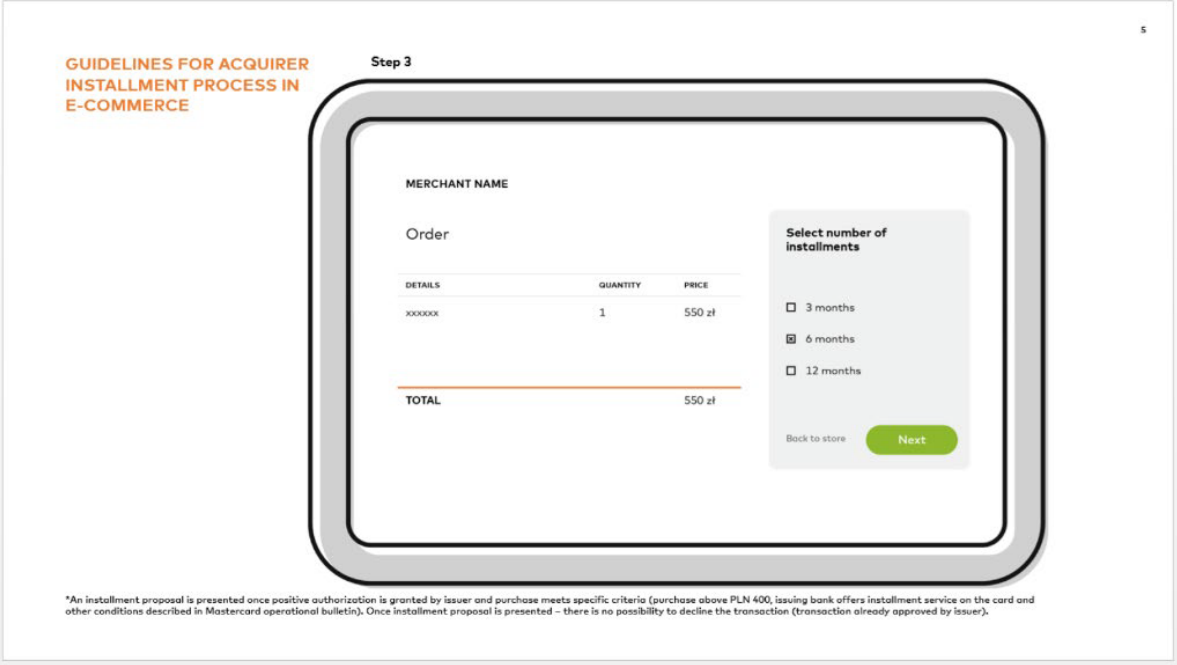


Figure 15: E-commerce Display Four in English

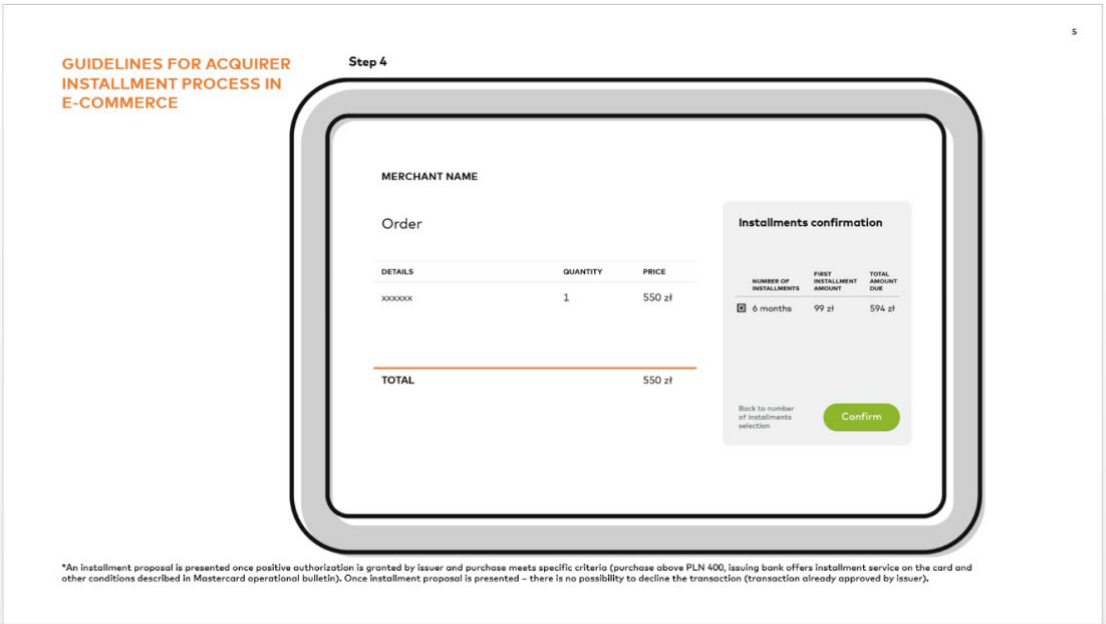
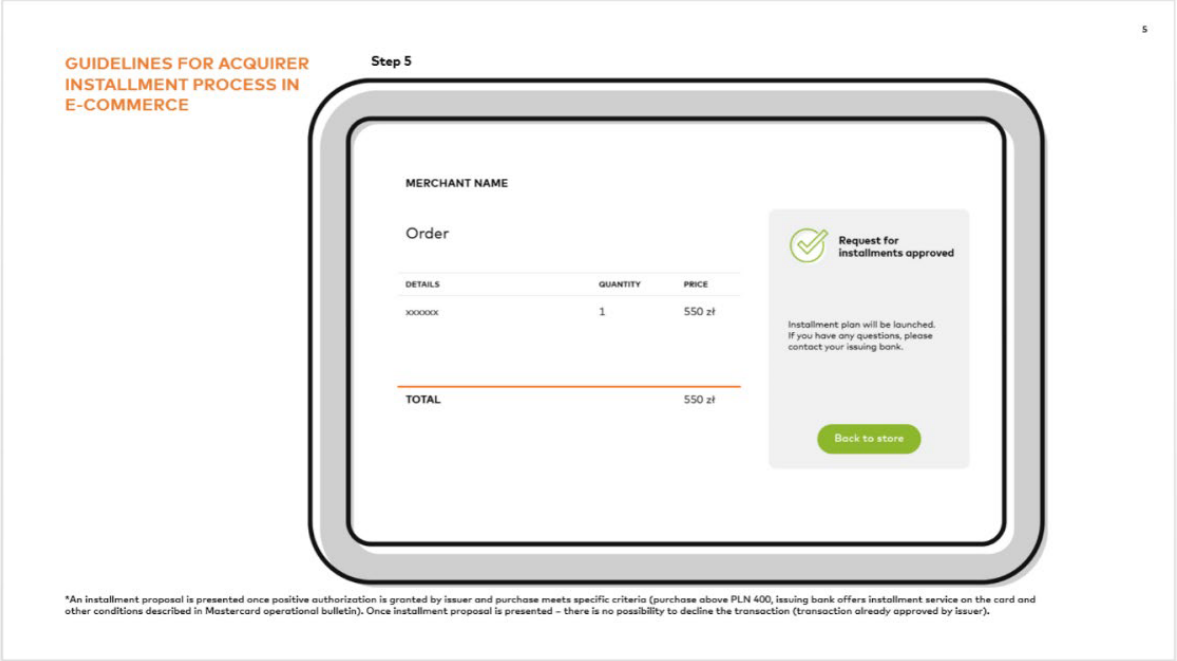


Figure 16: E-commerce Display Five in English



Ukraine

Figure 17: POS Terminal Displays in Ukrainian

Figure 18: POS Terminal Displays in English

Figure 19: E-commerce Displays in Ukrainian

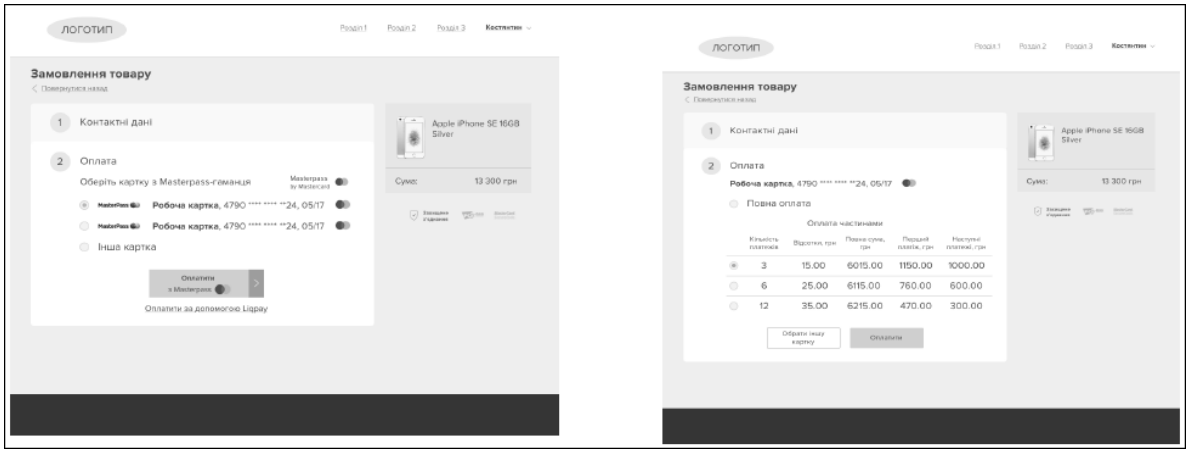
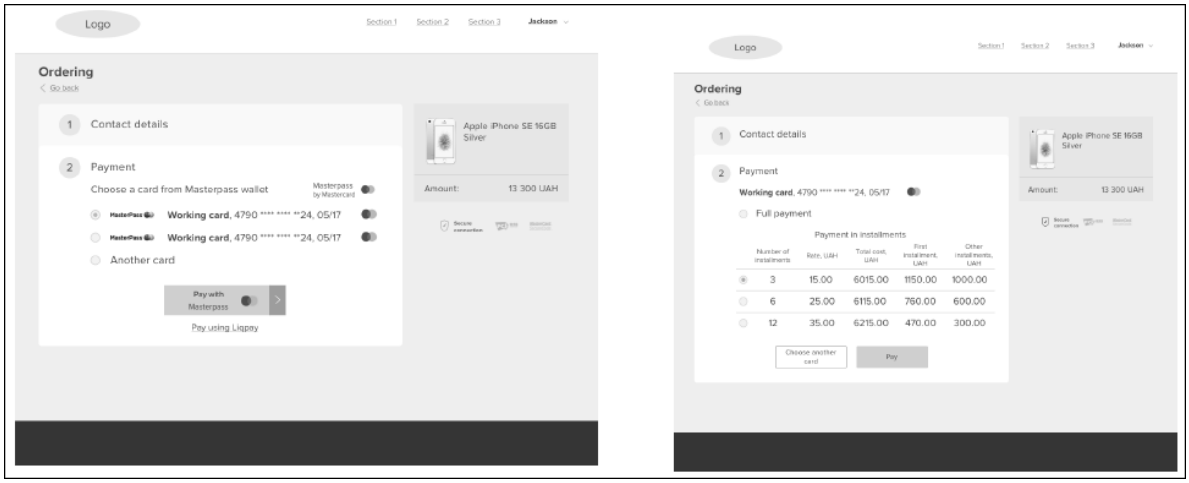


Figure 20: E-commerce Displays in English



Model Receipt Texts for Installments

Czech Republic

For Receipts in Czech	For Receipts in English
"Celkové náklady: XXXXXX CZK"	"Total cost: XXXXXXX CZK"
"Počet splátek: YY"	"Number of payments: YY"
"První splátek: XX CZK"	"First payment: XX CZK"
"Následující splátek: XX CZK"	"Subsequent payment: XX CZK"
"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: XXXXXX Ft" "Részletek száma': YY"	"Total amount: XXXXXXX HUF" "Number of payments: YY"
"Első Havi részlet: XX Ft"	"First Monthly payment: XX HUF"
"Havi részlet: XX Ft"	"Subsequent payment: XX HUF"
"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 ratalny 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: XXXXXXX ГРН»	"Total cost: XXXXXXX UAH"
«Кількість платежів: YY»	"Number of payments: YY"
«Перший платіж: XX ГРН»	"First payment: XX UAH"
«Наступні платежі: XX ГРН»	"Subsequent payment: XX UAH"
«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 website 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 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....360
Acceptor....360
Access Device....360
Account....360
Account Enablement System....361
Account Holder....361
Account PAN....361
Account PAN Range....361
Acquirer....361
Activity(ies)....361
Affiliate Customer, Affiliate....361
Area of Use....362
Association Customer, Association....362
ATM Access Fee....362
ATM Owner Agreement....362
Automated Teller Machine (ATM)....362
ATM Terminal....362
ATM Transaction....363
Bank Branch Terminal....363
BIN....363
Brand Fee....363
Brand Mark....363
Card....363
Cardholder....363
Cardholder Communication....364
Cardholder Verification Method (CVM)....364
Cardholder-initiated Transaction (CIT)....364
China Deposit Transaction....364
China Funds Transfer Funding Transaction....364
China Funds Transfer Payment Transaction....365
China Funds Transfer Request....365
China Funds Transfer Transaction....365
China Recurring Payment Transaction – Recurring Payment Terms....365

China Switch Manual Transaction....365
Chip Card (Smart Card, Integrated Circuit Card, IC Card, or ICC)....365
Chip Transaction....365
Chip-only MPOS Terminal....366
Cirrus Acceptance Mark....366
Cirrus Access Device....366
Cirrus Account....366
Cirrus Brand Mark....366
Cirrus Card....366
Cirrus Customer....367
Cirrus Payment Application....367
Cirrus Word Mark....367
Competing ATM Network....367
Competing International ATM Network....367
Competing EFT POS Network....367
Competing North American ATM Network....368
Consumer Device Cardholder Verification Method, Consumer Device CVM, CDCVM....368
Contact Chip Transaction....368
Contactless Payment Device....368
Contactless Transaction....369
Control, Controlled....369
Corporation....369
Corporation System....369
Credential-on-file Transaction....369
Credentials Management System....370
Cross-border Transaction....370
Customer....370
Customer Report....370
Data Storage Entity (DSE)....370
Device Binding....370
Digital Activity(ies)....371
Digital Activity Agreement....371
Digital Activity Customer....371
Digital Activity Service Provider (DASP)....371
Digital Activity Sponsoring Customer....371
Digital Goods....371
Digital Wallet....371
Digital Wallet Operator (DWO)....372
Digital Wallet Operator (DWO) Security Incident, DWO Security Incident....372

Digital Wallet Operator Mark, DWO Mark 372
Digitization, Digitize 372
Domestic Transaction 372
Dual Interface 372
Electronic Money 373
Electronic Money Issuer 373
Electronic Money Institution 373
EMV Mode Contactless Transaction 373
Funding Transaction 373
Gaming Payment Transaction 374
Gateway Customer 374
Gateway Processing 374
Gateway Transaction 374
Global Collection Only (GCO) Data Collection Program 374
Government Controlled Merchant 374
Host Card Emulation (HCE) 374
Hybrid Terminal 375
ICA 375
Identification & Verification (ID&V) 375
Independent Sales Organization (ISO) 375
Installment Lending Agreement 375
Installment Provider 375
Interchange System 376
Inter-European Transaction 376
Interregional Transaction 376
Intracountry Transaction 376
Intra–European Transaction 376
Intra–Non–SEPA Transaction 377
Intraregional Transaction 377
Issuer 377
License, Licensed 377
Licensee 377
Maestro 377
Maestro Acceptance Mark 377
Maestro Access Device 378
Maestro Account 378
Maestro Brand Mark 378
Maestro Card 378
Maestro Customer 378

Maestro Payment Application....378
Maestro Word Mark....378
Magnetic Stripe Mode Contactless Transaction....379
Manual Cash Disbursement Transaction....379
Marks....379
Mastercard....379
Mastercard Acceptance Mark....379
Mastercard Access Device....379
Mastercard Account....380
Mastercard Biometric Card....380
Mastercard Brand Mark....380
Mastercard-branded Application Identifier (AID)....380
Mastercard Card....380
Mastercard Cloud-Based Payments....380
Mastercard Consumer-Presented QR Transaction....380
Mastercard Customer....381
Mastercard Digital Enablement Service....381
Mastercard Europe....381
Mastercard Incorporated....381
Mastercard Payment Application....381
Mastercard Safety Net....381
Mastercard Symbol....382
Mastercard Token....382
Mastercard Token Account Range....382
Mastercard Token Vault....382
Mastercard Word Mark....382
Member, Membership....383
Merchandise Transaction....383
Merchant....383
Merchant Agreement....383
Merchant Card-on-File Tokenization....383
Merchant Token Requestor....383
Merchant-initiated Transaction (MIT)....384
Mobile Payment Device....384
Mobile POS (MPOS) Terminal....384
MoneySend Payment Transaction....384
Multi-Account Chip Card....384
Non-Mastercard BIN Maestro card-not-present (CNP) debit card....384
Non-Mastercard Funding Source....385

Non-Mastercard Receiving Account....385
Non-Mastercard Systems and Networks Standards....385
On-behalf Token Requestor....385
On-Device Cardholder Verification....385
Originating Account Holder....385
Originating Institution (OI)....385
Ownership, Owned....386
Participation....386
Pass-through Digital Wallet....386
Pass-through Digital Wallet Operator (DWO)....386
Payment Account Reference (PAR)....386
Payment Application....386
Payment Facilitator....387
Payment Transaction....387
Payment Transfer Activity(ies) (PTA)....387
Personal Data....387
Point of Interaction (POI)....387
Point-of-Sale (POS) Terminal....387
Point–of–Sale (POS) Transaction....388
Portfolio....388
Principal Customer, Principal....388
Processed PTA Transaction....388
Processed Transaction....388
Program....389
Program Service....389
PTA Account....389
PTA Account Number....389
PTA Account Portfolio....389
PTA Agreement....389
PTA Customer....389
PTA Originating Account....390
PTA Program....390
PTA Receiving Account....390
PTA Settlement Guarantee Covered Program....390
PTA Settlement Obligation....390
PTA Transaction....390
Quick Response (QR) Code....390
Receiving Account Holder....391
Receiving Agent....391

Receiving Customer....391
Receiving Institution (RI)....391
Region....391
Remote Electronic Transaction....391
Rules....391
Service Provider....392
Settlement Obligation....392
Shared Deposit Transaction....392
Solicitation, Solicit....392
Special Issuer Program....392
Sponsor, Sponsorship....392
Sponsored Digital Activity Entity....393
Sponsored Merchant....393
Sponsored Merchant Agreement....393
Staged Digital Wallet....393
Staged Digital Wallet Operator (DWO)....394
Standards....394
Stand-In Parameters....394
Stand-In Processing Service....394
Stored Credential....394
Strong Customer Authentication (SCA)....395
Sub-licensee....395
Terminal....395
Third Party Processor (TPP)....395
Token....395
Token Aggregator....395
Token Requestor....395
Token Vault....396
Tokenization, Tokenize....396
Transaction....396
Transaction Data....396
Transaction Information Document (TID)....396
Transaction Management System....396
Trusted Service Manager....397
Virtual Account....397
Volume....397
Wallet Token Requestor....397
Word Mark....397

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.

Acceptor

The Merchant, Sponsored Merchant, ATM owner, or other entity that accepts a Card pursuant to a Merchant Agreement, Sponsored Merchant Agreement, or ATM Owner Agreement for purposes of conducting a Transaction.

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 an ATM Transaction with a Card (and if contactless-enabled, an Access Device) 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 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.

Cardholder-initiated Transaction (CIT)

A Transaction in which the Cardholder actively participates by presenting a Card or Access Device at the POI or agreeing to the use of a Stored Credential to complete the Transaction, and may be required to perform a CVM or other Cardholder authentication.

China Deposit Transaction

A domestic deposit to an Account conducted at an ATM Terminal located in China, initiated with a Card issued by a China Customer, and processed through the China Switch.

China Funds Transfer Funding Transaction

A domestic financial transaction sent by the China Switch on behalf of the Originating Institution to the Funding Institution to fund the subsequent associated China Funds Transfer Payment Transaction.

China Funds Transfer Payment Transaction

A domestic financial transaction sent by the China Switch on behalf of the Originating Institution to the Receiving Institution to transfer the funds into a receiving account.

China Funds Transfer Request

A domestic non-financial transaction sent by the Original Institution to the China Switch to initiate the China Funds Transfer Transactions.

China Funds Transfer Transaction

A China domestic Transactions that facilitates the funds transfer from an Account to another Account. Each China Funds Transfer Transaction contains two associated transactions, the China Funds Transfer Funding Transaction and the China Funds Transfer Payment Transaction.

China Recurring Payment Transaction – Recurring Payment Terms

The recurring payment terms are the terms and conditions agreed by Merchant and Cardholder for China domestic recurring payment Transactions. It includes card acceptor name, merchandise or service, payment account, recurring payment frequency or condition, and ending date (if applicable). The Acquirer must populate the recurring payment terms in each China domestic recurring payment Transaction message.

China Switch Manual Transaction

China domestic Transactions, manually initiated by the Acquirer via the China Dispute Resolution Platform, that includes manual preauthorization reversal, manual preauthorization complete and manual refund.

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 Transaction

A Contact Chip Transaction or a Contactless Transaction.

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.

Cirrus Acceptance Mark

A Mark consisting of the Cirrus Brand Mark placed on the dark blue acceptance rectangle, available at 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 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.

Credential-on-file Transaction

A Transaction initiated at a Merchant location with a Stored Credential, pursuant to the Cardholder's express authorization for the use of such Stored Credential to effect the Transaction.

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 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 (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.

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.

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.

Funding Transaction

A Funding Transaction is a Point-of-Sale (POS) Transaction for the purchase of funds transfer services that involves the transfer of funds from an eligible Account by an Acquirer on behalf of the Cardholder (directly or indirectly) for the purpose of either: (a) funding a subsequent and linked funds transfer from the Cardholder to another person or entity or (b) transferring funds into another eligible financial account held by that same Cardholder. Eligible Accounts and eligible financial accounts are set out in the *Mastercard MoneySend and Funding Transactions Program Standards*.

Gaming Payment Transaction

A type of Payment Transaction that transfers winnings or value usable for gambling or gaming to a Mastercard or Maestro Account.

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.

Government Controlled Merchant

A Merchant that is a government entity or an entity that is at least fifty percent (50%) owned or controlled (either directly, indirectly, legally or beneficially) by a government or government entity.

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 as ISO Program Service.

Installment Lending Agreement

The agreement between the Installment Service Provider and an End User, which includes terms and conditions governing the relationship between the parties, such as lending amount and repayment terms.

Installment Provider

An Installment Service Provider that accepts a Card for the remittance phase of the Installment Lending Agreement, or other entity that accepts a Card pursuant to the Cardholder's agreement to remit payment in installments for the purchase of goods or services from a retailer on whose behalf the Installment Provider offers installment billing services.

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), the Settlement Account Management (SAM) system and the China Switch 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.

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 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, sounds, animations, haptics, visual depictions, 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.

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 22210000 to 27209999 or 51000000 to 55999999.

Mastercard Biometric Card

A Mastercard or Maestro Chip Card containing a fingerprint sensor and compliant with the Corporation's biometric Standards.

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-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 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 *M/Chip 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 Card-on-File Tokenization

The use of the Mastercard Digital Enablement Service (MDES) to replace Mastercard or Maestro Account data (meaning PAN and expiration date), that the Cardholder expressly authorized a Merchant to store for use in a future Transaction, with a Mastercard Token.

Merchant Token Requestor

A Merchant approved by the Corporation to conduct Digital Activity and authorized to connect directly or indirectly 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.

Merchant-initiated Transaction (MIT)

A Card-not-present Transaction that a Merchant initiates based on a prior agreement with the Cardholder, and in which the Cardholder does not actively participate. An MIT may be a recurring payment (standing order, subscription, unscheduled COF, or installment payment) or industry practice (partial shipment, related/delayed charge, no-show, or resubmission).

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 *Mastercard MoneySend and Funding Transactions Program Standards*.

Multi-Account Chip Card

A Chip Card with more than one Account encoded in the chip.

Non-Mastercard BIN Maestro card-not-present (CNP) debit card

A U.S. Region or U.S. Territory issued debit card with a Primary Account Number starting with a four and enhanced with Maestro functionality that transacts card-not-present at a Maestro Merchant located in the U.S. Region or a U.S. Territory.

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, other Customer, Network Enablement Partner, or other entity 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. Also called a Token Aggregator.

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 Sponsored Merchant, and upon the performance of a Transaction, transfers the Account data to the Merchant or Sponsored Merchant, 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 Sponsored Merchant, and which in doing so, performs any one or more of the services 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 Transaction and Gaming Payment Transaction.

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

One of the following:

- An attended or unattended device including any commercial off-the-shelf (COTS) or other device enabled with mobile point-of-sale (MPOS) functionality, that is in the physical possession of a Merchant and is deployed in or at the Merchant's premises, and which enables a Cardholder to use a Card or Access Device to effect a Transaction for the purchase of products or services sold by such Merchant; or
- 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 a Manual Cash Disbursement Transaction. A POS Transaction conducted by a Merchant 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, a Network Enablement Partner, or other entity approved by the Corporation Participating.

Program Service

Any service described 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, the Mastercard Send Cross-Border Service, and the Mastercard Gaming and Gambling Payments Program.

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 Transactions (e-commerce Transactions, recurring payments, installments, Card-on-file Transactions, in-app Transactions, and Transactions completed through a Digital Wallet). 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 or entity that performs Program Service. The Corporation has the sole right to determine whether a person or entity 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 which case, the Principal or Association is the Sponsor of the Affiliate and the Affiliate is Sponsored by the Principal or Association;
- a Payment Facilitator and a Sponsored Merchant, in which case the Payment Facilitator is the Sponsor of the Sponsored Merchant and the Sponsored Merchant is Sponsored by the Payment Facilitator; or
- a Digital Activity Sponsoring Customer and a Sponsored Digital Activity Entity, in which case the Digital Activity Sponsoring Customer is the Sponsor of the Sponsored Digital Activity Entity.

"Sponsorship" means the Sponsoring of a Customer, a Sponsored Merchant, or a Sponsored Digital Activity Entity.

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.

Sponsored Merchant

A merchant that, pursuant to an agreement with a Payment Facilitator, is authorized to accept Cards when properly presented. A Sponsored Merchant is also referred to as Submerchant.

Sponsored Merchant Agreement

An agreement between a Sponsored Merchant and a Payment Facilitator that sets forth the terms pursuant to which the Sponsored Merchant is authorized to accept Cards. A Sponsored Merchant Agreement is also referred to as Submerchant Agreement.

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.

Stored Credential

Mastercard or Maestro Account data (meaning PAN and expiration date) retained by a Merchant or its Acquirer in accordance with the Cardholder's express authorization for the Merchant to store such Account data (or a Tokenized replacement of the originally provided Account data generated by Merchant Card-on-File Tokenization) for use in future Transactions.

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.

Terminal

Any attended or unattended device capable of the electronic capture and exchange of Account data that meets the Corporation requirements for Terminal eligibility, functionality, and security, and 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 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.

Token Aggregator

See On-behalf Token Requestor.

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.

Tokenization, Tokenize

The process by which a Mastercard Token replaces an Account PAN or a PTA Account Number.

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 Information Document (TID)

The record of a Transaction generated by the Card Acceptor and provided in electronic or hard copy format to its Acquirer, with a copy provided to the Cardholder upon request or as required in accordance with the Standards or applicable law; a Transaction receipt.

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. 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.

EMV® is a registered trademark of EMVCo LLC in the United States and other countries. For more information, see http://www.emvco.com.

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.

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 Technical Resource Center (TRC). Go to the Rules collection of the References section for centralized information.