



# Customer Interface Specification

6 April 2012

---

## Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

### **Proprietary Rights**

The information contained in this document is proprietary and confidential to MasterCard International Incorporated, one or more of its affiliated entities (collectively “MasterCard”), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

### **Trademarks**

Trademark notices and symbols used in this document reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services 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.

### **Translation**

A translation of any MasterCard manual, bulletin, release, or other MasterCard document into a language other than English is intended solely as a convenience to MasterCard customers. MasterCard provides any translated document to its customers “AS IS” and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall MasterCard be liable for any damages resulting from reliance on any translated document. The English version of any MasterCard document will take precedence over any translated version in any legal proceeding.

### **Information Available Online**

MasterCard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on MasterCard OnLine®. Go to Publications [Support](#) for centralized information.

---

# Summary of Changes, 6 April 2012

This document reflects changes associated with Dual Message System Release 12.Q2 Document.

Description of Change	Where to Look
Please note that the term “customer” has been defined as an alternative term for and having the same meaning as “member.” As reflected in its certificate of incorporation, MasterCard International Incorporated is authorized to issue membership interests, including principal memberships, association memberships, and affiliate memberships, with a holder of a membership interest referred to as a “member.” While the terminology in the certificate of incorporation will remain the same, going forward in all other instances, absent a need to do otherwise, the term “customer” will be substituted for the term “member.” In addition, the term “principal” will appear as an alternative term for “principal member,” “association” as an alternative to “association member,” and “affiliate” as an alternative to “affiliate member.”	Global change
<b>Chapter 2, “About Message Definitions”</b>	
Added Authorization Request Response/0110—Issuer Edit Error message flow.	<a href="#">Authorization Request Response/0110—Issuer Edit Error</a>
<b>Chapter 4, “Data Element Definitions”</b>	
Added to DE 4—(Amount, Transaction), application notes, the following: <b>For Automated Fuel Dispenser (AFD) Transactions:</b>	<a href="#">DE 4—Amount, Transaction</a>
Effective 12 June 2012 the contents of DE 4 may equal zero when the authorization Advice/0120 message is sent by a Europe region acquirer for an AFD transaction in Europe and contains DE 18 (Merchant Type) = 5542 (Fuel Dispenser, Automated) and DE 60 (Advice Reason Code) = 191 (Acquirer Processing System [APS] Completed Authorization Transaction). Issuers should be prepared to receive zero amount AFD completion advices from any acquirer as there is no Authorization Platform edit restricting such advices from Europe region acquirers.	
Added to DE 18 (Merchant Type), application notes: This edit only applies to request and advice messages originated by dual message acquires. This edit does not apply to messages originated by single message acquirers and therefore dual message issuers should expect to receive this data.	<a href="#">DE 18—Merchant Type</a>
Added to DE 35 (Track 2 Data), DE35 is optional for 0120 AFD completion advice. See Chapter 5 AFD Completion for more detail.	<a href="#">DE 35—Track 2 Data</a>
Added to DE 37 (Retrieval Reference Number), application notes, Acquirers may construct DE 37 in the same manner for MasterCard, as is indicated above for Visa messages.	<a href="#">DE 37—Retrieval Reference Number</a>
Added to DE 39, Authorization Advice Response/0130 Response Codes the following value: 12 = Invalid transaction.	<a href="#">Authorization Advice Response/0130 Response Codes</a>

Description of Change	Where to Look
Added to DE 45 (Track 1 Data), application notes, DE 45 is optional for 0120 AFD completion advice. Please refer to <i>AFD Completion</i> for more information.	<a href="#">DE 45—Track 1 Data</a>
Added to DE 48, subelement 33 (PAN Mapping File Information), usage, the following edit:	<a href="#">Subelement 33—PAN Mapping File Information</a>
Authorization Advice Response/0130—Issuer-generated	
Changed DE 48, subelement 36, subfield 1 (Merchant Verification Value), values:	<a href="#">Subfield 1—Merchant Verification Value</a>
<ul style="list-style-type: none"> <li>• From: Undefined and unedited except for format.</li> <li>• To: 0–9 and A–F</li> </ul>	
Added to DE 38, subelement 43 (3-D Secure for MasterCard SecureCode), value h the following:	<a href="#">Subelement 43—3-D Secure for MasterCard SecureCode</a>
Acquirer should remove from an Authorization Request/0100 before submitting message to MasterCard.	
Added to DE 48, subelement 43 (3-D Secure for MasterCard SecureCode), application notes the following:	<a href="#">Subelement 43—3-D Secure for MasterCard SecureCode</a>
MasterCard does not support “attempt”AAVs, and these should be removed from the authorization request before submitting to MasterCard.	
Changed the following fields in DE 48, subelement 48 (Mobile Program Indicators): data representation, data field, and subfields.	<a href="#">Subelement 48—Mobile Program Indicators</a>
Changed DE 48, subelement 48, subfield 1 (Remote Payments Program Type Identifier), attributes, length of length field and data representation.	<a href="#">Subfield 1—Remote Payments Program Type Identifier</a>
Added to DE 48, subelement 48, new subfield 2 (Reserved for Future Use), subfield 3 (Mobile Phone Number), and subfield 4 (Convenience Fee).	<a href="#">Subelement 48—Mobile Program Indicators</a>
Added to DE 48, subelement 63 (Trace ID) the following message types:	<a href="#">Subelement 63—Trace ID</a>
<ul style="list-style-type: none"> <li>• Authorization Request/0100, C • C</li> <li>• Authorization Advice/0120—Acquirer-generated, C • C</li> <li>• Authorization Advice/0120—System-generated, • C C</li> </ul>	
Added to DE 48, new subelement 64 (Transit Program)	<a href="#">Subelement 64—Transit Program</a>
Added to DE 48, new subelement 90 (Custom Payment Service Request Response [Visa-only])	<a href="#">Subelement 90—Custom Payment Service Request Response (Visa Only)</a>
Changed DE 48, subelement 91 (Custom Payment Service Response Transaction ID [Visa Only]), attributes, data field:	<a href="#">Subelement 91—Custom Payment Service Response Transaction ID (Visa Only)</a>
<ul style="list-style-type: none"> <li>• From: 1–4</li> <li>• To: 1–6</li> </ul>	

---

<b>Description of Change</b>	<b>Where to Look</b>
Changed DE 48, subelement 91 (Custom Payment Service Response Transaction ID [Visa Only]), when length field is 06:	<a href="#">Subelement 91—Custom Payment Service Response Transaction ID (Visa Only)</a>
<ul style="list-style-type: none"> <li>• From: Downgraded by Visa (2 bytes alphanumeric), followed by the Visa downgrade reason code (2 two bytes alphanumeric). Please refer to the Visa Base I Technical Specifications manual for specific downgrade reason codes and meanings.</li> <li>• To: Downgraded by Visa (2 bytes alphanumeric), followed by either the Visa validation code (4 bytes alphanumeric) or the downgrade reason code (2 bytes alphanumeric code followed by two spaces). Please refer to the Visa Base I Technical Specifications manual for more information on Visa CPS validation codes and specific CPS downgrade reason codes and meanings.</li> </ul>	
Added to DE 48, subelement 99 (MasterCard Corporate Fleet Card Vehicle Number), usage, the following:	<a href="#">Subelement 99—MasterCard Corporate Fleet Card Vehicle Number</a>
<ul style="list-style-type: none"> <li>• Authorization Advice/0120—Acquirer-generated, C •.C</li> <li>• Authorization Advice Response/0130—Issuer-generated, CE •.CE</li> </ul>	
Added to DE 55 Subelements, Tag Value 9F34, the following:	<a href="#">DE 55—Subelements</a>
The presence of 9F34 is mandatory for all authorization messages containing DE 55 that are transmitted from acquirer chip systems certified by MasterCard on or after 13 April 2012. The presence of 9F34 is mandatory for all authorization messages containing DE 55 effective 1 April 2017.	
Changed DE 61 (Point-of-Service (POS) Data), subfield 11 (POS Card Data Terminal Input Capability Indicator), values,	<a href="#">Subfield 11—POS Card Data Terminal Input Capability Indicator</a>
<ul style="list-style-type: none"> <li>• From: 3 = Contactless M/Chip (Proximity Chip). Terminal supports <i>PayPass</i> M/Chip and <i>PayPass</i> magstripe transactions. The terminal also may support contact transactions, however this value must only be used for contactless transactions.</li> <li>• To: 3 = Contactless M/Chip (Proximity Chip). Value 3 indicates that the terminal supports <i>PayPass</i> M/Chip and <i>PayPass</i> magstripe transactions. The terminal also may support other card input types, including contact transactions.</li> </ul>	
and	
<ul style="list-style-type: none"> <li>• From: 4 = Contactless Magnetic Stripe (Proximity Chip) only. Terminal supports <i>PayPass</i> magstripe transactions. The terminal also may support contact transactions, however this value must only be used for contactless magstripe transactions.</li> <li>• To: 4 = Contactless Magnetic Stripe (Proximity Chip) only. Value 4 indicates that the terminal supports <i>PayPass</i> magstripe transactions. The terminal also may support other card input types, including contact transactions.</li> </ul>	
Added to the application notes the following:	
Acquirers should submit, and issuers should accept, value 3 when the terminal has <i>PayPass</i> contactless M/Chip capability.	
Acquirers should submit, and issuers should accept, value 4 when the terminal has <i>PayPass</i> contactless magnetic stripe capability.	

<b>Description of Change</b>	<b>Where to Look</b>
<p>The PAN entry mode (DE 22 [Point-of-Service Entry Model], subfield 1 [POS Terminal PAN Entry Model]) may be any mode supported by the terminal. Acquirers may also continue to pass the POS Card Data Terminal Capability indicator in DE 61, subfield 11 as they do today.</p>	
<p>Changed DE 63 (Network Data), subfield 1 (Financial Network Code) footnote content from DE 130 to DE 120.</p>	<a href="#">Subfield 1—Financial Network Code</a>
<p>Added to DE 63, subfield 1 the following financial network codes: DAG, DAP, DAS, DOS, MBP, MBT, MOC, SAG, SAL, SAP, SAS, SOS, and WBE.</p>	
<p>Added to DE 112, Mexcta—Payment Transactions, new subelement 006 (Financial Institution ID [FIID]).</p>	<a href="#">Subelement 006—Financial Institution ID (FIID)</a>
<p>Changed DE 120 (Record Data), subfield 01 (AVS Service Indicator 1) attributes and values for Visa:</p> <ul style="list-style-type: none"> <li>• From: 49</li> <li>• To: 29</li> </ul>	<a href="#">Subfield 01—AVS Service Indicator 1</a>
<b>Chapter 5, Program and Service Format Requirements</b>	
<p>Changed Account Status Inquiry Service Acquirer Requirements</p>	<a href="#">Account Status Inquiry Service</a>
<ul style="list-style-type: none"> <li>• From: At the issuer's discretion, the acquirer may receive an Authorization Request Response/0110 message where DE 39 may contain either the value 05 (Do not honor), or 85 (Not declined). If the issuer is unable to reply, the acquirer will receive a response code of 91 (Authorization System or issuer system inoperative).</li> <li>• To: At the issuer's discretion, the acquirer may receive an Authorization Request Response/0110 message where DE 39 may contain either the value 00 (Approved), 05 (Do not honor), or 85 (Not declined). If the issuer is unable to reply, the acquirer will receive a response code of 91 (Authorization System or issuer system inoperative).</li> </ul>	
<p>Issuer Requirements</p>	
<ul style="list-style-type: none"> <li>• From: The issuer, at its discretion, will send the acquirer an Authorization Request Response/0110 message where DE 39 may contain either the value 05 or 85. If the issuer is unable to reply, the acquirer will receive a response code of 91 (Authorization System or issuer system inoperative).</li> <li>• To: The issuer, at its discretion, will send the acquirer an Authorization Request Response/0110 message where DE 39 may contain either the value 00, 05, or 85. If the issuer is unable to reply, the acquirer will receive a response code of 91 (Authorization System or issuer system inoperative).</li> </ul>	
<p>Added to Authorization Request Response/0110—Account Status Inquiry, DE 39 (Response Code), values/comments the following edit: 00 = Approved</p>	<a href="#">Authorization Request Response/0110—Account Status Inquiry</a>

Description of Change	Where to Look
Added to Authorization Advice/0120—Acquirer-generated (Automated Fuel Dispenser Completion), Critical AFD Advice Message Data.	<a href="#">Authorization Advice/0120—Acquirer-generated (Automated Fuel Dispenser Completion)</a>
Changed Authorization Request/0100—ATM Bill Payment, Europe Acquired, DE 18 (Merchant Type), values/comments:	<a href="#">Authorization Request/0100—ATM Bill Payment, Europe Acquired</a>
<ul style="list-style-type: none"> <li>• From: Must contain value 6050 = Quasi Cash-member In addition, transactions may be identified with a more precise MCC related to the nature of the bill that is being paid.</li> <li>• To: Contains value 6050 = Quasi Cash—Member Financial Institution or a more precise MCC related to the nature of the bill that is being paid, for example, MCC 4900 (Utilities-Electric, Gas, Heating Oil, Sanitary, Water) for utilities bills. MCC 6011 (Member Financial Institution-Automated Cash Disbursements) must not be used. This edit only applies to request and advice messages originated by dual message acquires. This edit does not apply to messages originated by single message acquirers and therefore dual message issuers should expect to receive this data.</li> </ul>	
Changed Contact and Contactless Chip Specific Value Constraints	<a href="#">Contact and Contactless Chip Specific Value Constraints</a>
<ul style="list-style-type: none"> <li>• From: 3 = The terminal also may support contact transactions, however this value must only be used for contactless transactions. DE 22 subfield 1 applicable values: 07 (PAN auto-entry via contactless M/Chip) and 91 (PAN auto-entry via contactless magnetic stripe)</li> <li>• To: 3 = Value 3 indicates that the terminal supports <i>Paypass</i> M/Chip and <i>Paypass</i> magstripe transactions. The terminal may also support other card input types, including contact transactions.</li> </ul>	
Changed Contact and Contactless Chip Specific Value Constraints	<a href="#">Contact and Contactless Chip Specific Value Constraints</a>
<ul style="list-style-type: none"> <li>• From: 4 = Terminal supports <i>PayPass</i> magstripe transactions. The terminal also may support contact transactions, however this value must only be used for contactless magstripe transactions. DE 22, subfield 1 applicable value 91 (PAN auto-entry via contactless magnetic stripe).</li> <li>• To: 4 = Value 4 indicates that the terminal supports <i>Paypass</i> magstripe transactions. The terminal may also support other card input types, including contact transactions.</li> </ul>	

---

## Table of Contents

<b>Chapter 1 Overview .....</b>	<b>1-i</b>
The Customer Interface Specification Format .....	1-1
Issuer Post-on Authorization.....	1-2
Bit Mapped Message Encoding Scheme .....	1-3
Authorization Platform Processing Terms and Acronyms .....	1-4
Customer Interface Specification Notations .....	1-4
Data Length Notations .....	1-4
Data Representation Notations .....	1-5
Data Field Notations .....	1-6
Data Justification Notations.....	1-6
Date and Time Notations.....	1-7
Entity Notations .....	1-7
Presence Notations .....	1-8
Presence Requirement Notations .....	1-8
Program and Service Category Notations.....	1-9
Authorization Platform Messages.....	1-10
List of Authorization Messages.....	1-10
Message Type Identifier Presence Requirements by Program and Service .....	1-12
Character Sets .....	1-14
Extended ASCII to Extended EBCDIC Character Set Conversion.....	1-15
Swedish Domestic Authorization Switching Character Set.....	1-18
<b>Chapter 2 Message Definitions and Flows .....</b>	<b>2-i</b>
About Message Definitions .....	2-1
About Authorization Messages.....	2-1
About Authorization Advice Messages.....	2-2
About Authorization Response Acknowledgement Messages.....	2-5
About Issuer File Update Messages .....	2-6
About Reversal Messages.....	2-6
About Administrative Messages .....	2-8
About Network Management Messages .....	2-10
About Message Flows .....	2-12
Authorization Message Routing Timers.....	2-12
Authorization Request/0100 and Authorization Request Response/0110 .....	2-13

## Table of Contents

---

Authorization Request/0100—Communication Failure at Acquirer.....	2-14
Authorization Request/0100—Communication Failure at Issuer.....	2-15
Authorization Request Response/0110—Communication Failure at Acquirer.....	2-17
Authorization Request Response/0110—Communication Failure at Issuer.....	2-19
Authorization Request Response/0110—Stand-In System Allowed.....	2-21
Authorization Request Response/0110—Not Eligible for Alternate Processing.....	2-27
Authorization Request/0100—Chip PIN Management .....	2-31
Authorization Request/0100—Chip PIN Management (Failure to Transmit/Apply Script to Chip Card) .....	2-33
Authorization Request/0100—Chip PIN Management (Issuer Network Failure-Unable to Connect).....	2-35
Authorization Request/0100—Chip PIN Management (Issuer Network Failure, No Response from Issuer).....	2-36
Authorization Request/0100—Chip PIN Management (Acquirer Network Failure-Unable to Connect).....	2-38
Authorization Request/0100—Chip PIN Management (Acquirer Network Failure-Unable to Connect with Acquirer) .....	2-39
Guaranteed Advice Message Delivery .....	2-41
Acquirer Response Acknowledgement/0180 Messages.....	2-49
Alternate Issuer Host Processing for Online Europe Region Members .....	2-50
Authorization Response Negative Acknowledgement/0190 (Responding to the Authorization Request Response/0110) .....	2-59
Authorization Response Negative Acknowledgement/0190 (Responding to the Reversal Request Response/0410).....	2-60
Issuer File Update Request/0302 and Issuer File Update Request Response/0312.....	2-61
Reversal Messages.....	2-62
Administrative Request/0600 and Administrative Request Response/0610 .....	2-71
Administrative Request/0600, Acquirer Edit Failure .....	2-72
Administrative Request/0600, Communication Failure at Issuer .....	2-73
Administrative Request Response/0610, Communication Failure at Acquirer .....	2-74
Administrative Request Response/0610, No Issuer Response .....	2-75
Administrative Request Response/0610, Late Issuer Response .....	2-76
Administrative Request Response/0610, Issuer Edit Failure .....	2-77
Administrative Advice/0620 and Administrative Advice Response/0630.....	2-78
Administrative Advice/0620 and Administrative Advice Response/0630—Invalid Message, System-generated .....	2-79
Administrative Advice/0620 and Administrative Advice Response/0630—RiskFinder, System-generated.....	2-80
Network Management Request 0800—Sign-On/Sign-Off.....	2-81
Network Management Request/0800—RiskFinder Sign-On/Sign-Off.....	2-82

---

Network Management Request/0800—Solicited SAF .....	2-83
Network Management Request/0800—Unsolicited SAF.....	2-84
Network Management Request/0800—RiskFinder SAF.....	2-85
Network Management Request/0800—Network Connection Status, Member-generated.....	2-86
Network Management Request/0800—Network Connection Status, System-generated.....	2-87
Network Management Request/0800—Host Session Activation/Deactivation.....	2-88
Network Management Request/0800—PEK Exchange Authorization Platform-Initiated .....	2-89
Network Management Request/0800—PEK Exchange Member-Initiated.....	2-90

## **Chapter 3 Message Layouts..... 3-i**

Authorization Request/0100.....	3-1
Authorization Request Response/0110.....	3-5
Authorization Advice/0120—Acquirer-generated.....	3-9
Authorization Advice/0120—Issuer-generated .....	3-13
Authorization Advice/0120—System-generated .....	3-16
Authorization Advice Response/0130—Issuer-generated (Responding to a System-generated 0120 from SAF) .....	3-19
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120).....	3-21
Authorization Advice Response/0130—System-generated (Responding to an Acquirer-generated 0120).....	3-24
Authorization Advice Response/0130—System-generated (Responding to an Issuer-generated 0120).....	3-26
Authorization Response Acknowledgement/0180.....	3-28
Authorization Response Negative Acknowledgement/0190.....	3-29
Issuer File Update Request/0302.....	3-30
Issuer File Update Request Response/0312 .....	3-31
Reversal Request/0400 .....	3-32
Reversal Request Response/0410 .....	3-37
Reversal Advice/0420.....	3-40
Reversal Advice Response/0430.....	3-44
Administrative Request/0600.....	3-46
Administrative Request Response/0610 .....	3-48
Administrative Advice/0620—System-generated .....	3-50

## Table of Contents

---

Administrative Advice/0620—Member-generated .....	3-52
Administrative Advice Response/0630 .....	3-53
Network Management Request/0800—Sign-On/Sign-Off .....	3-54
Network Management Request/0800—RiskFinder SAF Request .....	3-56
Network Management Request/0800—Network Connection Status, Member-generated .....	3-57
Network Management Request/0800—Network Connection Status, System-generated.....	3-58
Network Management Request/0800—Host Session Activation/Deactivation.....	3-59
Network Management Request/0800—PEK Exchange.....	3-60
Network Management Request/0800—PEK Exchange On Demand.....	3-61
Network Management Request Response/0810—Sign-On/Sign-Off .....	3-62
Network Management Request Response/0810—RiskFinder SAF Request .....	3-63
Network Management Request Response/0810—Network Connection Status, Member-generated .....	3-64
Network Management Request Response/0810—Network Connection Status, System-generated .....	3-65
Network Management Request Response/0810—Host Session Activation/Deactivation.....	3-66
Network Management Request Response/0810—PEK Exchange .....	3-67
Network Management Request Response/0810—PEK Exchange-On Demand.....	3-68
Network Management Advice/0820—RiskFinder SAF End of File .....	3-69
Network Management Advice/0820—PEK Exchange .....	3-70
<b>Chapter 4 Data Element Definitions .....</b>	<b>4-i</b>
Data Element Layout.....	4-1
Subelement Layout .....	4-1
Subfield Layout .....	4-2
Position Layout .....	4-2
List of Data Elements (Numeric Order).....	4-2
List of Data Elements (Alphabetic Order) .....	4-7
Message Type Identifier.....	4-11
Message Types and Applicable Program or Service .....	4-14
About Primary and Secondary Bit Maps .....	4-15
Primary Bit Map .....	4-16
DE 1—Bit Map, Secondary .....	4-18
DE 2—Primary Account Number (PAN) .....	4-20

## Table of Contents

---

About Primary Account Number.....	4-23
DE 3—Processing Code.....	4-24
Subfield 1—Cardholder Transaction Type Code.....	4-25
Subfield 2—Cardholder "From Account" Type Code .....	4-27
Subfield 3—Cardholder "To Account" Type Code .....	4-28
DE 4—Amount, Transaction .....	4-28
DE 5—Amount, Settlement.....	4-31
DE 6—Amount, Cardholder Billing.....	4-32
DE 7—Transmission Date and Time.....	4-34
Subfield 1—Date.....	4-36
Subfield 2—Time .....	4-36
DE 8—Amount, Cardholder Billing Fee.....	4-37
DE 9—Conversion Rate, Settlement.....	4-37
Subfield 1—Decimal Indicator.....	4-38
Subfield 2—Conversion Rate .....	4-39
DE 10—Conversion Rate, Cardholder Billing.....	4-39
Subfield 1—Decimal Indicator.....	4-40
Subfield 2—Cardholder Billing Conversion Rate .....	4-41
DE 11—System Trace Audit Number (STAN).....	4-41
DE 12—Time, Local Transaction.....	4-43
DE 13—Date, Local Transaction .....	4-44
DE 14—Date, Expiration.....	4-45
DE 15—Date, Settlement .....	4-46
DE 16—Date, Conversion.....	4-48
DE 17—Date, Capture .....	4-49
DE 18—Merchant Type .....	4-49
DE 19—Acquiring Institution Country Code.....	4-51
DE 20—Primary Account Number (PAN) Country Code.....	4-51
DE 21—Forwarding Institution Country Code .....	4-53
DE 22—Point-of-Service (POS) Entry Mode .....	4-53
Subfield 1—POS Terminal PAN Entry Mode .....	4-54
Subfield 2—POS Terminal PIN Entry Mode .....	4-56
Authorization Platform Edits .....	4-57
DE 23—Card Sequence Number.....	4-60
DE 24—Network International ID .....	4-61

## Table of Contents

---

DE 25—Point-of-Service (POS) Condition Code.....	4-62
DE 26—Point-of-Service (POS) Personal ID Number (PIN) Capture Code.....	4-62
DE 27—Authorization ID Response Length.....	4-63
DE 28—Amount, Transaction Fee.....	4-64
Subfield 1—Debit/Credit Indicator .....	4-65
Subfield 2—Amount .....	4-66
DE 29—Amount, Settlement Fee .....	4-66
Subfield 1—Debit/Credit Indicator .....	4-66
Subfield 2—Amount .....	4-67
DE 30—Amount, Transaction Processing Fee.....	4-67
Subfield 1—Debit/Credit Indicator .....	4-68
Subfield 2—Amount .....	4-68
DE 31—Amount, Settlement Processing Fee.....	4-68
Subfield 1—Debit/Credit Indicator .....	4-69
Subfield 2—Amount .....	4-69
DE 32—Acquiring Institution ID Code .....	4-69
DE 33—Forwarding Institution ID Code.....	4-71
DE 34—Primary Account Number (PAN), Extended.....	4-73
DE 35—Track 2 Data .....	4-74
DE 36—Track 3 Data .....	4-76
DE 37—Retrieval Reference Number.....	4-76
Subfield 1—Transaction Date and Initiator Discretionary Data.....	4-78
Subfield 2—Terminal Transaction Number.....	4-78
DE 38—Authorization ID Response .....	4-79
DE 39—Response Code.....	4-80
Authorization Request Response/0110 Response Codes.....	4-82
Authorization Advice/0120 Response Codes.....	4-84
Authorization Advice Response/0130 Response Codes .....	4-86
Authorization Advice Response/0180 Response Codes .....	4-87
Authorization Negative Acknowledgement/0190 Response Codes.....	4-87
Issuer File Update Request Response/0312 Response Codes .....	4-87
Reversal Request/0400 Message Response Codes.....	4-87
Reversal Request Response/0410 Response Codes .....	4-89
Reversal Advice/0420 Response Codes.....	4-90
Reversal Advice Response/0430 Message and Administrative Advice Response/0630 Response Codes.....	4-92
Administrative Request Response/0610 Response Codes .....	4-93

---

## Table of Contents

Network Management Request Response/0810 Response Codes .....	4-93
DE 40—Service Restriction Code .....	4-94
DE 41—Card Acceptor Terminal ID.....	4-94
DE 42—Card Acceptor ID Code .....	4-96
DE 43—Card Acceptor Name/Location for All Transactions.....	4-97
Subfield 1—Merchant Name ("Doing Business As" name) .....	4-98
Subfield 2—Space .....	4-99
Subfield 3—Merchant's City .....	4-99
Subfield 4—Space .....	4-99
Subfield 5—Merchant's State (or Country Code, if not U.S.).....	4-100
DE 43—Card Acceptor Name/Location for ATM Transactions.....	4-100
Subfield 1—ATM Owning Institution or Terminal/Merchant Address or Both.....	4-101
Subfield 2—Space .....	4-101
Subfield 3—ATM or Merchant Location City .....	4-102
Subfield 4—Space .....	4-102
Subfield 5—ATM or Merchant State, Province, or Country Code Location .....	4-102
DE 43—Card Acceptor Name/Location for Bankcard-Activated Public Phones.....	4-103
Subfield 1—Abbreviation "TEL" .....	4-104
Subfield 2—Phone Number Dialed.....	4-104
Subfield 3—Abbreviation "M" .....	4-105
Subfield 4—Call Duration .....	4-105
Subfield 5—Space .....	4-105
Subfield 6—Call Origin City.....	4-106
Subfield 7—Space .....	4-106
Subfield 8—Call Origin State or Country Code.....	4-106
DE 44—Additional Response Data .....	4-107
DE 44 Values by Program or Service .....	4-108
DE 45—Track 1 Data .....	4-110
DE 46—Expanded Additional Amounts.....	4-112
DE 47—Additional Data—National Use .....	4-112
DE 48—Additional Data—Private Use .....	4-113
DE 48 Transaction Category Code .....	4-114
DE 48 Subelement Encoding Scheme in Authorization Request/0100 Messages .....	4-115
DE 48 Subelement Encoding Scheme in Network Management Messages.....	4-116
List of DE 48 Subelements .....	4-116
Subelement 10—Encrypted PIN Block Key .....	4-120
Subelement 11—Key Exchange Block Data (Single-Length Keys).....	4-120

## Table of Contents

---

Subelement 11—Key Exchange Block Data (Double-Length Keys) .....	4-121
Subelement 11—Key Exchange Block Data (Triple-Length Keys).....	4-123
Subelement 12—Routing Indicator .....	4-124
Subelement 13—MasterCard Hosted Mobile Phone Top-up Request Data.....	4-125
Subelement 15—Authorization System Advice Date and Time.....	4-126
Subelement 16—Processor Pseudo ICA.....	4-127
Subelement 20—Cardholder Verification Method .....	4-128
Subelement 23—Payment Initiation Channel.....	4-129
Subelement 25—MasterCard Cash Program Data .....	4-130
Subelement 32—MasterCard Assigned ID.....	4-131
Subelement 33—PAN Mapping File Information .....	4-132
Subelement 34—Dynamic CVC 3 ATC Information .....	4-136
Subelement 35— <i>PayPass</i> Non-Card Form Factor Request/Response .....	4-139
Subelement 36—Visa Defined Data (Visa Only).....	4-140
Subelement 38—Account Category.....	4-141
Subelement 39—Expert Monitoring Compromised Account Service Information .....	4-142
Subelement 40—Electronic Commerce Merchant/Cardholder Certificate Serial Number (Visa Only) .....	4-144
Subelement 41—Electronic Commerce Certificate Qualifying Information.....	4-146
Subelement 42—Electronic Commerce Indicators .....	4-151
Subelement 43—Universal Cardholder Authentication Field (UCAF) .....	4-153
Subelement 43—3-D Secure for MasterCard SecureCode .....	4-154
Subelement 43—Static AAV for Maestro or MasterCard Advance Registration Program .....	4-155
Subelement 43—Secure Electronic Commerce Verification Service (Visa Only) .....	4-156
Subelement 44—Visa 3-D Secure Electronic Commerce Transaction Identifier (XID) (Visa Only) .....	4-156
Subelement 45—Visa 3-D Secure Electronic Commerce Transaction Response Code (Visa Only) .....	4-157
Subelement 46—Card-Level Result (Visa Only) .....	4-158
Subelement 47—MasterCard Payment Gateway Transaction Indicator.....	4-159
Subelement 48—Mobile Program Indicators.....	4-160
Subelement 51—Merchant On-behalf Services .....	4-162
Subelement 55—Merchant Fraud Scoring Data .....	4-165
Subelement 58—ATM Additional Data.....	4-168
Subelement 61—POS Data Extended Condition Codes .....	4-171
Subelement 63—Trace ID .....	4-174
Subelement 64—Transit Program.....	4-176
Subelement 71—On-behalf Services .....	4-178

---

Subelement 72—Issuer Chip Authentication.....	4-182
Subelement 74—Additional Processing Information.....	4-183
Subelement 75—Fraud Scoring Data .....	4-186
Subelement 76—MasterCard Electronic Acceptance Indicator .....	4-189
Subelement 77—Payment Transaction Type Indicator .....	4-190
Subelement 78—U.S. Deferred Billing Indicator (Visa Only).....	4-191
Subelement 79—Chip CVR/TVR Bit Error Results.....	4-192
Subelement 80—PIN Service Code .....	4-195
Subelement 82—Address Verification Service Request .....	4-196
Subelement 83—Address Verification Service Response.....	4-196
Subelement 84—Merchant Advice Code.....	4-198
Subelement 84—Visa Response Codes (Visa Only) .....	4-198
Subelement 85—U.S. Existing Debt Indicator (Visa Only).....	4-199
Subelement 86—Relationship Participant Indicator (Visa Only) .....	4-200
Subelement 87—Card Validation Code Result .....	4-200
Subelement 87—CVV2 Response (Visa Only) .....	4-202
Subelement 88—Magnetic Stripe Compliance Status Indicator .....	4-202
Subelement 89—Magnetic Stripe Compliance Error Indicator .....	4-203
Subelement 90—Lodging and Auto Rental Indicator .....	4-204
Subelement 90—Custom Payment Service Request (Visa Only).....	4-205
Subelement 90—Custom Payment Service Request Response (Visa Only).....	4-206
Subelement 91—Acquirer Reference Data (American Express Only) .....	4-207
Subelement 91—Custom Payment Service Request Transaction ID (Visa Only).....	4-207
Subelement 91—Custom Payment Service Response Transaction ID (Visa Only) .....	4-208
Subelement 92—CVC 2.....	4-209
Subelement 92—CVV2 Data (Visa Only) .....	4-210
Subelement 93—Fleet Card ID Request Data (Visa Only) .....	4-211
Subelement 94—Commercial Card Inquiry Request (Visa Only) .....	4-212
Subelement 94—Commercial Card Inquiry Response (Visa Only) .....	4-213
Subelement 95—MasterCard Promotion Code.....	4-214
Subelement 95—American Express Customer ID Number (American Express Only) .....	4-215
Subelement 96—Visa Market-Specific Data Identifier (Visa Only).....	4-215
Subelement 97—Prestigious Properties Indicator (Visa Only) .....	4-216
Subelement 98—MasterCard Corporate Fleet Card ID/Driver Number.....	4-217
Subelement 99—MasterCard Corporate Fleet Card Vehicle Number .....	4-218
DE 48—Authorization Platform Edits.....	4-219
DE 49—Currency Code, Transaction .....	4-228

## Table of Contents

---

DE 50—Currency Code, Settlement .....	4-229
DE 51—Currency Code, Cardholder Billing.....	4-231
DE 52—Personal ID Number (PIN) Data.....	4-232
DE 53—Security-Related Control Information.....	4-233
Subfield 1—PIN Security Type Code .....	4-234
Subfield 2—PIN Encryption Type Code .....	4-234
Subfield 3—PIN Block Format Code .....	4-235
Subfield 4—PIN Key Index Number.....	4-235
Subfield 5—Reserved for Future Use.....	4-235
Subfield 6—Reserved for Future Use.....	4-236
DE 54—Additional Amounts.....	4-236
Subfield 1—Account Type .....	4-238
Subfield 2—Amount Type .....	4-238
Subfield 3—Currency Code .....	4-239
Subfield 4—Amount .....	4-239
DE 55—Integrated Circuit Card (ICC) System-Related Data.....	4-240
DE 55—Subelement Encoding Scheme .....	4-240
DE 55—Subelements .....	4-241
DE 55—Authorization Platform Edits.....	4-244
DE 56—Reserved for ISO Use .....	4-246
DE 57—DE 59—Reserved for National Use.....	4-247
DE 60—Advice Reason Code.....	4-247
Subfield 1—Advice Reason Code .....	4-248
Subfield 2—Advice Detail Code.....	4-251
Subfield 3—Advice Detail Text.....	4-264
DE 61—Point-of-Service (POS) Data .....	4-264
Subfield 1—POS Terminal Attendance .....	4-265
Subfield 2—Reserved for Future Use.....	4-265
Subfield 3—POS Terminal Location.....	4-266
Subfield 4—POS Cardholder Presence .....	4-266
Subfield 5—POS Card Presence.....	4-267
Subfield 6—POS Card Capture Capabilities .....	4-267
Subfield 7—POS Transaction Status.....	4-267
Subfield 8—POS Transaction Security.....	4-268
Subfield 9—Reserved for Future Use.....	4-268
Subfield 10—Cardholder-Activated Terminal Level.....	4-269
Subfield 11—POS Card Data Terminal Input Capability Indicator.....	4-269

---

## Table of Contents

Subfield 12—POS Authorization Life Cycle.....	4-270
Subfield 13—POS Country Code .....	4-271
Subfield 14—POS Postal Code.....	4-271
Authorization Platform Edits .....	4-272
DE 62—Intermediate Network Facility (INF) Data .....	4-274
DE 63—Network Data .....	4-276
Subfield 1—Financial Network Code.....	4-277
Subfield 2—Banknet Reference Number .....	4-287
DE 64—Message Authentication Code.....	4-287
DE 65—Bit Map, Extended.....	4-288
DE 66—Settlement Code .....	4-288
DE 67—Extended Payment Code .....	4-289
DE 68—Receiving Institution Country Code.....	4-289
DE 69—Settlement Institution Country Code.....	4-289
DE 70—Network Management Information Code .....	4-290
Network Management Request/0800—Sign-On/Sign-Off .....	4-291
Network Management Request/0800—RiskFinder SAF Request .....	4-292
Network Management Advice/0820—RiskFinder SAF End of File .....	4-293
Network Management Request/0800—Network Connection Status, Member-generated.....	4-293
Network Management Request/0800—Network Connection Status, System-generated.....	4-293
Network Management Request/0800—Host Session Activation/Deactivation.....	4-293
Network Management Request/0800—PEK Exchange.....	4-294
Network Managment Request/0800—PEK Exchange-On Demand.....	4-294
DE 71—Message Number .....	4-294
DE 72—Message Number Last.....	4-294
DE 73—Date, Action.....	4-295
DE 74—Credits, Number .....	4-295
DE 75—Credits, Reversal Number .....	4-296
DE 76—Debits, Number .....	4-296
DE 77—Debits, Reversal Number .....	4-296
DE 78—Transfers, Number .....	4-297
DE 79—Transfers, Reversal Number.....	4-297
DE 80—Inquiries, Number.....	4-298
DE 81—Authorizations, Number.....	4-298

## Table of Contents

---

DE 82—Credits, Processing Fee Amount .....	4-298
DE 83—Credits, Transaction Fee Amount.....	4-299
DE 84—Debits, Processing Fee Amount.....	4-299
DE 85—Debits, Transaction Fee Amount .....	4-300
DE 86—Credits, Amount.....	4-300
DE 87—Credits, Reversal Amount .....	4-300
DE 88—Debits, Amount .....	4-301
DE 89—Debits, Reversal Amount .....	4-301
DE 90—Original Data Elements.....	4-302
Subfield 1—Original Message Type Identifier .....	4-302
Subfield 2—Original DE 11 (Systems Trace Audit Number) .....	4-303
Subfield 3—Original DE 7 (Transmission Date and Time).....	4-303
Subfield 4—Original DE 32 (Acquiring Institution ID Code) .....	4-304
Subfield 5—Original DE 33 (Forwarding Institution ID Code) .....	4-304
DE 91—Issuer File Update Code .....	4-304
DE 92—File Security Code.....	4-305
DE 93—Response Indicator .....	4-305
DE 94—Service Indicator.....	4-306
Subfield 1—Reserved for Future Use.....	4-306
Subfield 2—Acquirer/Issuer Indicator.....	4-307
Subfield 3—Address Data Indicator.....	4-307
DE 95—Replacement Amounts.....	4-308
Subfield 1—Actual Amount, Transaction .....	4-309
Subfield 2—Actual Amount, Settlement .....	4-310
Subfield 3—Actual Amount, Cardholder Billing.....	4-310
Subfield 4—Zero Fill.....	4-310
DE 96—Message Security Code .....	4-311
DE 97—Amount, Net Settlement.....	4-311
Subfield 1—Debit/Credit Indicator .....	4-312
Subfield 2—Amount .....	4-312
DE 98—Payee.....	4-312
DE 99—Settlement Institution ID Code .....	4-313
DE 100—Receiving Institution ID Code.....	4-313
DE 101—File Name .....	4-314
DE 102—Account ID 1 .....	4-315

---

## Table of Contents

DE 103—Account ID 2 .....	4-316
DE 104—Transaction Description .....	4-317
DE 105—DE 111—Reserved for Future Use .....	4-317
DE 112—Additional Data, National Use .....	4-317
DE 112—Encoding Scheme .....	4-318
Cuotas—Payment Transactions .....	4-319
Mexcta—PaymentTransactions .....	4-325
Parcelas—Payment Transactions .....	4-328
Percta—Payment Transactions .....	4-330
Philippines—Payment Transactions .....	4-332
UK Domestic Maestro Transactions .....	4-333
DE 113—Reserved for National Use .....	4-335
Generic Data, Administrative Request/0600 Message .....	4-336
Banking Data, Administrative Request/0600 Message .....	4-338
DE 114—Reserved for National Use .....	4-338
Consumer Application Request Data Administrative Request/0600 Message .....	4-339
Consumer Status Inquiry or Preapproved Offer Inquiry Data Administrative Request/0600 Message .....	4-341
Consumer Account Maintenance Data Administrative Request/0600 Message .....	4-342
Consumer Application Response Data Administrative Request Response/0610 Message .....	4-345
Consumer Account Maintenance Data Administrative Request Response/0610 Message .....	4-347
DE 115—Reserved for National Use .....	4-351
Business Application Request Data Administrative Request/0600 Message .....	4-352
Business Application Status Inquiry Data or Business Preapproved Offer Inquiry Data Administrative Request/0600 Message .....	4-354
Business Account Maintenance Data Administrative Request/0600 Message .....	4-354
Business Application Response Data Administrative Request Response/0610 Message .....	4-357
Business Account Maintenance Data Administrative Request Response/0610 Message .....	4-359
DE 116—Reserved For National Use .....	4-364
Consumer User Lookup Inquiry Data Administrative Request/0600 .....	4-365
Consumer Account Lookup Inquiry Data Administrative Request/0600 Message .....	4-365
Consumer Account Lookup Response Data Administrative Request Response/0610 Message .....	4-366
DE 117—Reserved for National Use .....	4-368
Business User Lookup Inquiry Data Administrative Request/0600 Message .....	4-369

## Table of Contents

---

Business Account Lookup Inquiry Data Administrative Request/0600 Message .....	4-369
Business Account Lookup Response Data Administrative Request Response/0610 Message .....	4-370
DE 118—Reserved for National Use .....	4-372
Authorized User Data Administrative Request/0600 Message .....	4-373
Trade Reference Data Administrative Request/0600 Message .....	4-373
Authorized User Response Data Administrative Request/0610 Message .....	4-374
DE 119—Reserved for National Use .....	4-375
Using DE 113–119 in Administrative 06xx Messages .....	4-376
DE 120—Record Data .....	4-379
Subfield 01—AVS Service Indicator 1.....	4-380
Subfield 02—AVS Service Indicator 2.....	4-380
Subfield 03—AVS Service Indicator 3.....	4-381
Subfield 04—AVS Service Indicator 4.....	4-382
Online File Maintenance.....	4-382
DE 121—Authorizing Agent ID Code .....	4-411
DE 122—Additional Record Data.....	4-412
DE 123—Receipt Free Text.....	4-413
DE 124—Member-defined Data .....	4-414
DE 124—Member-defined Data (General Use).....	4-414
DE 124—Member-defined Data ( <i>MoneySend</i> Only) .....	4-416
DE 124—Member-defined Data (Brazil Maestro Only) .....	4-416
Subfield 1—Unique Reference Number.....	4-416
Subfield 2—Sender/Payer/User ID .....	4-417
Subfield 3—Sender/Payer Address .....	4-417
Subfield 4—Reserved For Future Use .....	4-418
Subfield 6—Discretionary Message on Sales Slip Supported .....	4-418
Subfield 7—Discretionary Message on Sales Slip Code .....	4-419
Subfield 8—Discretionary Message on Sales Slip Content .....	4-419
Subfield 9—Phoneshop (Phone Company ID) .....	4-419
Subfield 10—Phoneshop (Cell Phone Number) .....	4-420
Subfield 11—Phoneshop (Message Security Code) .....	4-420
Subfield 12—Merchant CNPJ Number .....	4-420
Subfield 13—Total Annual Effective Cost .....	4-421
DE 125—New PIN Data.....	4-421
DE 126—Private Data .....	4-422
DE 127—Private Data .....	4-422

---

DE 128—Message Authentication Code.....	4-424
---	-------

## **Chapter 5 Program and Service Format Requirements ..... 5-i**

Product Value Constraints .....	5-1
Permitted Transactions by Card Program.....	5-1
Value Constraints by Transaction Type.....	5-5
Account Status Inquiry Service .....	5-8
Authorization Request/0100—Account Status Inquiry .....	5-10
Authorization Request Response/0110—Account Status Inquiry .....	5-10
Authorization Platform Edits .....	5-11
Address Verification Service.....	5-11
Authorization Request/0100—AVS and Authorization Request .....	5-12
Authorization Request Response/0110—AVS and Authorization Request.....	5-13
Network Management Request/0800—AVS Sign-on .....	5-14
Alternate Processing .....	5-14
DE 48 and DE 120 Structure in AVS Transactions .....	5-14
Authorization Platform Edits .....	5-15
Automated Fuel Dispenser Completion .....	5-16
AFD Message Scenarios .....	5-16
Authorization Request/0100—Automated Fuel Dispenser Completion.....	5-17
Authorization Advice/0120—Acquirer-generated (Automated Fuel Dispenser Completion).....	5-17
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated).....	5-20
Alternate Processing .....	5-20
Account Level Management.....	5-21
Enhanced Value and Product Graduation in Dual Message System Processing.....	5-21
High Value in Dual Message System Processing.....	5-24
ATM Bill Payment Service.....	5-25
Authorization Request/0100—ATM Bill Payment, Europe Acquired.....	5-25
Authorization Request/0100—ATM Bill Payment, Non-Europe Acquired .....	5-26
Authorization Platform Edits .....	5-27
ATM Credit Card Cash Advance in Installments.....	5-27
Authorization Request/0100—ATM Installment Inquiry .....	5-27
Authorization Request Response/0110—ATM Installment Inquiry .....	5-28
Authorization Request/0100—ATM Installment Withdrawal .....	5-29
Authorization Request Response/0110—ATM Installment Withdrawal .....	5-30
Balance Inquiry—ATM.....	5-31

## Table of Contents

---

Authorization Request/0100—ATM Balance Inquiry .....	5-31
Authorization Request/0100—ATM Balance Inquiry Edits .....	5-32
Authorization Request Response/0110—ATM Balance Inquiry .....	5-32
Authorization Request Response/0110—ATM Balance Inquiry Edits .....	5-33
Authorization Advice/0120—Acquirer-generated—ATM Balance Inquiry Edits .....	5-34
Alternate Processing .....	5-34
Balance Inquiry—Point-of-Sale .....	5-34
Authorization Request/0100—POS Balance Inquiry .....	5-35
Authorization Request Response/0110—POS Balance Inquiry .....	5-36
Authorization Request/0100—POS Balance Inquiry Edits .....	5-36
Authorization Request/0110—POS Balance Inquiry Edits .....	5-37
Authorization Advice/0120—Acquirer-generated—POS Balance Inquiry Edits .....	5-38
Alternate Processing .....	5-39
Balance Inquiry—Short Message Service .....	5-39
Authorization Request/0100—Short Message Service Balance Inquiry .....	5-39
Balance Inquiry—Mobile Remote Payments Program .....	5-40
Authorization Request/0100—Mobile Remote Payments Program Balance Inquiry .....	5-40
Chip-Specific Value Constraints .....	5-40
Chip Partial Grade Value Constraints .....	5-41
Chip Full Grade Value Constraints .....	5-42
Contact and Contactless Chip Specific Value Constraints .....	5-42
Card Validation Code 2 .....	5-44
Authorization Request/0100—CVC 2 Verified .....	5-44
Authorization Request/0100—CVC 2 Unverified .....	5-45
Authorization Request/0100—CVC 2 Processed by Stand-In .....	5-46
Authorization Request/0100—CVC 2 Processed by X-Code .....	5-47
Authorization Request/0100—Processed by Limit-1 .....	5-48
CVC 2 DE 48 Structure .....	5-48
Authorization Request/0100—CVC 2 .....	5-49
Authorization Request Response/0110—CVC 2 .....	5-49
Card Validation Code 3 .....	5-50
Authorization Request Response/0110—CVC 3 Result .....	5-50
Currency Conversion .....	5-50
Amount-Related Data Elements in Authorization and Reversal Messages .....	5-51
Dual Message System Processing .....	5-53
Acquirer Send MTIs in Authorization and Reversal Messages .....	5-53

---

Acquirer Receive MTIs in Authorization and Reversal Messages .....	5-54
Issuer Receive MTIs in Authorization and Reversal Messages .....	5-55
Issuer Send MTIs in Authorization and Reversal Messages.....	5-56
Currency Conversion in RiskFinder Transactions.....	5-57
Alternate Processing .....	5-57
Authorization Platform Edits .....	5-58
Electronic Commerce Processing.....	5-60
No Security Protocol.....	5-61
Channel Encryption .....	5-62
Authorization Request/0100—Electronic Commerce Purchase .....	5-63
Authorization Request Response/0110—Electronic Commerce Purchase .....	5-65
Authorization Platform Edits .....	5-65
MasterCard <i>SecureCode</i> .....	5-66
Static AAV and the Maestro and MasterCard Advance Registration Programs.....	5-68
Forgotten Card at ATM.....	5-69
Reversal Request/0400—Forgotten Card.....	5-69
Fraud Scoring Service .....	5-70
Authorization Request/0100—Fraud Scoring .....	5-70
Alternate Processing .....	5-71
Gaming Payment Transactions.....	5-71
Authorization Request/0100—Gaming Payment.....	5-71
Reversal Request/0400—Gaming Payment .....	5-72
Authorization Platform Edits .....	5-73
Maestro Pre-authorized Transactions .....	5-73
Authorization Request/0100—Maestro Pre-Authorization .....	5-73
Authorization Advice/0120—Maestro Pre-Authorization Completion .....	5-74
Maestro Recurring Payments Program .....	5-74
Authorization Request/0100—Maestro Recurring Payment.....	5-76
Authorization Platform Edits .....	5-76
Magnetic Stripe Compliance .....	5-78
Authorization Request/0100—Magnetic Stripe-read.....	5-79
Authorization Request Response/0110—Magnetic Stripe-read.....	5-80
MasterCard Hosted Mobile Phone Top-up ATM Transactions.....	5-80
Authorization Request/0100—MasterCard Hosted Mobile Phone Top-up .....	5-81
Authorization Platform Edits .....	5-82
MasterCard inControl Service.....	5-83
Authorization Request/0100—inControl Purchase Control .....	5-83

## Table of Contents

---

Dual Message System Processing.....	5-84
MasterCard inControl Real Card Spend Control.....	5-86
Process of a MasterCard inControl Service Eligible Transaction .....	5-86
Authorization Request/0100—inControl Real Card Spend Control .....	5-88
Authorization Advice/0120—inControl Real Card Spend Control .....	5-88
MasterCard inControl Virtual Card Mapping and Spend Control Service.....	5-89
Authorization Request/0100—inControl Virtual Card Mapping and Spend Control Service .....	5-89
Exception Processing.....	5-89
MasterCard <i>MoneySend</i> .....	5-90
Authorization Request/0100—MasterCard <i>MoneySend</i> Funding Transactions.....	5-92
Reversal Request/0400—MasterCard <i>MoneySend</i> Funding Transaction .....	5-93
Authorization Platform Edits .....	5-94
Authorization Request/0100—MasterCard <i>MoneySend</i> Payment Transactions.....	5-94
Reversal Request/0400—MasterCard <i>MoneySend</i> Payment Transaction.....	5-95
Authorization Platform Edits .....	5-96
Merchant Advice Codes .....	5-98
Merchant Advice Codes Used with Response Codes .....	5-98
M/Chip Processing Services.....	5-99
Program use of M/Chip Processing Service Data Elements .....	5-100
Chip To Magnetic Stripe Conversion .....	5-101
M/Chip Cryptogram Pre-validation .....	5-105
Combined Service Option.....	5-109
M/Chip Cryptogram Validation in Stand-In Processing.....	5-109
Mobile Remote Payments .....	5-113
Authorization Platform Edits .....	5-114
Partial Approvals.....	5-115
Authorization Request/0100—Partial Approval.....	5-115
Authorization Request Response/0110—Partial Approval.....	5-116
Reversal Request/0400—Partial Approval .....	5-117
Reversal Advice/0420—Partial Approval.....	5-117
Authorization Advice/0120—Issuer-generated (to RiskFinder) .....	5-118
Authorization Advice/0120—Acquirer-generated.....	5-118
Alternate Processing .....	5-119
Authorization Platform Edits .....	5-119
Payment Transactions .....	5-121
Authorization Request/0100—Payment Transaction Message .....	5-121

---

Authorization Request Response/0110—Payment Transaction .....	5-122
Authorization Platform Edits .....	5-123
<i>PayPass CVC 3 Processing Service</i> .....	5-125
Authorization Request/0100—CVC 3 .....	5-126
Dynamic CVC 3 Application Transaction Counter (ATC) Processing .....	5-127
Dynamic CVC 3 Application Transaction Counter (ATC) Information .....	5-128
MCC109 ( <i>PayPass Application Transaction Counter File</i> ) .....	5-128
Card Validation Code Result .....	5-130
Optional Non-valid CVC 3 Processing .....	5-130
ATC Data Extract File .....	5-131
Alternate Processing .....	5-132
<i>PayPass Mapping Service for PayPass M/Chip and Contact M/Chip Transactions</i> .....	5-132
<i>PayPass Mapping Service Processing of PayPass M/Chip and Contact M/Chip Transactions</i> .....	5-133
Authorization Platform Edits .....	5-134
<i>Pay with Rewards Service</i> .....	5-135
Authorization Request/0100—Pay with Rewards .....	5-135
Authorization Request Response/0110—Pay With Rewards .....	5-136
Authorization Platform Edits .....	5-137
<i>PIN Management Service</i> .....	5-140
<i>Chip PIN Management Service</i> .....	5-140
<i>Magnetic Stripe PIN Management Service</i> .....	5-143
<i>PIN Processing for Europe Region Members</i> .....	5-150
PIN Translation Edits .....	5-150
PIN Validation .....	5-151
PIN Validation Edits .....	5-153
PIN Key Management .....	5-156
PIN Verification Value (PVV)/PIN Offset on File Service .....	5-156
<i>PIN Processing for non-Europe Members</i> .....	5-159
Acquirer Requirements .....	5-159
Authorization Request/0100—PIN Transactions .....	5-160
Authorization Request Response/0110—PIN Transactions .....	5-161
Issuer Requirements .....	5-163
Support for Both Acquiring and Issuing Processing .....	5-166
Cleartext Use Prohibited .....	5-166
Emergency Static PEK or Emergency KEK Process .....	5-167
PIN Translation and Verification Process .....	5-170

## Table of Contents

---

Private Label Processing .....	5-177
Authorization Request/0100—Private Label Processing .....	5-177
Private Label with Balance Inquiry .....	5-178
Merchant Verification Service.....	5-178
Co-brand Proprietary Transaction Management Service .....	5-179
Card Activation for Private Label Processing .....	5-181
Card Activation Plus Initial Load for Private Label Processing.....	5-185
Product Inquiry Service .....	5-186
Authorization Request/0100—Product Inquiry Service .....	5-187
Proximity Payments .....	5-187
Authorization Request/0100—Proximity Payments.....	5-187
Purchase of Goods or Services with Cash Back .....	5-189
Authorization Request/0100—Purchase of Goods or Services with Cash Back .....	5-189
Issuer Response Options .....	5-190
Reversal Request/0400 .....	5-191
Reversal Advice/0420.....	5-192
Authorization Advice/0120.....	5-192
Authorization Advice/0120—Acquirer-generated.....	5-193
Alternate Processing .....	5-193
Authorization Platform Edits .....	5-194
Real-time Substantiation.....	5-197
Participation in Real-time Substantiation.....	5-197
Merchant Terminal Verification.....	5-198
Real-time Substantiation Amounts .....	5-198
Transaction Processing Examples .....	5-199
Authorization Platform Edits .....	5-202
Recurring Payment Test Transactions .....	5-204
Reversal Processing.....	5-205
Full Reversals .....	5-205
Partial Reversals .....	5-205
Reversals of Balance Inquiry Transactions.....	5-205
Reversals of Purchase of Goods or Services with Cash Back Transactions.....	5-206
Alternate Processing .....	5-207
Authorization Platform Edits .....	5-208
RiskFinder .....	5-209
Authorization Advice/0120—To RiskFinder .....	5-209
Authorization Advice Response/0130—From RiskFinder.....	5-210

## Table of Contents

---

Network Management/08xx—To and From RiskFinder.....	5-210
Administrative Advice/0620 .....	5-211
Admininistrative Advice Response/0130 .....	5-216
Transaction Blocking .....	5-216
Transaction Block Setup Configuration.....	5-216
Authorization Platform Edits .....	5-217
Transaction Blocking for Inactive BINs .....	5-217
Visa Custom Payment Service .....	5-218
Authorization Request/0100—Visa Custom Payment Service.....	5-218
Authorization Request Response/0110—Visa Custom Payment Service .....	5-219
DE 48 Structure in a Visa Custom Payment Service Transaction.....	5-220
Visa Programs .....	5-221
Visa CVV2 .....	5-221
Visa Fleet Card ID.....	5-222
Visa Commercial Card Inquiry .....	5-223

---

# Chapter 1    Overview

*This section discusses the various conventions that the MasterCard Authorization Platform has adopted from the International Organization for Standardization (ISO) 8583-1987 message formats. Standard message flows are presented for acknowledgements, advices, and error conditions.*

---

The Customer Interface Specification Format .....	1-1
Issuer Post-on Authorization.....	1-2
Bit Mapped Message Encoding Scheme .....	1-3
Authorization Platform Processing Terms and Acronyms .....	1-4
Customer Interface Specification Notations .....	1-4
Data Length Notations .....	1-4
Data Representation Notations.....	1-5
Data Field Notations .....	1-6
Data Justification Notations.....	1-6
Date and Time Notations.....	1-7
Entity Notations .....	1-7
Presence Notations .....	1-8
Presence Requirement Notations .....	1-8
Program and Service Category Notations.....	1-9
Authorization Platform Messages.....	1-10
List of Authorization Messages.....	1-10
Message Type Identifier Presence Requirements by Program and Service .....	1-12
Character Sets .....	1-14
Extended ASCII to Extended EBCDIC Character Set Conversion.....	1-15
Swedish Domestic Authorization Switching Character Set.....	1-18

# The Customer Interface Specification Format

This document contains the MasterCard implementation of the ISO 8583–1987 international message standard for processing authorization information using the MasterCard Dual Message System, Authorization Platform. It provides MasterCard customers with information necessary for development of an application-level online software interface between customer processor systems (CPSs) and the MasterCard Dual Message System.

## Benefits

All programs and services carrying the MasterCard brand use the ISO 8583–1987 message standard.

Benefits of using the ISO 8583–1987 international message standard include:

- Flexibility—Customers may use this interface as a “gateway” vehicle to other credit card and debit card networks. These networks include Visa’s credit and debit card systems; and all major travel and entertainment (T&E) card authorization services. Customers using these gateway capabilities can eliminate the time and expense involved in developing, operating, and maintaining multiple communication links to various regional, national, and international authorization networks in which they may participate.
- Capacity—This interface allows MasterCard and its customers to take full advantage of the MasterCard Worldwide Network. This network features a fully-distributed network architecture at both the application and data-transport (communication network) levels. It provides direct high-speed “peer-to-peer” transaction routing (for example, acquirer-to-issuer), capable of handling several thousands of transactions per second.
- Functionality—MasterCard customers whose proprietary card processing systems support the Authorization Platform standard specified in this document can be assured that their systems will support:
  - All existing MasterCard programs and services, without requiring development of new system interfaces
  - Other national and international networks developed in accordance with ISO 8583–1987 interchange specifications
  - Upgrades related to future revisions of ISO standards

## NOTE

**MasterCard reserves the right to record, store, and use all data transmitted by the MasterCard Dual Message System in online electronic transactions, subject to MasterCard privacy and security compliance policies and applicable laws and regulations, without further notice.**

**NOTE**

**Throughout this document, functional references to “online” indicate an acquirer or issuer that is directly connected to a MasterCard Interface Processor (MIP) and does not imply any Web-based or Internet connection.**

## **Issuer Post-on Authorization**

The Authorization Platform and all MasterCard programs and services employ the “Post-on-Authorization” concept for handling issuer side transaction processing of authorization messages. This concept ensures necessary system integrity and optimizes efficient use of network resources.

The “Post-on-Authorization” concept is far more efficient than the alternative “Post-on-Completion” processing method. **It does not require** Completion Confirmation and Completion Response messages in order for the issuer processing system (IPS) to process Authorization Request/0100 messages. In contrast, the “Post-on-Completion” method **does require** propagation of Completion Confirmation and Completion Response messages between the acquirer and the issuer.

Under the Post-on-Authorization concept, when the Authorization Platform receives an Authorization Request Response/0110 message, it assumes that the issuer’s authorization approval affected the cardholder’s “credit line” or “open-to-buy” limit immediately. The system does not send an Authorization Confirmation message to the issuer. The issuer must assume that the transaction processed normally (**unless advised otherwise** by a Reversal Advice/0420). The Reversal Request/0400 message also may affect Post-on-Authorization processing because it cancels either a part or all of the authorization.

The Authorization Platform sends a response message to the issuer **only** if the Authorization Request Response/0110 message is “late.” This occurs, for example, when the IPS does not respond within the predetermined time (times-out) and the Authorization Platform forwards the message to the Stand-In System to process the transaction on behalf of the issuer. The Authorization Platform then sends the issuer an Authorization Negative Acknowledgement/0190 message, indicating that the Authorization Request Response/0110 message is “unrecognizable”.

If the issuer receives an Authorization Negative Acknowledgement/0190 message, the issuer must assume that the Authorization Platform:

- Timed-out the IPS
- Immediately went to the Stand-In System or alternate authorizer processing to service this transaction

If the issuer does not select Stand-In options, the Authorization Platform automatically sends an Authorization Request Response/0110 message to the acquirer with a negative response code (“transaction request denied”). **The issuer always must reverse any effect upon the cardholder’s account.** Later, the issuer receives an Authorization Advice/0120 message indicating the specific action taken by the Stand-In System.

#### NOTE

**The term “post” in Post-on-Authorization does not refer to actual posting of cardholder accounts for billing purposes. Post-on-Authorization refers only to the technique used to maintain accurate settlement reconciliation totals between the Authorization Platform and any attached CPS. The IPS handles actual posting of cardholder account data for cardholder billing purposes. Posting of the cardholder account data is not an Authorization Platform function.**

## Bit Mapped Message Encoding Scheme

A description of the bit map scheme.

All customer interface specification (CIS) messages are variable-length, with a bit map scheme used as the first data element(s) of the message following the Message Type Identifier (MTI) to indicate the presence or absence of additional data elements in the message. Each bit map is a 64-bit string contained within an eight-byte data element. The first bit in each bit map is 1 or 0 to indicate the presence or absence of another (immediately following) bit map data element.

The Authorization Platform uses a maximum of two-bit maps: a “Primary” and a “Secondary” Bit Map. Bits 1 or 0 in the Primary Bit Map indicate the presence or absence of DE 2 (Primary Account Number [PAN]) through DE 64 (Message Authentication Code [MAC]). Bits 1 or 0 in the Secondary Bit Map indicate the presence or absence of DE 66 (Settlement Code) through DE 128 (Message Authentication Code [MAC]).

#### NOTE

**All bit positions are interpreted from left to right within each bit map. For example, within the Primary Bit Map, the leftmost bit is “bit number 1” and the rightmost bit is “bit number 64.”**

Bit number 1 in the Primary Bit Map and bit number 65 in the Secondary Bit Map (that is, the first bit in each bit map) do not have corresponding data elements. These bits indicate the presence or absence of additional data elements in the message. If bit number 1 is 1, the Secondary Bit Map is present and selected data elements in the range DE 66–DE 128 exist in the Secondary Bit Map of the message. Bit number 65 **must always be 0** because no additional bit maps are defined beyond the Secondary Bit Map.

Each message **must** contain the Primary Bit Map. The Secondary Bit Map must be included only if data elements DE 66–DE 128 are present in the message.

## Authorization Platform Processing Terms and Acronyms

Authorization Platform processing terms and acronyms are used in describing the logical flow of an Authorization Platform message from one point to another.

The following Authorization Platform terms or acronyms are used in describing the CIS message format:

- Acquirer processing system (APS)
- Customer processing system (CPS)
- Issuer processing system (IPS)
- Point of Sale (POS)

## Customer Interface Specification Notations

The Customer Interface Specification notations describe the Customer Interface Specification (CIS) format.

The CIS format is described with the following notations:

- Data Length
- Data Representation
- Date and Time
- Entities
- Presence
- Presence Requirements

### Data Length Notations

Data length notations indicate the format of the data length.

<b>Notation</b>	<b>Description</b>
All length fields are encoded as numeric EBCDIC, right-justified with leading zeros. If a customer sends ASCII, it is converted to EBCDIC and back to ASCII again if needed.	
-digit(s)	Fixed length in number of positions.  Example: “n-3” indicates a three-position numeric data element.
	Example: “an-10” indicates a 10-position alphanumeric data element.
...digit(s)	Variable length, with maximum number of positions specified.  Example: “n...11” indicates a variable-length numeric data element of 1–11 digits.

<b>Notation</b>	<b>Description</b>
	Example: “an...25” indicates a variable-length alphanumeric data element of 1–25 positions.
LLVAR	Present with a variable-length data element attribute, indicates that the data element contains two fields:
LL	The length field and represents the number of positions in the variable-length data field that follows. The length field contains a value in the range 01–99.
VAR	The variable-length data field Example: “an...25; LLVAR” represents a variable-length alphanumeric data element with a length of 1–25 positions.
LLLVAR	Present with a variable-length data element attribute, indicates that the data element contains two fields:
LLL	The length field and represents the number of positions in the variable-length data field that follows. The length field contains a value in the range 001–999.
VAR	The variable-length data field Example: “an...500; LLLVAR” indicates a variable-length alphanumeric data element having a length of 1–500 positions.

## Data Representation Notations

Data representation notations indicate how data is represented. All message data elements are aligned on byte boundaries. The following data types are encoded using EBCDIC or ASCII display character representation, except for binary data.

<b>Notation</b>	<b>Description</b>
a	alphabetic characters A–Z and a–z
n	numeric digits 0–9
an	alphabetic and numeric characters (excluding spaces and special characters)
ans	alphabetic, numeric, space, and special characters
b	space

## Overview

### Customer Interface Specification Notations

---

Notation	Description
b	binary representation of data in eight-bit bytes All binary data elements are constructed of bit-strings that have lengths that are an integral number of eight-bit bytes. No binary data element has a length of less than eight bits (one byte) “b-8” indicates a fixed-length binary field of eight characters (eight bytes, 64 bits).
s	special character
ns	numeric and special characters

All track 2 or track 3 (attribute “ans”) data elements are encoded as EBCDIC representations of the hexadecimal data specified in the ISO 7811 and 7812 specifications. Thus, a hexadecimal “D” (binary 1101) is encoded as an EBCDIC “D” character, and so forth. The “LL” or “LLL” length specification associated with these data elements specifies the data element length in number of **bytes**.

## Data Field Notations

Data field notations indicate where the data exists in the data element.

Notation	Description
Contents of subfields	Subfield number or number range Example: Contents of subfields 1–8
Contents of position(s)	Position number or number range Example: Contents of positions 1–8
N/A	Not applicable

## Data Justification Notations

Data justification indicates the position of the data in the data element.

Notation	Description
Left	Data is left justified
Right	Data is right justified
See subfields	Data justification is defined in the subfield description indicating the subfield justification may vary between subfields
N/A	Not applicable

## Date and Time Notations

Date and time notations indicate the format of the data that represents date and time.

Notation	Description
MM	month (two digits; 01–12)
DD	day (two digits; 01–31)
YY	year (last two digits of calendar year; 00–99)
hh	hour (two digits; 00–23)
mm	minute (two digits; 00–59)
ss	second (two digits; 00–59)

## Entity Notations

Entity notations identify who is responsible for a message (acquirer, issuer, processor, or the Authorization Platform) at any given point.

### Purpose

Several entities may insert or modify data elements in an Authorization Platform message as it flows from the message origin to the Authorization Platform and from the Authorization Platform to the message destination. These entities typically include the customer or processor at the origin, the Authorization Platform, and the customer or processor at the destination. In the message format layouts, the following three entities provide information to the originator, the Authorization Platform, and destination related to the data element requirements.

### Notations

Notation	Description
Org	Originator Requirements. The message originator must satisfy this data element's requirements. Examples of originators include acquirers sending Authorization Request/0100 or Network Management Request/0800 messages.
Sys	Authorization Platform Requirements. The Authorization Platform may insert, correct, modify, or echo this data element while, for example, routing a message from the origin to the destination. The Authorization Platform may overwrite the data element and thereby destroy any previous content.
Dst	Destination Requirements. The message destination must expect this data element (read it) and accept this data element (process it) if the originator requirements are satisfied. Examples of destinations include issuers receiving Authorization Request/0100 or Network Management Request/0800 messages.

## Presence Notations

Presence notations indicate if and how data is present. These notations appear in the originator (Org), Authorization Platform (Sys), and destination (Dst).

Notation	Description
M	Mandatory. The data element is required in the message.
C	Conditional. The data element is required in the message if the conditions described in the accompanying text apply.
O	Optional. The data element is not required, but may be included in the message at the message initiator's option.
X	Authorization Platform. The Authorization Platform may (or will) insert or overwrite the data element, depending on specific Authorization Platform support services provided for individual programs and services.
ME	Mandatory Echo. The data element is required in a response message and must contain the same value ("echoed") from the original request or advice message.
CE	Conditional Echo. The data element is required in a response message if it was present in the original request or advice message, and it must contain the same value ("echoed") from the original message.
XE	Authorization Platform Echo. The data element must contain the value from the original request or advice (echoed), if present.
• or N/A	Not Required or Not Applicable. The data element is not required or is not applicable. The transaction originator should not include this data element if this code is present in the "Org" column.

## Presence Requirement Notations

Presence requirement notations describe the possible presence or usage requirements. An entity presence requirement is the three combined values in the originator (Org), Authorization Platform (Sys), and destination (Dst).

Org	Sys	Dst	Description
M	•	M	Mandatory; originator must provide the data element.
M	X	M	Mandatory; originator must provide the data element; Authorization Platform adjusts/appends data.
C	•	C	Conditionally required; conditions are described in Comments column.
C	X	C	Conditionally required; Authorization Platform adjusts/appends data.
•	X	C	Authorization Platform provides the data element conditionally.

<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Description</b>
•	X	M	Authorization Platform always provides the data element.
O	•	C	Optional; originator may provide the data element.
O	X	C	Optional; originator may provide the data element; Authorization Platform adjusts/appends data.
M	•	•	Mandatory; originator must provide the data element; Authorization Platform does not forward data.
C	•	•	Conditionally required; Authorization Platform does not forward data.
O	•	•	Optional; Authorization Platform does not forward data.
•	X	•	MasterCard use only.

## Program and Service Category Notations

Program and Service Category notations identify the various programs and services.

<b>Notation</b>	<b>Description</b>
MC	All MasterCard activity the Authorization Platform processes.
NP	Network processing services activity (often referred to as private label activity) the Authorization Platform processes that does not fall into one of the following categories: MasterCard (MC), Visa (VI), and Travel and Entertainment (TE).  <b>This specification indicates the “most general” Authorization Platform data element requirements for private label activity.</b>  Processors that support all these general data element specifications are able to access or participate in any Authorization Platform credit card or debit card gateway. For detailed information on specific gateways, refer to the appropriate program or service user manual.
VI	Visa activity the Authorization Platform processes.  <b>This specification includes Authorization Platform requirements for accepting Visa activity.</b>
TE	Travel and Entertainment (T&E) card activity the Authorization Platform processes that does not fall into one of the following categories: MasterCard (MC), network processing services activity (NP), and Visa (VI).  <b>This specification includes Authorization Platform interface requirements for Travel and Entertainment (T&amp;E) card activity, including American Express, and Diners Club.</b>
MS	Maestro card transactions that the Authorization Platform processes.
CI	Cirrus card transactions that the Authorization Platform processes.

## Overview

### Authorization Platform Messages

---

## Authorization Platform Messages

Authorization Platform messages are those financial transaction messages used to transmit authorization, file update, reversal, administrative, and network management data across the MasterCard Worldwide Network.

The Authorization Platform supports the following financial transaction message types:

- Authorization/01xx messages
- Issuer File Update/03xx messages
- Reversal/04xx messages
- Administrative/06xx messages
- Network Management/0800 messages

## List of Authorization Messages

The following table lists the message types the Authorization Platform supports and indicates the entities that each message type originates with. The Authorization Platform may not support all message types for each MasterCard program or service.

MTI	Description	Acquirer	Issuer	Authorization Platform
<b>Authorization/01xx messages</b>				
0100	Authorization Request	✓		
0110	Authorization Request Response		✓	✓
0120	Authorization Advice—Acquirer-generated	✓		
0120	Authorization Advice—Issuer-generated		✓	✓
0120	Authorization Advice—System-generated			✓
0130	Authorization Advice Response—Issuer-generated (Responding to an Acquirer-generated 0120)			✓
0130	Authorization Advice Response—Issuer-generated (Responding to a System-generated 0120 from SAF)			✓
0130	Authorization Advice Response—System-generated			✓
0180	Authorization Response Acknowledgement	✓		
0190	Authorization Response Negative Acknowledgement			✓
<b>Issuer File Update/03xx messages</b>				

**Overview**  
**List of Authorization Messages**

---

<b>MTI</b>	<b>Description</b>	<b>Acquirer</b>	<b>Issuer</b>	<b>Authorization Platform</b>
0302	Issuer File Update Request			✓
0312	Issuer File Update Request Response			✓
<b>Reversal/04xx messages</b>				
0400	Reversal Request		✓	
0410	Reversal Request Response		✓	✓
0420	Reversal Advice			✓
0430	Reversal Advice Response		✓	
<b>Administrative/06xx messages</b>				
0600	Administrative Request		✓	
0610	Administrative Request Response		✓	
0620	Administrative Advice	✓	✓	✓
0630	Administrative Advice Response	✓	✓	
<b>Network Management/08xx messages</b>				
0800	Network Management Request—Sign-On/Sign-Off <sup>1</sup>	✓	✓	
0800	Network Management Request—SAF Request		✓	
0800	Network Management Request—RiskFinder SAF Request		✓	
0800	Network Management Request—Network Connection Status, Member-generated	✓	✓	
0800	Network Management Request—Network Connection Status, System-generated			✓
0800	Network Management Request—Host Session Activation/Deactivation	✓	✓	✓
0800	Network Management Request—PEK Exchange			✓
0800	Network Management Request—PEK Exchange—On Demand	✓	✓	
0810	Network Management Request Response—Sign-On/Sign-Off			✓

- 
1. Because the MasterCard Worldwide Network does not track session status information for an acquirer, Authorization Platform sign-on/sign-off for acquirers is not required. However, acquirers optionally may send Authorization Platform sign-on/sign-off messages (for example, if required by vendor software.)

## Overview

### Message Type Identifier Presence Requirements by Program and Service

MTI	Description	Acquirer	Issuer	Authorization Platform
0810	Network Management Request Response—SAF Request			✓
0810	Network Management Request Response—RiskFinder SAF Request			✓
0810	Network Management Request Response—Network Connection Status, Member-generated	✓	✓	
0810	Network Management Request Response—Network Connection Status, System-generated			✓
0810	Network Management Request Response/—Host Session Activation/Deactivation	✓	✓	✓
0810	Network Management Request Response/—PEK Exchange	✓	✓	
0810	Network Management Request Response/—PEK Exchange—On Demand			✓
0820	Network Management Advice—RiskFinder SAF End of File <sup>2</sup>			✓
0820	Network Management Advice—PEK Exchange			✓

### Message Type Identifier Presence Requirements by Program and Service

The following table lists the message type indicator (MTI) presence requirements for each authorization message type as it relates to the card program categories.

MTI	Description	MC	NP	VI	TE	MS	CI
0100	Authorization Request	✓	✓	✓	✓	✓	✓
0110	Authorization Request Response	✓	✓	✓	✓	✓	✓
0120	Authorization Advice—Acquirer-generated	✓	✓	•	•	✓	✓
0120	Authorization Advice—Issuer-generated	✓	✓	✓	✓	✓	✓
0120	Authorization Advice—System-generated	✓	✓	✓	✓	✓	✓
0130	Authorization Advice Response—Issuer-generated (Responding to an Acquirer-generated 0120)	✓	✓	✓	✓	✓	✓

2. The Authorization Platform does not support a Network Management Advice Acknowledgement/0830 message that responds to a Network Management Advice/0820 message.

**Overview**  
**Message Type Identifier Presence Requirements by Program and Service**

<b>MTI</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
0130	Authorization Advice Response—Issuer-generated (Responding to a System-generated 0120 from SAF)	✓	✓	✓	✓	✓	✓
0130	Authorization Advice Response—System-generated	✓	✓	✓	✓	✓	✓
0180	Authorization Acknowledgement	X	X	X	X	X	X
0190	Authorization Negative Acknowledgement	✓	✓	✓	✓	✓	✓
0302	Issuer File Update Request	✓	✓	•	•	✓	✓
0312	Issuer File Update Request Response	✓	✓	•	•	✓	✓
0400	Reversal Request/0400	✓	✓	✓	•	✓	✓
0410	Reversal Request Response/0410	✓	✓	✓	•	✓	✓
0420	Reversal Advice	✓	✓	✓	•	✓	✓
0430	Reversal Advice Response	✓	✓	✓	•	✓	✓
0600	Administrative Request/0600	✓	✓	•	•	•	•
0610	Administrative Request Response/0610	✓	✓	•	•	•	•
0620	Administrative Advice	✓	✓	✓	•	✓	✓
0630	Administrative Advice Response	✓	✓	✓	•	✓	✓
0800	Network Management Request	✓	✓	✓	✓	✓	✓
0810	Network Management Request Response	✓	✓	✓	✓	✓	✓
0820	Network Management Advice	✓	✓	✓	✓	✓	✓

**Table Key:**

✓ = The MTI must be provided for the program or service indicated.

X = Optional support (for example, when individual MasterCard customers may elect to support certain message types at their own discretion.)

• = The MTI is unavailable for the program or service

## Character Sets

Character sets define how letters, numbers, symbols, and special characters are displayed in computer text.

### What Character Sets does MasterCard Support?

MasterCard supports the following code pages for both standard and extended character sets:

- ASCII (ISO 8859-1)
- EBCDIC (Code Page 1047)

MasterCard supports standard EBCDIC formatted messages and bulk files. In addition to standard EBCDIC, MasterCard also supports the extended EBCDIC format as well as the standard and extended ASCII format for both authorization messages and selected bulk files. Members using the MIP to transmit bulk files will still need to adhere to the existing MasterCard File Transfer Protocol format—that is, EBCDIC (for Header and Trailer information).

**Extended characters: Within the full character set, the alphabet is represented as used in the English language (with no character “enhancements”) and also the characters that may be found, for example, in the Spanish alphabet where the tilde is used over the Á.**

MasterCard uses extended EBCDIC as the default character set type for sending messages unless otherwise specified by the customer.

Members also have the option to send and receive either standard or extended character sets for both ASCII and EBCDIC formats in specific data elements that contain text. Following are examples of some data elements that may contain standard or extended text characters:

- DE 42 (Card Acceptor ID Code)
- DE 43 (Card Acceptor Name/Location)
- DE 120 (Record Data)
- DE 123 (Receipt Free Text)
- DE 124 (Member-defined Data)

The following bulk files will be supported in ASCII:

- R311—AMS File Updates
- R361—AMS File Updates (TEST)

Members that want to receive messages in standard EBCDIC or extended or standard ASCII must inform MasterCard.

## Extended ASCII to Extended EBCDIC Character Set Conversion

Following is the list of how the extended ASCII character set is converted or mapped to the extended EBCDIC character set.

<b>ASCII Decimal Value</b>	<b>ASCII Hexadecimal Value</b>	<b>EBCDIC Decimal Value</b>	<b>EBCDIC Hexadecimal Value</b>	<b>Character Representation</b>	<b>Definition</b>
192	C0	100	64	À	Capital A, grave accent
193	C1	101	65	Á	Capital A, acute accent
194	C2	98	62	Â	Capital A, circumflex accent
195	C3	102	66	Ã	Capital A, tilde
196	C4	99	63	Ä	Capital A, dieresis or umlaut mark
197	C5	103	67	Å	Capital A, ring
198	C6	158	9E	Æ	Capital AE diphthong
199	C7	104	68	Ç	Capital C, cedilla
200	C8	116	74	È	Capital E, grave accent
201	C9	113	71	É	Capital E, acute accent
202	CA	114	72	Ê	Capital E, circumflex accent
203	CB	115	73	Ë	Capital E, dieresis or umlaut mark
204	CC	120	78	Ì	Capital I, grave accent
205	CD	117	75	Í	Capital I, acute accent
206	CE	118	76	Î	Capital I, circumflex accent
207	CF	119	77	Ï	Capital I, dieresis or umlaut mark
208	D0	172	AC	Ð	Capital Eth, Icelandic
209	D1	105	69	Ñ	Capital N, tilde
210	D2	237	ED	Ò	Capital O, grave accent
211	D3	238	EE	Ó	Capital O, acute accent
212	D4	235	EB	Ô	Capital O, circumflex accent

## Overview

### Character Sets

---

ASCII Decimal Value	ASCII Hexadecimal Value	EBCDIC Decimal Value	EBCDIC Hexadecimal Value	Character Representation	Definition
213	D5	239	EF	Ø	Capital O, tilde
214	D6	236	EC	Ö	Capital O, dieresis or umlaut mark
215	D7	191	BF	×	Multiply sign
216	D8	128	80	Ø	Capital O, slash
217	D9	253	FD	Ù	Capital U, grave accent
218	DA	254	FE	Ú	Capital U, acute accent
219	DB	251	FB	Û	Capital U, circumflex accent
220	DC	252	FC	Ü	Capital U, dieresis or umlaut mark
221	DD	186	BA	Ý	Capital Y, acute accent
222	DE	174	AE	Þ	Capital THORN, Icelandic
223	DF	89	59	ß	Small sharp s, German (sz ligature)
224	E0	68	44	à	Small a, grave accent
225	E1	69	45	á	Small a, acute accent
226	E2	66	42	â	Small a, circumflex accent
227	E3	70	46	ã	Small a, tilde
228	E4	67	43	ä	Small a, dieresis or umlaut mark
229	E5	71	47	å	Small a, ring
230	E6	156	9C	æ	Small ae diphthong (ligature)
231	E7	72	48	ç	Small c, cedilla
232	E8	84	54	è	Small e, grave accent
233	E9	81	51	é	Small e, acute accent
234	EA	82	52	ê	Small e, circumflex accent
235	EB	83	53	ë	Small e, dieresis or umlaut mark
236	EC	88	58	í	Small i, grave accent

<b>ASCII Decimal Value</b>	<b>ASCII Hexadecimal Value</b>	<b>EBCDIC Decimal Value</b>	<b>EBCDIC Hexadecimal Value</b>	<b>Character Representation</b>	<b>Definition</b>
237	ED	85	55	í	Small i, acute accent
238	EE	86	56	î	Small i, circumflex accent
239	EF	87	57	ï	Small i, dieresis or umlaut mark
240	F0	140	8C	ð	Small eth, Icelandic
241	F1	73	49	ñ	Small n, tilde
242	F2	205	CD	ò	Small o, grave accent
243	F3	206	CE	ó	Small o, acute accent
244	F4	203	CB	ô	Small o, circumflex accent
245	F5	207	CF	õ	Small o, tilde
246	F6	204	CC	ö	Small o, dieresis or umlaut mark
247	F7	225	E1	÷	Division sign
248	F8	112	70	ø	Small o, slash
249	F9	221	DD	ù	Small u, grave accent
250	FA	222	DE	ú	Small u, acute accent
251	FB	219	DB	û	Small u, circumflex accent
252	FC	220	DC	ü	Small u, dieresis or umlaut mark
253	FD	141	8D	ý	Small y, acute accent
254	FE	142	8E	þ	Small thorn, Icelandic
255	FF	223	DF	ÿ	Small y, dieresis or umlaut mark

## **Swedish Domestic Authorization Switching Character Set**

Members using the Swedish Domestic Authorization Switching Service (SASS) also may support Swedish national characters in EBCDIC as described in the following table.

<b>EBCDIC IBM-278</b>	<b>EBCDIC (Hexadecimal)</b>	<b>ASCII (Hexadecimal)</b>	<b>Graphic</b>	<b>Attribute</b>
Å	5B	24	\$	s
Ä	7B	23	#	s
Ö	7C	40	@	s
å	D0	7d	}	s
ä	C0	7b	{	s

---

## Chapter 2    Message Definitions and Flows

*This section provides message definitions of all message types the Authorization Platform uses followed by the detailed message flow diagrams that illustrate both the standard and exception (error condition) message processing.*

---

About Message Definitions .....	2-1
About Authorization Messages.....	2-1
Authorization Request/0100.....	2-1
Authorization Request Response/0110.....	2-2
About Authorization Advice Messages.....	2-2
Authorization Advice/0120—Acquirer-generated.....	2-3
Authorization Advice/0120—Issuer-generated.....	2-3
Authorization Advice/0120—System-generated .....	2-4
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120).....	2-4
Authorization Advice Response/0130—Issuer-generated (Responding to a System-generated 0120 from SAF) .....	2-4
Authorization Advice Response/0130—System-generated .....	2-4
About Authorization Response Acknowledgement Messages.....	2-5
Authorization Acknowledgement/0180.....	2-5
Authorization Negative Acknowledgement/0190.....	2-5
About Issuer File Update Messages .....	2-6
Issuer File Update Request/0302 .....	2-6
Issuer File Update Request Response/0312 .....	2-6
About Reversal Messages.....	2-6
Reversal Request/0400 .....	2-7
Reversal Request Response/0410 .....	2-7
Reversal Advice/0420.....	2-7
Reversal Advice Response/0430.....	2-7
About Administrative Messages .....	2-8
Administrative Request/0600.....	2-8
Administrative Request Response/0610 .....	2-8
Administrative Advice/0620 .....	2-9
Administrative Advice Response/0630 .....	2-10
About Network Management Messages .....	2-10
Network Management Request/0800 .....	2-11
Network Management Request Response/0810 .....	2-11

## Message Definitions and Flows

---

Network Management Advice/0820 .....	2-11
About Message Flows .....	2-12
Authorization Message Routing Timers.....	2-12
Authorization Request/0100 and Authorization Request Response/0110.....	2-13
Authorization Request/0100—Communication Failure at Acquirer.....	2-14
Authorization Request/0100—Communication Failure at Issuer.....	2-15
Authorization Request Response/0110—Communication Failure at Acquirer.....	2-17
Authorization Request Response/0110—Communication Failure at Issuer.....	2-19
Authorization Request Response/0110—Stand-In System Allowed.....	2-21
Authorization Request Response/0110—Not Received within the Time Limit.....	2-22
Authorization Request Response/0110—Received within the Time Limit but after Stand-In System Response .....	2-24
Authorization Request Response/0110—Received within the Time Limit and before Stand-In System Response .....	2-26
Authorization Request Response/0110—Not Eligible for Alternate Processing.....	2-27
Authorization Request Response/0110—No Issuer Response within Issuer Response Time Limit.....	2-27
Authorization Request Response/0110—Late Issuer Response .....	2-29
Authorization Request Response/0110—Issuer Edit Error .....	2-30
Authorization Request/0100—Chip PIN Management .....	2-31
Authorization Request/0100—Chip PIN Management (Failure to Transmit/Apply Script to Chip Card) .....	2-33
Authorization Request/0100—Chip PIN Management (Issuer Network Failure-Unable to Connect) .....	2-35
Authorization Request/0100—Chip PIN Management (Issuer Network Failure, No Response from Issuer) .....	2-36
Authorization Request/0100—Chip PIN Management (Acquirer Network Failure-Unable to Connect) .....	2-38
Authorization Request/0100—Chip PIN Management (Acquirer Network Failure-Unable to Connect with Acquirer).....	2-39
Guaranteed Advice Message Delivery.....	2-41
Standard Advice Delivery—All Advice Message Types.....	2-42
Authorization Advice/0120—Acquirer-generated, Issuer Available .....	2-43
Authorization Advice/0120—Acquirer-generated, Issuer Unavailable .....	2-44
Authorization Advice/0120—Issuer-generated .....	2-45
Authorization Advice/0120—System-generated .....	2-46
Advice Message Error Condition.....	2-47
Acquirer Response Acknowledgement/0180 Messages.....	2-49
Alternate Issuer Host Processing for Online Europe Region Members .....	2-50

---

Authorization Request/0100—Communication Failure at Issuer (Issuer is not signed in or transaction cannot be delivered) .....	2-51
Authorization Request Response/0110—Alternate Issuer Allowed .....	2-52
Authorization Request Response/0110—Not Received within Time Limit .....	2-54
Authorization Request Response/0110—Received within the Time Limit but after Alternate Issuer Response .....	2-56
Authorization Request Response/0110—Received within the Time Limit and before Alternate Issuer Response .....	2-58
Authorization Response Negative Acknowledgement/0190 (Responding to the Authorization Request Response/0110) .....	2-59
Authorization Response Negative Acknowledgement/0190 (Responding to the Reversal Request Response/0410) .....	2-60
Issuer File Update Request/0302 and Issuer File Update Request Response/0312 .....	2-61
Reversal Messages.....	2-62
Reversal Request/0400 and Reversal Request Response/0410 .....	2-63
Reversal Request/0400—No Issuer Response Received within the Time Limit .....	2-64
Reversal Request/0400—Issuer Response Received after the Time Limit .....	2-65
Reversal Request/0400—Issuer Signed Off .....	2-66
Reversal Request/0400—Issuer Response Contains Errors.....	2-67
Reversal Request/0400—Not Delivered to Issuer.....	2-68
Reversal Request Response/0410—Not Delivered to Acquirer .....	2-69
Reversal Advice/0420 and Reversal Advice Response/0430.....	2-70
Administrative Request/0600 and Administrative Request Response/0610 .....	2-71
Administrative Request/0600, Acquirer Edit Failure.....	2-72
Administrative Request/0600, Communication Failure at Issuer .....	2-73
Administrative Request Response/0610, Communication Failure at Acquirer.....	2-74
Administrative Request Response/0610, No Issuer Response .....	2-75
Administrative Request Response/0610, Late Issuer Response .....	2-76
Administrative Request Response/0610, Issuer Edit Failure .....	2-77
Administrative Advice/0620 and Administrative Advice Response/0630.....	2-78
Administrative Advice/0620 and Administrative Advice Response/0630—Invalid Message, System-generated .....	2-79
Administrative Advice/0620 and Administrative Advice Response/0630—RiskFinder, System-generated .....	2-80
Network Management Request 0800—Sign-On/Sign-Off.....	2-81
Network Management Request/0800—RiskFinder Sign-On/Sign-Off.....	2-82
Network Management Request/0800—Solicited SAF .....	2-83
Network Management Request/0800—Unsolicited SAF .....	2-84
Network Management Request/0800—RiskFinder SAF.....	2-85

## **Message Definitions and Flows**

---

Network Management Request/0800—Network Connection Status, Member-generated.....	2-86
Network Management Request/0800—Network Connection Status, System-generated.....	2-87
Network Management Request/0800—Host Session Activation/Deactivation.....	2-88
Network Management Request/0800—PEK Exchange Authorization Platform-Initiated .....	2-89
Network Management Request/0800—PEK Exchange Member-Initiated.....	2-90

## About Message Definitions

Message definitions describe the general purpose, type, routing, and response information of each Authorization Platform message type.

### About Authorization Messages

The authorization message definitions define the authorization request, advice, and response message types.

Authorization/01xx messages transport authorization-related information. “Authorization” is a term applied to transactions for which, by design, there is partial transaction data contained within the individual messages; no actual posting of accounts at the issuer processing system (IPS) occurs during this type of transmission. Consequently, all Authorization/01xx messages and advice transactions assume that follow-up information (for example, paper or electronic clearing transactions) will be used to effect actual settlement, cardholder account posting, and cardholder billing.

Authorization/01xx messages are defined as:

- Authorization Request messages
- Authorization Advice messages
- Authorization Response Acknowledgement messages

### Authorization Request/0100

The Authorization Request/0100 message requests approval authorization or guarantee for a transaction to proceed. The Authorization Request/0100 message is not intended to permit the application of this transaction to the cardholder’s account for issuing a bill or statement.

---

Type	Interactive
Routing	<ul style="list-style-type: none"><li>• From an acquirer processor system (APS) to the Authorization Platform.</li><li>• From the Authorization Platform to an IPS.</li></ul>
Response	An Authorization Request Response/0110 message is required.

---

## Message Definitions and Flows

### About Message Definitions

---

#### Authorization Request Response/0110

The Authorization Request Response must be sent in response to an Authorization Request/0100 message; it carries the response information required to service (approve or deny) the Authorization Request/0100 message.

Type	Interactive
Routing	<ul style="list-style-type: none"><li>• From an IPS to the Authorization Platform.</li><li>• From the Authorization Platform to an APS.</li></ul>
Response	The APS may provide an Authorization Acknowledgement/0180 message to the Authorization Platform to acknowledge positive receipt of the Authorization Request Response/0110 message from the Authorization Platform. <b>The Authorization Acknowledgement/0180 message is optional for an APS.</b>

#### About Authorization Advice Messages

The Authorization Platform uses guaranteed advice message delivery for all advice messages transmitted using the Authorization Platform.

Guaranteed advice message delivery provides a message routing facility. When an advice message is forwarded to the Authorization Platform, the Authorization Platform:

- Immediately secures the transaction for future delivery
- Responds to the advice message initiator with an advice response message, indicating that it received and secured the message
- Forwards the advice message to the appropriate receiving entity

The Authorization Platform guarantees the delivery of all advice messages routed through the MasterCard Worldwide Network. Occasionally, the Authorization Platform cannot immediately deliver an advice message (for example, because of a system or communication failure at the destination). In this case, the Authorization Platform stores the message on its store-and-forward (SAF) processing facilities and automatically delivers the message when communication is restored.

The receiver of an advice message must acknowledge receipt with an appropriate advice response message. When the Authorization Platform receives the advice response message, MasterCard considers advice delivery complete and removes the message from SAF processing queues.

The Guaranteed Advice Message Delivery messages include:

- Authorization Advice/0120—Acquirer-generated
- Authorization Advice/0120—Issuer-generated (to RiskFinder)
- Authorization Advice/0120—System-generated

- Authorization Advice Response/0130—Issuer-generated (Responding to a System-generated 0120 from SAF)
- Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)
- Authorization Advice Response/0130—Issuer-generated (Responding to a System-generated 0120 from SAF)
- Authorization Advice Response/0130—System-generated

### **Authorization Advice/0120—Acquirer-generated**

The Authorization Advice/0120—Acquirer-generated message advises of an authorization that was carried out on the issuer's behalf. It is not intended to permit the application of this transaction to the cardholder's account for issuing a bill or statement; for example, this is a “non-posting” advice message.

Type	Noninteractive
Routing	From the APS to an IPS.
Response	An Authorization Advice Response/0130—Issuer-generated message is required.

### **Automated Fuel Dispenser**

Acquirers of Automated Fuel Dispenser (AFD) merchants send an Authorization Advice/0120 message containing DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code), value 191 (Acquirer Processing System [APS] Completed Authorization Transaction) to the issuer providing the actual transaction amount for each approved AFD transaction.

### **Authorization Advice/0120—Issuer-generated**

Authorization Request/0100 messages may contain Bank Identification Number (BINs) that customers have selected for scoring. For these transactions, issuers create and send Authorization Advice/0120 messages to the RiskFinder™ scoring system. The RiskFinder scoring system sends to the issuer an Authorization Advice Response/0130 to acknowledge receipt of the Authorization Advice/0120.

Type	Noninteractive
Routing	From the IPS to the Authorization Platform.
Response	An Authorization Advice Response/0130—System-generated message is required.

## **Message Definitions and Flows**

### **About Message Definitions**

---

#### **Authorization Advice/0120—System-generated**

The Authorization Advice/0120—System-generated message advises of an authorization that was carried out on the issuer's behalf. It is not intended to permit the application of this transaction to the cardholder's account for issuing a bill or statement; for example, this is a “non-posting” advice message.

Type	Noninteractive
Routing	From the Authorization Platform to an IPS.
Response	An Authorization Advice Response/0130—Issuer-generated message is required.

#### **Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)**

The Authorization Advice Response/0130—Issuer-generated message indicates positive receipt of an Authorization Advice/0120—Acquirer-generated message.

Type	Noninteractive
Routing	From the IPS to the APS when responding to the Authorization Advice/0120—Acquirer-generated message.
Response	None

#### **Authorization Advice Response/0130—Issuer-generated (Responding to a System-generated 0120 from SAF)**

The Authorization Advice Response/0130—Issuer-generated message indicates positive receipt of an Authorization Advice/0120—System-generated message from SAF.

Type	Noninteractive
Routing	From an IPS to the Authorization Platform when responding to the Authorization Advice/0120—System-generated message.
Response	None

#### **Authorization Advice Response/0130—System-generated**

The Authorization Advice Response/0130—System-generated message indicates positive receipt of an Authorization Advice/0120 message.

Type	Noninteractive
Routing	From the Authorization Platform to the APS or IPS.
Response	None

## About Authorization Response Acknowledgement Messages

For APS customers, the Authorization Platform provides optional interactive response acknowledgement for Authorization/0100 messages. Acknowledgement messages indicate positive receipt of a response or advice message.

Acquirers are not required to support Authorization Response Acknowledgement/0180 messages, but MasterCard encourages acquirer customers to select this option and to support these messages. Customers may select this option at network configuration time.

The Authorization Response Acknowledgement messages include:

- Authorization Response Acknowledgement/0180
- Authorization Response Negative Acknowledgement/0190

### Authorization Acknowledgement/0180

The Authorization Advice Acknowledgement/0180 message indicates positive acknowledgement that it received a previous Authorization Request Response/0110 message. The Authorization Acknowledgement/0180 message is optional for an APS.

Type	Interactive
Routing	From an APS to the Authorization Platform.
Response	None

### Authorization Negative Acknowledgement/0190

The Authorization Platform sends to an IPS an Authorization Negative Acknowledgement/0190 message only in response to late or invalid Authorization Request Response/0110 messages from an IPS. This informs the IPS that the Authorization Platform has timed-out or rejected the Authorization Request Response/0110 message and initiated Stand-In processing or alternate authorization services on the issuer's behalf. The Authorization Platform also may send the Authorization Negative Acknowledgement/0190 in response to a late or invalid Reversal Request Response/0410 message. In this scenario, the Authorization Negative Acknowledgement/0190 message informs the IPS that the Authorization Platform responded to the acquirer.

Type	Interactive
Routing	From the Authorization Platform to an IPS.
Response	None

## About Issuer File Update Messages

Issuers use Issuer File Update/03xx messages to update individual data files or system parameter tables that the Authorization Platform maintains on their behalf. The Authorization Platform uses these data files to control the operation of standard and optional features that customers may select when they participate in one or more of the MasterCard program and service offerings.

The Issuer File Update messages include:

- Issuer File Update Request/0302
- Issuer File Update Request Response/0312

### **Issuer File Update Request/0302**

The Issuer File Update Request/0302 message requests an Issuer File Update or inquiry action to be initiated on the issuer's behalf.

Type	Interactive
Routing	From an IPS to the Authorization Platform.
Response	An Issuer File Update Request Response/0312 message is required.

### **Issuer File Update Request Response/0312**

The Issuer File Update Request Response/0312 message must be sent in response to a Issuer File Update Request/0302; it indicates the disposition of the Issuer File Update Request/0302 message.

Type	Interactive
Routing	From the Authorization Platform to an IPS.
Response	None

## About Reversal Messages

Reversal Request/0400 messages are generated by an acquirer when the acquirer is unable to deliver an issuer's Authorization Request Response/0110 to a merchant. Merchants also may initiate a Reversal Request/0400 message to cancel the full or partial amount of the original authorization amount.

Reversal/04xx messages include:

- Reversal Request/0400
- Reversal Request Response/0410
- Reversal Advice/0420

- Reversal Advice Response/0430

### **Reversal Request/0400**

The Reversal Request/0400 message reverses fully or partially an earlier authorization request.

Type	Interactive
Routing	From acquirer to the issuer or intermediate network facility.
Response	A Reversal Request Response/0410 message is required.

### **Reversal Request Response/0410**

The Reversal Request Response/0410 message is sent in response to a Reversal Request/0400 message and denotes the disposition of the Reversal Request/0400 message.

Type	Interactive
Routing	From the issuer to the acquirer
Response	None

### **Reversal Advice/0420**

The Reversal Advice/0420 message fully reverses a previous Authorization Request/0100. It advises an issuer of a Reversal Request/0400 responded to by the Authorization Platform.

The Authorization Platform may generate this message on detection of an exception condition while processing a previous Authorization Request Response/0110 message.

The Authorization Platform may generate this message when an issuer is unavailable to respond a Reversal Request/0400 or is delayed in providing a Reversal Request Response/0410 message.

Type	Noninteractive
Routing	From the Authorization Platform to an IPS.
Response	A Reversal Advice Response/0430 message is required.

### **Reversal Advice Response/0430**

The Reversal Advice Response/0430 message must be sent in response to a Reversal Advice/0420 message to acknowledge positive receipt of that message.

## Message Definitions and Flows

### About Message Definitions

---

Type	Noninteractive
Routing	From an IPS to the Authorization Platform.
Response	None

## About Administrative Messages

Administrative messages requests confirmation of data or transmits data in a format other than identified in this International Standard. Member generated advice messages are used to transmit administrative (free format) textual messages between any two parties participating as customers on the Authorization Platform. Authorization Platform generated advice messages return indecipherable messages to a message originator and transmit to an issuer risk scores generated by the RiskFinder scoring system.

Administrative messages include:

- Administrative Request/0600
- Administrative Request Response/0610
- Administrative Advice/0620—System-generated
- Administrative Advice/0620—Member-generated
- Administrative Advice/0630

### Administrative Request/0600

The Administrative Request/0600 message contains customer data in DE 113-119 (Reserved for National Use) and the type of usage in DE 60 (Advice Reason Code). Any eligible Administrative Request/0600 message is routed to the issuer associated to the account range within DE 2 (Primary Account Number [PAN]) and the appropriate response timer is set for the issuer Administrative Request Response/0610 message. The response timer is configured by each DE 60 usage type and initially will be set at a default of 30 seconds for each usage type.

Type	Interactive
Routing	From acquirer to issuer
Response	An Administrative Request Response/0610 message is required.

### Administrative Request Response/0610

The Authorization Platform forwards from the issuer to the acquirer an Administrative Request Response/0610 message that contains the issuer's response data, if the issuer provided a timely response or DE 39 (Response Code), value 91 (Authorization Platform or issuer system inoperative), if an issuer response is not provided within applicable time limits.

---

Type	Interactive
Routing	From issuer to acquirer
Response	none

## Administrative Advice/0620

Administrative Advice/06xx messages are “administrative” messages that two parties participating in a given MasterCard program or service offering may use when using the Authorization Platform.

The Authorization Platform routes messages from an “originator” to a “receiver” and, in general, does not distinguish whether the originator or receiver is an issuer or an acquirer.

The Authorization Platform uses only “noninteractive” Administrative Advice/06xx messages. These messages fall under the general category of “advice” messages, and as such, are subject to the Authorization Platform Guaranteed Advice Delivery procedures that are standard for all advice messages. If the Authorization Platform cannot immediately deliver these messages to their intended destination, the Authorization Platform automatically assumes the responsibility for storing them in the SAF System. When network delivery-point communication has been reestablished and the receiver requests delivery of the advice messages, the Authorization Platform forwards them to the proper destination.

In all cases, DE 60 (Advice Reason Code) within the Administrative Advice/0620 message determines the specific reason for the advice message.

Following are how the Administrative Advice/06xx messages are used:

- Administrative Advice/0620—System Generated messages are used to:
  - Return indecipherable messages to a message originator with an appropriate error condition code, indicating the point at which the Authorization Platform terminated message parsing or message processing. In general, messages returned in Administrative Advice/0620 messages will have improperly coded or garbled Message Type Indicators (MTIs) or improperly coded bit maps.
  - Transmit to an issuer risk scores generated by the RiskFinder scoring system.
- Administrative Advice/0620—Member-generated messages are used to transmit administrative (free format) textual messages between any two parties participating as members on the Authorization Platform.

## Message Definitions and Flows

### About Message Definitions

---

Type	Noninteractive
Routing	Between any two parties participating on the Authorization Platform.
Response	An Administrative Advice Response/0630 message is required.

### Administrative Advice Response/0630

The Administrative Advice Response/0630 message must be sent in response to an Administrative Advice/0620 message to acknowledge positive receipt of that message.

Type	Noninteractive
Routing	From the receiver to the originator of the related Administrative Advice/0620 message.
Response	None

## About Network Management Messages

The Authorization Platform, CPSs, APSS, IPSS, and intermediate network facilities (INFs) use Network Management/08xx messages to coordinate system or network events or tasks. These systems also use these messages to communicate network status conditions.

Network Management/08xx messages include:

- Network Management Request/0800
- Network Management Request Response/0810
- Network Management Advice/0820

Typical uses of Network Management/08xx messages include:

- Sign on to and sign off from the Authorization Platform
- Perform a Network Connection Status to MasterCard
- Perform Host Session Activation or Deactivation
- Perform encryption key management
- Sign on to and sign off from RiskFinder by prefix
- Request RiskFinder SAF message transmission
- Advice of SAF end-of-file/end-of transmission condition for RiskFinder

The Authorization Platform routes Network Management/08xx messages from an “originator” to a “receiver” and, in general, does not distinguish whether the originator or receiver is an issuer or an acquirer.

## **Network Management Request/0800**

The Network Management Request/0800 message controls the MasterCard Worldwide Network by communicating or coordinating system condition or system security. DE 70, a mandatory data element in all Network Management/08xx messages, determines specific Network Management/08xx message functions.

Type	Interactive
Routing	Between the Authorization Platform and any other party (such as CPS, APS, IPS, INF) communicating directly with the Authorization Platform. May be originated by either party.
Response	A Network Management Request Response/0810 message is required.

## **Network Management Request Response/0810**

The Network Management Request Response/0810 message must be sent in response to a Network Management Request/0800 to acknowledge positive receipt of that message.

Type	Interactive
Routing	From “receiver” to “originator” of the related Network Management Request/0800.
Response	None

## **Network Management Advice/0820**

The Network Management Advice/0820 message advises of a previous Network Management Request/0800 message. There is no response to a Network Management Advice/0820 message.

Type	Noninteractive
Routing	From the Authorization Platform to any other party (such as CPS, APS, IPS, INF) communicating directly with the Authorization Platform.
<b>NOTE</b>	
<b>May not be originated by any party other than the Authorization Platform.</b>	
Response	None

## Message Definitions and Flows

### About Message Flows

---

## About Message Flows

Message flows describe the overall standard and exception process of a message type or message pair in various scenarios. Each message flow provides an illustration of the process with the associated stages that describe each part of the process. All Authorization/01xx message flows are illustrated without showing the optional (acquirer-selected) use of the Authorization Acknowledgement/0180 message.

## Authorization Message Routing Timers

Following are the specific Authorization Platform message routing timer values applicable to acquirer-generated 0100, 0120, and 0400 messages. All system-generated Advice/0120, Issuer File Update/03xx, Administrative/06xx, and Network Management/08xx, messages remain unchanged and retain their current timer values.

Product and Transaction Type	Issuer Response Time (in seconds)	Alternate Authorization Service Provider (if applicable)	Acquirer Minimum Wait Time(in seconds)
MasterCard Credit – POS	9 <sup>1</sup>	3	12 <sup>1</sup>
MasterCard – POS PIN for Credit	18	6	24
MasterCard – ATM	12	6	18
Debit MasterCard – POS		Same as MasterCard Credit – POS	
Maestro – All	18	6	24
UK Domestic Maestro	11	6	17
Cirrus – ATM	18	6	24
Private Label – POS	12	6	18
AMEX – POS	12	6	18
Visa – POS	12	6	18

- 
1. For transactions acquired in the countries of Brazil, Canada, the United Kingdom, and the United States, MasterCard has reduced the timers by 2 additional seconds. In these countries, the maximum time MasterCard will wait before invoking alternate authorization provider processing is reduced to 7 seconds and the minimum time that an acquirer must wait is reduced to 10 seconds.

MasterCard reserves the right to adjust local market timer values based on specific market conditions and as additional exception countries are added, they will be announced in the Global Operations Bulletins.

## Authorization Request/0100 and Authorization Request Response/0110

This message flow describes the standard authorization transaction process.



1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Authorization Request/0100 message to the issuer.
3. The issuer<sup>2</sup> generates an appropriate Authorization Request Response/0110 message and sends it to the Authorization Platform.
4. The Authorization Platform forwards the Authorization Request Response/0110 message to the acquirer.

---

2. The “issuer” in the illustration may in fact be a MasterCard IPS used for Dual Message System processing. Optional issuer processing services are available to MasterCard customers in support of various programs and services; for example, the Authorization Platform may provide IPS services for customers that elect to use this service.

## **Authorization Request/0100—Communication Failure at Acquirer**

This message flow describes exception processing when communication fails between the APS and the Authorization Platform (resubmit processing is not supported).



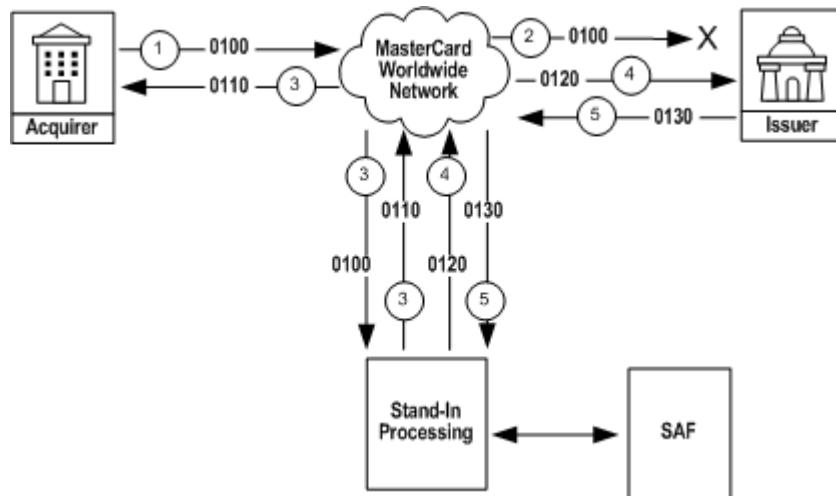
1. The acquirer initiates an Authorization Request/0100 message, but it cannot be delivered to the Authorization Platform because of system failure.
2. The acquirer completes the transaction at the point of interaction. In most cases, the APS simply denies the transaction. However, the APS may elect to approve the transaction for completion for various reasons.

Depending on the type of systems failure and the operating procedures or regulations governing the program or service involved, the acquirer, the merchant, or both may be required to assume full or partial liability for the transaction if it is completed without appropriate issuer authorization.

If the acquirer elects to authorize the transaction at the point of interaction, the acquirer may be required to accept financial liability for the transaction. The acquirer may notify the issuer of the authorization it approved on the issuer's behalf by sending an Authorization Advice/0120 message.

## Authorization Request/0100—Communication Failure at Issuer

This message flow describes exception processing when communication fails between the IPS and the Authorization Platform during an Authorization Request/0100 message.



1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization platform.
2. The Authorization platform attempts to forward the Authorization Request/0100 message to the issuer but is unable to complete the message transmission because of a communication link failure or IPS failure. As a result, the Authorization platform immediately sends the Authorization Request/0100 message to Stand-In processing for alternate processing functions.
3. After the Authorization platform sends the Authorization Request/0100 message, if the issuer permits Stand-In processing to authorize transactions, Stand-In processing generates an appropriate Authorization Request Response/0110 message on the issuer's behalf and forwards it to the acquirer. Stand-In processing also generates an Authorization Advice/0120 message and forwards it to the Authorization platform store-and-forward (SAF) process for later transmission to the issuer.

### NOTE

**Stand-In processing generates and forwards Authorization Advice/0120 messages for “approved,” “declined,” and “capture card” Authorization Request/0100 messages.**

4. When communication re-establishes with the IPS, the Stand-In System SAF process forwards the Authorization Advice/0120 message to the issuer. This action allows the issuer to update its cardholder “open-to-buy” and “velocity” data files in a timely manner.
5. The issuer, upon receiving and securing the Authorization Advice/0120 message, returns an Authorization Advice Response/0130 message to the

## **Message Definitions and Flows**

### **About Message Flows**

---

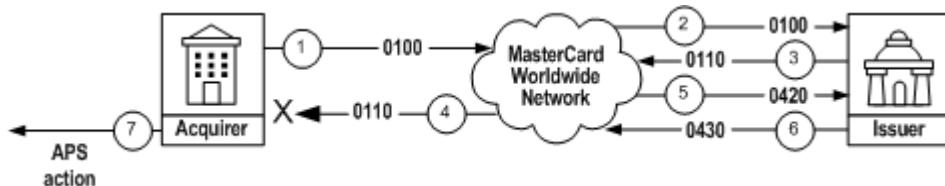
Authorization Platform to indicate positive receipt of the Authorization Advice/0120 message.

#### **NOTE**

**Each time the SAF process receives an Authorization Advice/0130 message, it sends the next Authorization Advice/0120 message. This process repeats until there are no more Authorization Advice/0120 messages. If the Authorization Platform does not receive an Authorization Advice Response/0130 message, it assumes the issuer did not receive the previous Authorization Advice/0120 message, ceases the SAF session, and places an unqueued Authorization Advice/0120 message into the queue for delivery.**

## Authorization Request Response/0110—Communication Failure at Acquirer

This message flow describes exception processing when communication fails between the Authorization Platform and the APS during an Authorization Request Response/0110 message.



1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Authorization Request/0100 message to the issuer.
3. The issuer generates an appropriate Authorization Request Response/0110 message and sends it to the Authorization Platform.
4. The Authorization Platform attempts to forward the Authorization Request Response/0110 message to the acquirer but cannot successfully complete the transmission because of communications link failure or APS failure.
5. The Authorization Platform has determined that the issuer's Authorization Request Response/0110 message is "undeliverable," so the Authorization Platform immediately generates a Reversal Advice/0420 message<sup>3</sup> back to the issuer if the Authorization Request Response/0110 message indicates an approval.

The purpose of this advice is to let the issuer know that its Authorization Request Response/0110 message was undelivered and that the issuer should "reverse" or otherwise adjust its cardholder authorization files as necessary to reflect that the transaction could not be completed.

6. The issuer responds back to the Authorization Platform with a Reversal Advice Response/0430 message to acknowledge positive receipt of the Reversal Advice/0420 message.
7. Meanwhile, if the APS is still operating, it detects a time-out condition on the Authorization Request Response/0110 message that it is expecting from the Authorization Platform. When the time-out occurs, the APS must make a decision whether to authorize the transaction at the point of interaction. If the APS denies the transaction, the message flow terminates at this point.

3. Does not apply in the case of a MasterCard Hosted Mobile Phone Top-up request. If the issuer approves the MasterCard Hosted Mobile Phone Top-up transaction, the Authorization Platform will complete the MasterCard Hosted Mobile Phone Top-up request. The acquirer should provide the cardholder with notification at the ATM that the top-up request will be complete within 15 minutes.

## **Message Definitions and Flows**

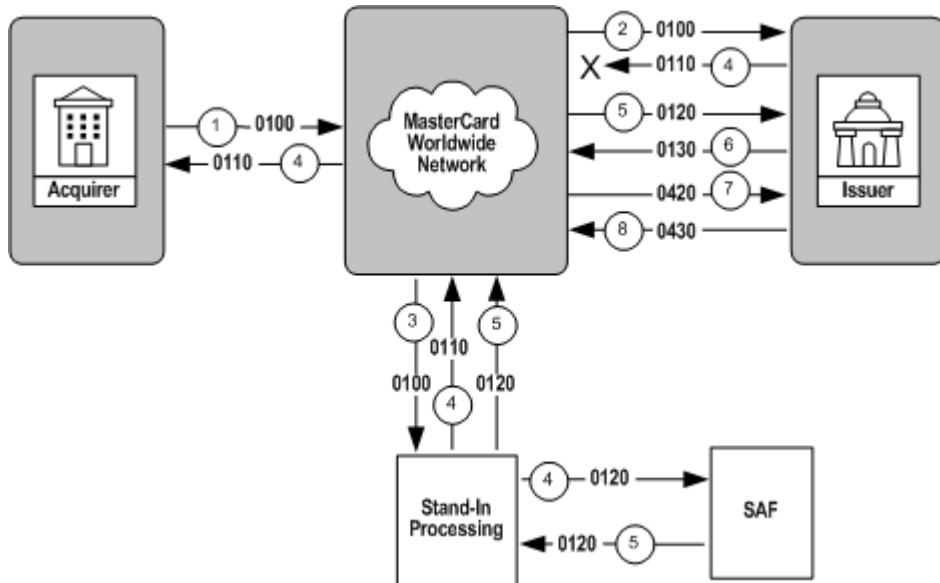
### **About Message Flows**

---

If the acquirer elects to authorize the transaction at the point of interaction, the acquirer may be required to accept financial liability for the transaction. The acquirer may notify the issuer of the authorization it approved on the issuer's behalf by sending an Authorization Advice/0120 message.

## Authorization Request Response/0110—Communication Failure at Issuer

This message flow describes exception processing when communication fails between the Authorization Platform and the IPS during an Authorization Request Response/0110 message.



1. The acquirer initiates an Authorization Request/0100 message.
2. The Authorization Platform forwards the Authorization Request/0100 message to the issuer.
3. The IPS cannot return the appropriate Authorization Request Response/0110 message because of a communications failure between the IPS and the Authorization Platform. The IPS **must** assume that the Authorization Platform or the acquirer will take appropriate action at this point and should reverse any effect to its cardholder or velocity files that may have taken place during the authorization process.

If Stand-In processing or an alternate authorization process subsequently approves the transaction, the issuer can receive a later notification by a SAF Authorization Advice/0120 message.

The Authorization Platform detects a time-out condition from the issuer on the Authorization Request Response/0110 message. If the issuer permits Stand-In processing, the Authorization Platform sends an Authorization Request/0100 message to Stand-In processing.

4. Stand-In processing generates an appropriate Authorization Request Response/0110 message on the issuer's behalf and forwards it to the acquirer. It also generates an Authorization Advice/0120 message and forwards it to the Authorization Platform SAF process for later transmission to the issuer.

## Message Definitions and Flows

### About Message Flows

---

#### NOTE

**Stand-In processing generates and forwards Authorization Advice/0120 messages for both “approved” and “declined” Authorization Request/0100 messages.**

5. When communication re-establishes with the IPS, the Stand-In System SAF process forwards the Authorization Advice/0120 message to the issuer. This action allows the issuer to update its cardholder “open-to-buy” and “velocity” data files in a timely manner.
6. The issuer, on receiving and securing the Authorization Advice/0120 message, returns an Authorization Advice Response/0130 message to the Authorization Platform to indicate positive receipt of the Authorization Advice/0120 message.

#### NOTE

**Each time the SAF process receives an Authorization Advice Response/0130 message, it sends the next Authorization Advice/0120 message. This process repeats until there are no more Authorization Advice/0120 messages.  
If the Authorization Platform does not receive an Authorization Advice Response/0130 message, it assumes the issuer did not receive the previous Authorization Advice/0120 message and ceases the SAF session.**

7. The Authorization Platform sends a Reversal Advice/0420 message containing the following values to the issuer because no issuer response is received:
  - DE 39 = 82 (Time-out at issuer)
  - DE 60, subfield 1 = 402 (Banknet advice: IPS time-out error)
8. When the issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message.

## **Authorization Request Response/0110—Stand-In System Allowed**

Following are the Authorization Request Response/0110 exception condition message flows that illustrate when Stand-In System processing is allowed on the transaction:

- Authorization Request Response/0110—Not Received within Time Limits
- Authorization Request Response/0110—Received within the Time Limit but after Stand-In System Response
- Authorization Request Response/0110—Received within Time Limit and before Stand-In System Response

### **NOTE**

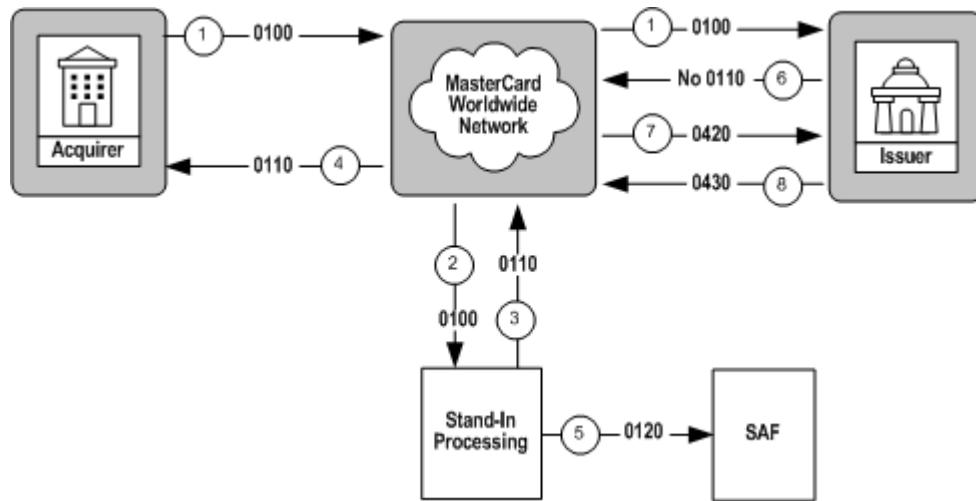
[\*\*Authorization Message Routing Timers\*\*](#) provides details regarding specific time limits.

## Message Definitions and Flows

### About Message Flows

#### Authorization Request Response/0110—Not Received within the Time Limit

This message flow describes exception processing when no issuer Authorization Request Response/0110 message is received within the defined time limits after receipt of the Authorization Request/0100 message for transactions that are allowed to be processed by the Stand-In System.

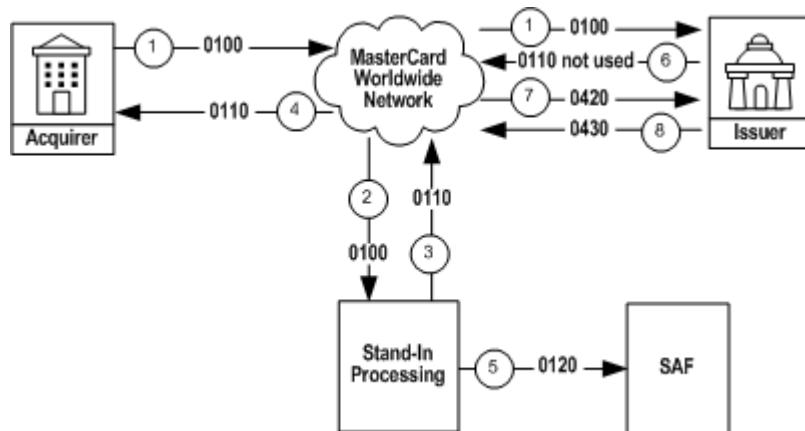


1. The acquirer sends the Authorization Request/0100 message to the Authorization Platform, and the Authorization Platform forwards the Authorization Request/0100 message to the issuer.
2. If the Authorization Platform does not receive the Authorization Request Response/0110 message from the issuer within the time limit, the Authorization Platform sends the Authorization Request/0100 message to the Stand-In System.
3. The Stand-In System forwards the Authorization Request Response/0110 message to the Authorization Platform.
4. The Authorization Request Response/0110 message received from the Stand-In System is forwarded by the Authorization Platform to the acquirer.
5. The Stand-In System creates an Authorization Advice/0120 message and stores it in a SAF queue for guaranteed delivery to the issuer.
6. The Authorization Platform does not receive the Authorization Request Response/0110 message from the issuer within the time limit.
7. The Authorization Platform sends a Reversal Advice/0420 message containing the following values to the issuer because no issuer response is received:
  - DE 39 = 82 (Time-out at issuer)
  - DE 60, subfield 1 = 402 (Banknet advice: IPS time-out error)

8. When the issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.

## Authorization Request Response/0110—Received within the Time Limit but after Stand-In System Response

This message flow describes exception processing when the issuer's Authorization Request Response/0110 message is received within the time limit but after the Stand-In System response. Issuers can retrieve SAF messages upon request.

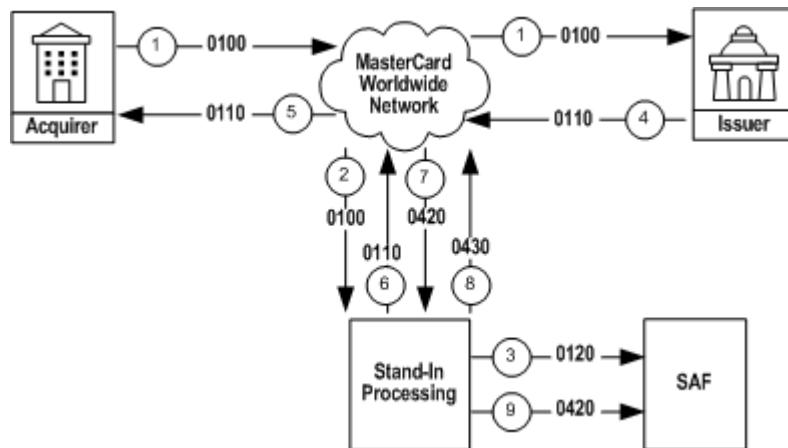


1. The acquirer sends the Authorization Request/0100 message to the Authorization Platform, and the Authorization Platform forwards the Authorization Request/0100 message to the issuer.
2. If the Authorization Platform does not receive the Authorization Request Response/0110 message within the time limit from the issuer, the Authorization Platform sends the Authorization Request/0100 message to the Stand-In System.
3. The Stand-In System forwards the Authorization Request Response/0110 message to the Authorization Platform.
4. The Authorization Platform sends the Authorization Request Response/0110 message to the acquirer.
5. The Stand-In System creates an Authorization Advice/0120 message and stores it in a SAF queue for guaranteed delivery to the issuer.
6. The issuer's Authorization Request Response/0110 message is received within the time limit but the issuer's response is not used because the issuer's response was received after the Authorization Request Response/0110 message from the Stand-In System.
7. The Authorization Platform sends a Reversal Advice/0420 message containing the following values to the issuer to reverse the issuer's response that was not used:
  - DE 39 = the value from the issuer's Authorization Request Response/0110
  - DE 60, subfield 1 = 400 (Banknet advice: APS error; unable to deliver response)

8. When the issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.

## **Authorization Request Response/0110—Received within the Time Limit and before Stand-In System Response**

This message flow describes exception processing when the issuer's Authorization Request Response/0110 message is received within the time limit but before the Stand-In System response.



1. The acquirer sends the Authorization Request/0100 message to the Authorization Platform, and the Authorization Platform forwards the Authorization Request/0100 message to the issuer.
2. If the Authorization Platform does not receive the Authorization Request Response/0110 message within the time limit from the issuer, the Authorization Platform sends the Authorization Request/0100 message to the Stand-In System.
3. The Stand-In System creates an Authorization Advice/0120 message and stores it in SAF for guaranteed delivery to the issuer.
4. The issuer sends the Authorization Request Response/0110 message to the Authorization Platform.
5. The Authorization Platform receives the issuer's Authorization Request Response/0110 message within the time limit and before the Stand-In System response, and sends the issuer's Authorization Request Response/0110 message to the acquirer.
6. The Stand-In System forwards the Authorization Request Response/0110 message to the Authorization Platform.
7. The Authorization Platform sends the Reversal Advice/0420 message to the Stand-In System to reverse the Stand-In System's response that was not used.
8. The Stand-In System generates a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.
9. The Stand-In System stores the Reversal Advice/0420 in SAF for guaranteed delivery to the issuer.

## Authorization Request Response/0110—Not Eligible for Alternate Processing

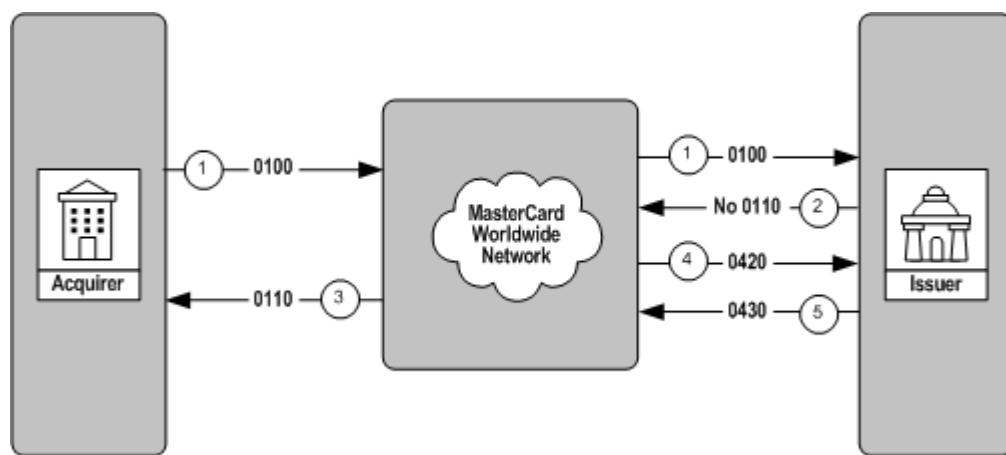
These message flows describe authorization message processing when the transaction is not eligible for alternate processing.

These message flows describe exception processing when:

- Authorization Request Response/0110—No Issuer Response
- Authorization Request Response/0110—Late Issuer Response
- Authorization Request Response/0110—Issuer Edit Error

### Authorization Request Response/0110—No Issuer Response within Issuer Response Time Limit

This message flow describes exception processing when the issuer's Authorization Request Response/0110 message is not received within the allowed issuer response time limit after receipt of the Authorization Request/0100 message.



1. The acquirer sends the Authorization Request/0100 message to the Authorization Platform, and the Authorization Platform forwards the Authorization Request/0100 message to the issuer.
2. The Authorization Platform does not receive the issuer's Authorization Request Response/0110 within the response time allowed for the issuer.
3. The Authorization Platform sends the Authorization Request Response/0110 to the acquirer where DE 39 (Response Code) = 91 (Issuer Authorization Platform or Issuer Inoperative).
4. The Authorization Platform sends the Reversal Advice/0420 message to the issuer containing the following values:
  - DE 39 = 82 (Time-out at issuer)
  - DE 60, subfield 1 = 402 (Banknet advice: IPS time-out error)

## **Message Definitions and Flows**

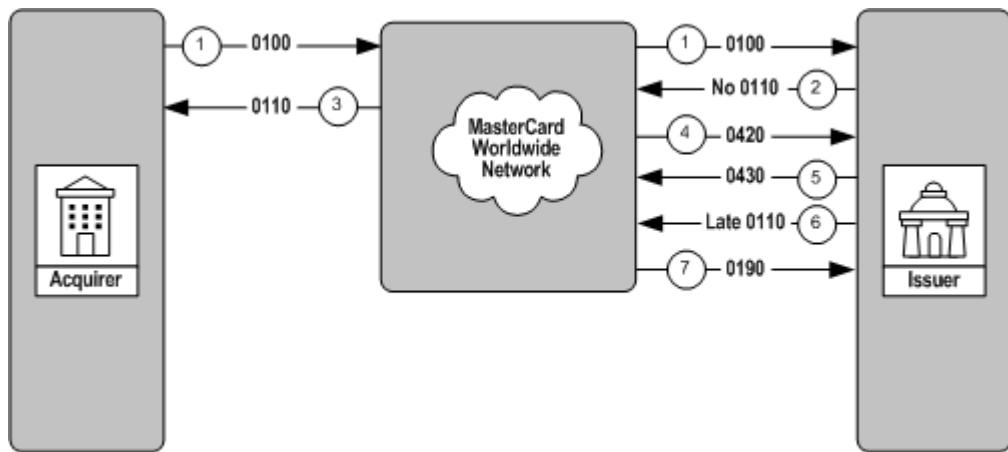
### **About Message Flows**

---

5. When the issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.

## Authorization Request Response/0110—Late Issuer Response

This message flow describes exception processing when the Authorization Platform detects a time-out condition on an expected Authorization Request Response/0110 message from an issuer, and then receives a “late” Authorization Request Response/0110 message.



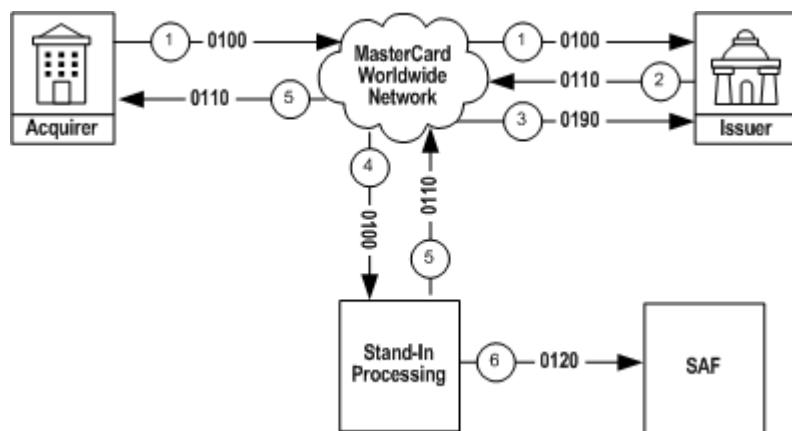
1. The acquirer sends the Authorization Request/0100 message to the Authorization Platform, and the Authorization Platform forwards the Authorization Request/0100 message to the issuer.
2. The Authorization Platform does not receive the Authorization Request Response/0110 message within the time limits from the issuer.
3. The Authorization Platform generates an Authorization Request Response/0110 message where DE 39 (Response Code) = 91 (Issuer Authorization Platform or Issuer Inoperative) and forwards it to the acquirer.
4. The Authorization Platform sends a Reversal Advice/0420 message containing the following values to the issuer because no issuer response is received:
  - DE 39 = 82 (Time-out at issuer)
  - DE 60, subfield 1 = 402 (Banknet advice: IPS time-out error)
5. When the issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.
6. The Authorization Platform receives a “late” Authorization Request Response/0110 message from the issuer.
7. The Authorization Platform sends an Authorization Response Negative Acknowledgement/0190 message to the issuer, indicating it has no record of a corresponding Authorization Request/0100 message.

**NOTE**

**There is no response necessary from the issuer after the Authorization Platform sends an Authorization Response Negative Acknowledgement/0190 message.**

**Authorization Request Response/0110—Issuer Edit Error**

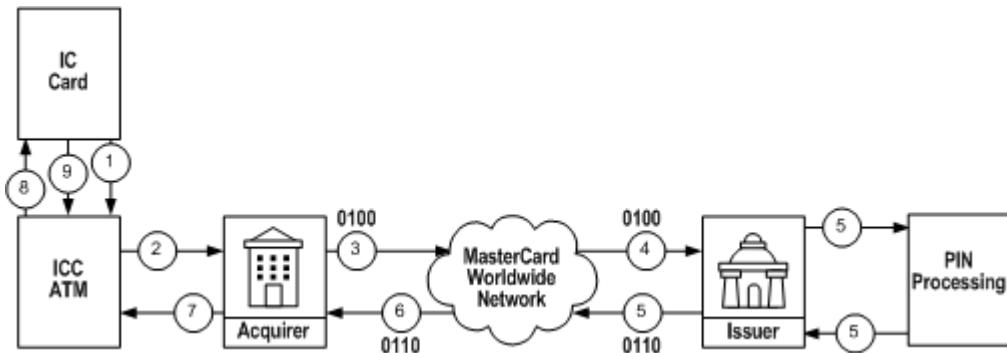
This message flow describes exception processing when an invalid issuer Authorization Request Response/0110 message is received after receipt of the Authorization Request/0100 message for transactions that are allowed to be processed by the Stand-In System.



1. The acquirer sends the Authorization Request/0100 message.
2. The issuer generates an invalid or late Authorization Request Response/0110 message.
3. The Authorization Platform sends an Authorization Response Negative Acknowledgement/0190 message to the issuer.
4. The Authorization Platform sends the Authorization Request/0100 message to Stand-In processing.
5. Stand-In processing generates an appropriate Authorization Request Response/0110 message on the issuer's behalf and forwards it to the acquirer.
6. The Stand-In System also generates an Authorization Advice/0120 message and forwards it to the Authorization Platform SAF process for later transmission to the issuer.

## Authorization Request/0100—Chip PIN Management

This message flow describes standard transaction processing when changing or unblocking a PIN on a chip card.



1. The cardholder initiates a PIN change or PIN unblock transaction at the ATM.
2. The ATM requests an Authorization Request Cryptogram (ARQC) from the chip card.
  - For a **PIN change** transaction, if the card does not provide the ARQC and declines the request with an Application Authentication Cryptogram (AAC), processing stops.
  - For a **PIN unblock** transaction, if the card does not provide the ARQC and declines the request with an AAC, processing will continue (because the PIN is blocked, it may be unable to generate an AC). The acquirer inserts the AAC in DE 55 (Integrated Circuit Card [ICC] System-related Data) of the Authorization Request/0100 message.
3. The acquirer sends an Authorization Request/0100—Chip PIN Management Request message to the Authorization Platform.
4. The Authorization Platform forwards the Authorization Request/0100 message to the issuer.
5. The issuer sends an Authorization Request Response/0110 message to the Authorization Platform approving or declining the request.
  - If approved, the issuer must insert the PIN change or PIN unblock script in DE 55. If the transaction is a PIN change, the issuer also stores the old online PIN and updates its system with the new online PIN.
  - If declined, the issuer may insert the PIN change or PIN unblock script in DE 55 and block the card, if stolen.
6. The Authorization Platform forwards the Authorization Request Response/0110 message to the acquirer.
7. The acquirer host sends the response to the ATM.
8. The ATM transmits the script to the card.

## **Message Definitions and Flows**

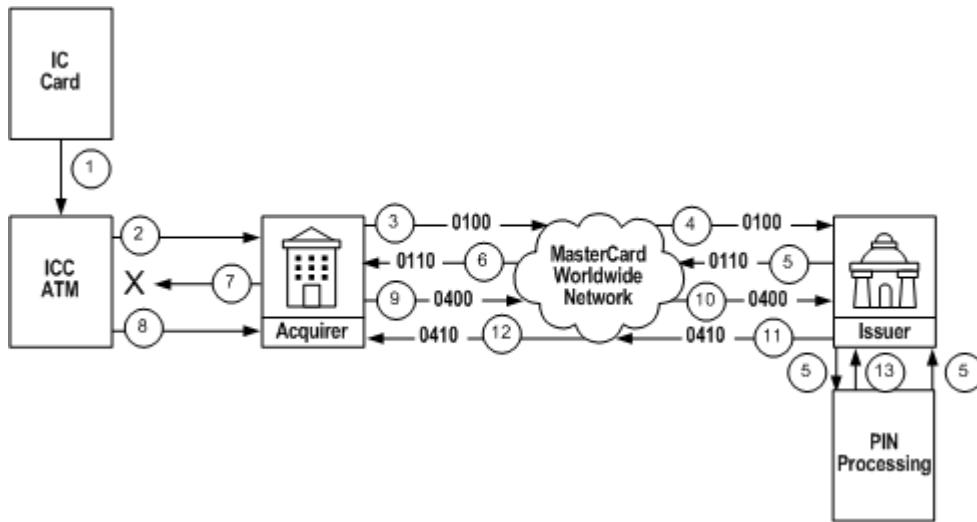
### **About Message Flows**

---

9. The chip card applies the script and provides the script processing result to the ATM.

## Authorization Request/0100—Chip PIN Management (Failure to Transmit/Apply Script to Chip Card)

This message flow describes the transaction process when there is a failure in transmitting the script to the chip card, or a failure in applying the script to the chip card.



1. The cardholder initiates a PIN change or PIN unblock transaction at the ATM.
2. The ATM requests an Authorization Request Cryptogram (ARQC) from the chip card.
  - For a **PIN change** transaction, if the card does not provide the ARQC and declines the request with an Application Authentication Cryptogram (AAC), processing stops.
  - For a **PIN unblock** transaction, if the card does not provide the ARQC and declines the request with an AAC, processing will continue (because the PIN is blocked, it may be unable to generate an ARQC). The acquirer inserts the AAC in DE 55 (Integrated Circuit Card [ICC] System-related Data) of the Authorization Request/0100 message.
3. The acquirer sends an Authorization Request/0100—Chip PIN Management Request message to the Authorization Platform.
4. The Authorization Platform forwards the Authorization Request/0100 to the issuer.
5. The issuer sends an Authorization Request Response/0110 message to the Authorization Platform approving or declining the request.
  - If approved, the issuer must insert the PIN change or PIN unblock script in DE 55. If the transaction is a PIN change, the issuer also stores the old online PIN and updates its system with the new online PIN.
  - If declined, the issuer may insert the PIN change or PIN unblock script in DE 55 and block the card, if stolen.

## **Message Definitions and Flows**

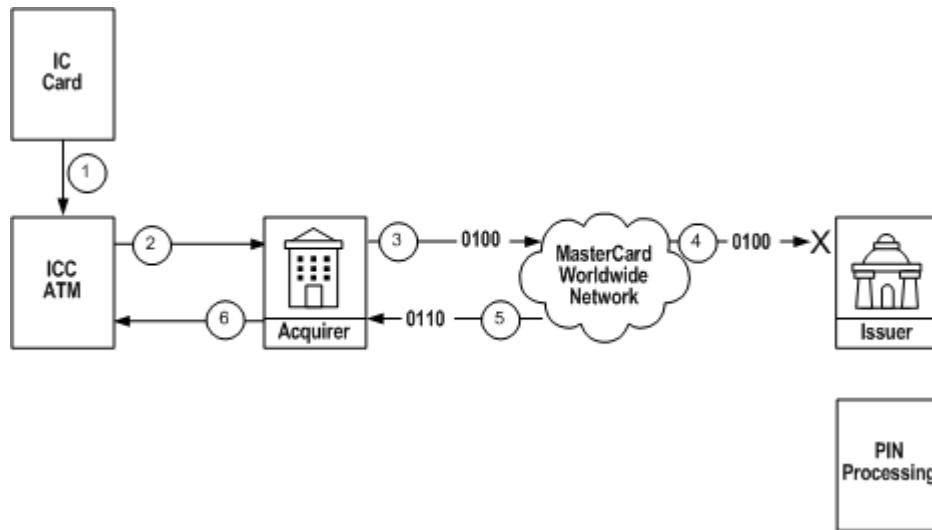
### **About Message Flows**

---

6. The Authorization Platform forwards the Authorization Request Response/0110 message to the acquirer.
7. One of the following scenarios may occur:
  - The acquirer cannot send the script in DE 55 to the ATM (as illustrated), or
  - The ATM cannot transmit the script to the chip card, or
  - The chip card cannot process the script
8. The ATM sends the processing result to the acquirer.
9. The acquirer sends a Reversal Request/0400 message to the Authorization Platform.
10. The Authorization Platform forwards the Reversal Request/0400 message to the issuer.
11. The issuer sends a Reversal Request Response/0410 message to the Authorization Platform.
12. The Authorization Platform forwards the Reversal Request Response/0410 message to the acquirer.
13. If the issuer originally approved a PIN change, the issuer reactivates the old online PIN.

## Authorization Request/0100—Chip PIN Management (Issuer Network Failure-Unable to Connect)

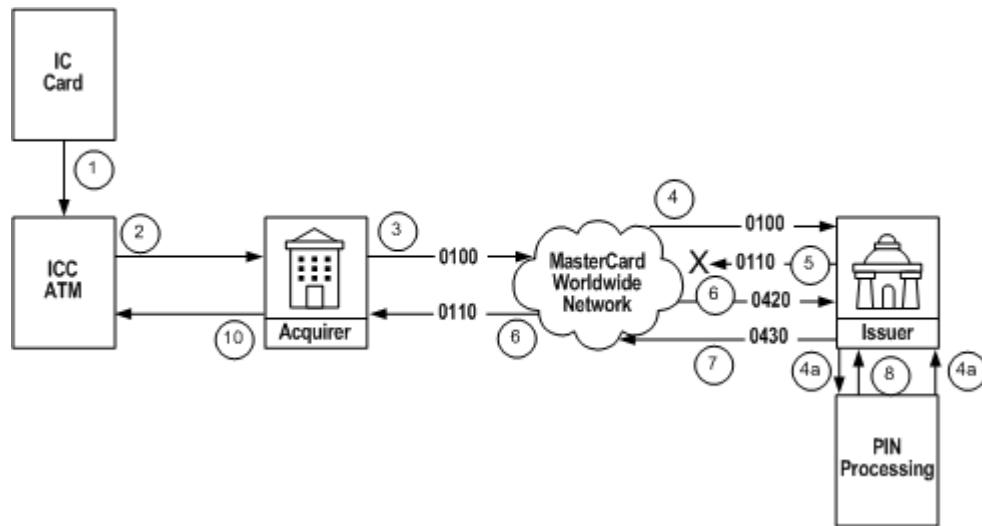
This message flow describes the transaction process when there is a network failure at the issuer.



1. The cardholder initiates a PIN change or PIN unblock transaction at the ATM.
2. The ATM requests an Authorization Request Cryptogram (ARQC) with a zero amount from the chip card.
  - For a **PIN change** transaction, if the card does not provide the ARQC and declines the request with an Application Authentication Cryptogram (AAC), processing stops.
  - For a **PIN unblock** transaction, if the card does not provide the ARQC and declines the request with an AAC, processing will continue (because the PIN is blocked, it may be unable to generate an ARQC). The acquirer inserts the AAC in DE 55 (Integrated Circuit Card [ICC] System-related Data) of the Authorization Request/0100 message.
3. The acquirer sends an Authorization Request/0100—Chip PIN Management Request message to the Authorization Platform.
4. The Authorization Platform forwards the Authorization Request/0100 to the issuer; however, the 0100 message does not reach the issuer and results in a timeout at the issuer MIP.
5. The Authorization Platform sends an Authorization Request Response/0110 to the acquirer with DE 39 = 91 (Authorization Platform or issuer system inoperative).
6. The acquirer sends a message to the ATM indicating that the service is unavailable.

## **Authorization Request/0100—Chip PIN Management (Issuer Network Failure, No Response from Issuer)**

This message flow describes the transaction process when the issuer response is unsuccessfully delivered to the Authorization Platform or is delivered too late.



1. The cardholder initiates a PIN change or PIN unblock transaction at the ATM.
2. The ATM requests an Authorization Request Cryptogram (ARQC) with a zero amount from the chip card.
  - For a **PIN change** transaction, if the card does not provide the ARQC and declines the request with an Application Authentication Cryptogram (AAC), processing stops.
  - For a **PIN unblock** transaction, if the card does not provide the ARQC and declines the request with an AAC, processing will continue (because the PIN is blocked, it may be unable to generate an ARQC). The acquirer inserts the AAC in DE 55 (Integrated Circuit Card [ICC] System-related Data) of the Authorization Request/0100 message.
3. The acquirer sends an Authorization Request/0100 message to the Authorization Platform.
4. The Authorization Platform forwards the Authorization Request/0100 to the issuer.
5. The issuer fails to send the Authorization Request Response/0110 message to the Authorization Platform in time.
6. The Authorization Platform sends a Reversal Advice/0420 message to the issuer with DE 39 (Response Code) = 82 (Timeout at issuer).

---

If a response is received from the issuer after the allowed response time limit for ATM transactions<sup>4</sup>, the Authorization Platform will send the issuer an Authorization Response Negative Acknowledgement/0190 message with DE 39 = 68 (Response received too late) (not illustrated).

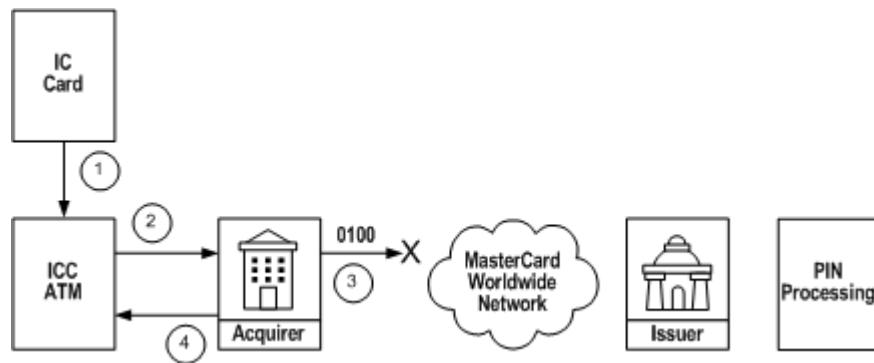
7. The issuer sends a Reversal Advice Response/0430 message to the Authorization Platform acknowledging receipt of the Reversal Advice/0420 message.
8. If the original transaction was a PIN change, the issuer restores the old online PIN.
9. The Authorization Platform sends the acquirer an Authorization Request Response/0110 message with DE 39 = 91 (Authorization Platform or issuer system inoperative).
10. The acquirer sends a message to the ATM, indicating that the service is unavailable.

---

4. For MasterCard and Debit MasterCard only.

## **Authorization Request/0100—Chip PIN Management (Acquirer Network Failure-Unable to Connect)**

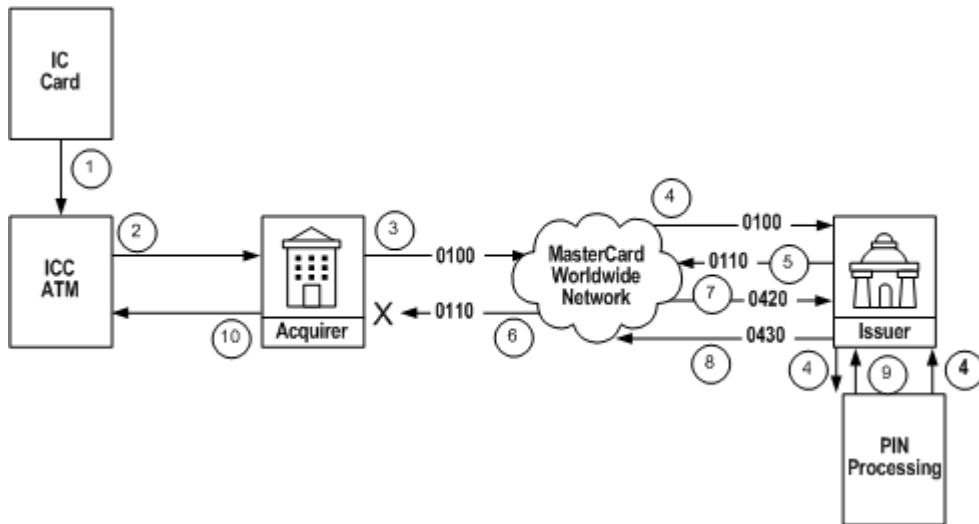
This message flow describes the transaction process when there is a network failure at the acquirer.



1. The cardholder initiates a PIN change or PIN unblock transaction at the ATM.
2. The ATM requests an Authorization Request Cryptogram (ARQC) with a zero amount from the chip card.
  - For a **PIN change** transaction, if the card does not provide the ARQC and declines the request with an Application Authentication Cryptogram (AAC), processing stops.
  - For a **PIN unblock** transaction, if the card does not provide the ARQC and declines the request with an AAC, processing will continue (because the PIN is blocked, it may be unable to generate an ARQC). The acquirer inserts the AAC in DE 55 (Integrated Circuit Card [ICC] System-related Data) of the Authorization Request/0100 message.
3. The acquirer sends an Authorization Request/0100—Chip PIN Management Request message to the Authorization Platform; however, the message does not reach the Authorization Platform.
4. The acquirer times out and sends a message to the ATM indicating that the service is unavailable.

## Authorization Request/0100—Chip PIN Management (Acquirer Network Failure-Unable to Connect with Acquirer)

This message flow describes the transaction process when the Authorization Platform is unable to successfully deliver the issuer's response message to the acquirer.



1. The cardholder initiates a PIN change or PIN unblock transaction at the ATM.
  2. The ATM requests an Authorization Request Cryptogram (ARQC) with a zero amount from the chip card.
    - For a **PIN change** transaction, if the card does not provide the ARQC and declines the request with an Application Authentication Cryptogram (AAC), processing stops.
    - For a **PIN unblock** transaction, if the card does not provide the ARQC and declines the request with an AAC, processing will continue (because the PIN is blocked, it may be unable to generate an ARQC). The acquirer inserts the AAC in DE 55 (Integrated Circuit Card [ICC] System-related Data) of the Authorization Request/0100 message.
  3. The acquirer sends an Authorization Request/0100—Chip PIN Management Request message to the Authorization Platform.
  4. The Authorization Platform forwards the Authorization Request/0100 to the issuer.
- If the transaction is a PIN change, the issuer stores the old online PIN and updates its system with the new online PIN.
5. The issuer sends the Authorization Request Response/0110 message to the Authorization Platform.
  6. The Authorization Platform fails to deliver the Authorization Request Response/0110 message to the acquirer.

## **Message Definitions and Flows**

### **About Message Flows**

---

7. The Authorization Platform sends the issuer a Reversal Advice/0420 message.
8. The issuer sends a Reversal Advice Response/0430 message to the Authorization Platform acknowledging receipt of the Reversal Advice/0420 message.
9. If the original transaction is a PIN change, the issuer restores the old online PIN.
10. The acquirer's system times out and sends a message to the ATM indicating that the service is unavailable.

#### **NOTE**

**The issuer may receive two reversals—one from the Authorization Platform to identify the undelivered response and a second from the acquirer as a result of a system timeout.**

## **Guaranteed Advice Message Delivery**

The guaranteed advice message delivery process provides a message routing facility. The Authorization Platform uses guaranteed advice message delivery for **all** advice messages transmitted using the Authorization Platform.

### **The Guaranteed Message Delivery Process**

When an advice message is forwarded to the Authorization Platform, the Authorization Platform:

1. Immediately secures the transaction for future delivery
2. Responds to the advice message initiator with an advice response message, indicating that it received and secured the message
3. Forwards the advice message to the appropriate receiving entity

The Authorization Platform guarantees the delivery of all advice messages routed through the MasterCard Worldwide Network. Occasionally, the Authorization Platform cannot immediately deliver an advice message (for example, because of a system or communication failure at the destination). In this case, the Authorization Platform stores the message on its store-and-forward (SAF) processing facilities and automatically delivers the message when communication is restored.

The receiver of an advice message must acknowledge receipt with an appropriate advice response message. When the Authorization Platform receives the advice response message, MasterCard considers advice delivery complete and removes the message from SAF processing queues.

Authorization Advice/0120—Acquirer-generated messages are immediately sent to the issuer. The issuer responds with an Authorization Advice/0130—Issuer-generated message that the Authorization Platform forwards to the acquirer.

The Authorization Platform Guaranteed Advice Message Delivery process processes all MasterCard advice messages including the following:

- Authorization Advice/0120—Acquirer-generated
- Authorization Advice/0120—Issuer-generated (to RiskFinder)
- Authorization Advice/0120—System-generated
- Reversal Advice/0420
- Administrative Advice/0620

## **Standard Advice Delivery—All Advice Message Types**

This message flow describes the standard transaction processing of all advice messages originating from customer processing systems(CPS) connected to the Authorization Platform. The only exception is the Network Management Advice/0820 message, which has no response message.



1. The CPS forwards the advice message to the Authorization Platform.
2. The Authorization Platform returns an appropriate advice response message when it secures the advice message.
3. The Authorization Platform forwards the advice message to the receiving entity.
4. The receiving entity returns an appropriate advice response message as positive acknowledgement of receipt when it secures the advice message.

**NOTE**

**Only the Authorization Platform generates Network Management Advice/0820 messages. Network Management Advice/0820 messages do not require any type of response message.**

## Authorization Advice/0120—Acquirer-generated, Issuer Available

This message flow describes the transaction process of the Authorization Advice/0120—Acquirer-generated and Authorization Advice Response/0130—Issuer-generated message when the issuer is available.



1. The acquirer initiates an Authorization Advice/0120—Acquirer-generated message containing DE 60, subfield 1, value 190 or 191, and then passes the 0120 message to the Authorization Platform.  
The Authorization Platform inserts DE 48, subelement 15 (Authorization Platform Advice Date and Time) into the message and forwards the Authorization Advice/0120—Acquirer-generated message to the issuer.
2. The issuer returns an Authorization Advice Response/0130—Issuer-generated message to the acquirer to indicate positive receipt of the Authorization Advice/0120—Acquirer-generated message. The issuer's advice response message will contain DE 48, subelement 15 (Authorization Platform Advice Date and Time).

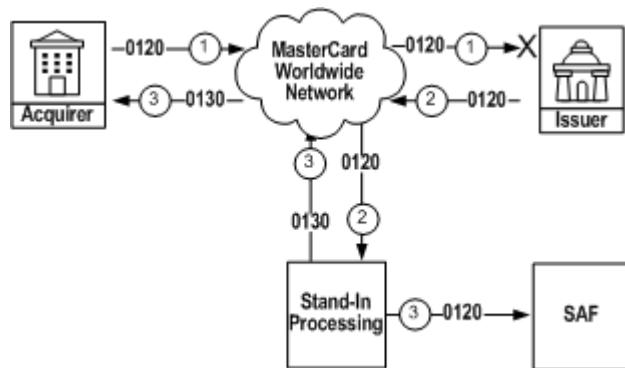
## Message Definitions and Flows

### About Message Flows

---

#### Authorization Advice/0120—Acquirer-generated, Issuer Unavailable

This message flow describes the transaction process of the Authorization Advice/0120—Acquirer-generated and Authorization Advice Response/0130—System-generated message when the issuer is unavailable or there is no issuer response.



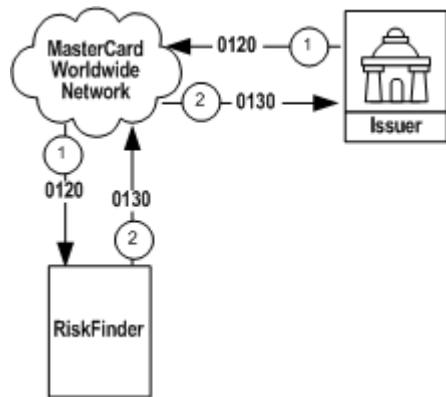
1. The acquirer initiates an Authorization Advice/0120—Acquirer-generated message containing DE 60, subfield 1, value 190 or 191, and then forwards the 0120 message to the Authorization Platform.
2. The Authorization Platform determines that the Authorization Advice/0120—Acquirer-generated message cannot be delivered to the issuer host. The Authorization Platform routes the Authorization Advice/0120—Acquirer-generated message to the Stand-In System to add to the issuer SAF queue.
3. The Stand-In System places the Authorization Advice/0120—Acquirer-generated message into the store-and-forward (SAF) queue for guaranteed delivery to the issuer. The Stand-In System responds to the acquirer with an Authorization Advice Response/0130—System-generated message containing DE 48, subelement 15 (Authorization Platform Advice Date and Time).

#### NOTE

**Members in the Europe region that route to an alternate issuer host for alternate processing instead of the Stand-In System will still receive an Authorization Advice/0120—Acquirer-generated as described here. Alternate issuer host processing does not send Reversal Request/0400 or Authorization Advice/0120 messages to the alternate host.**

## Authorization Advice/0120—Issuer-generated

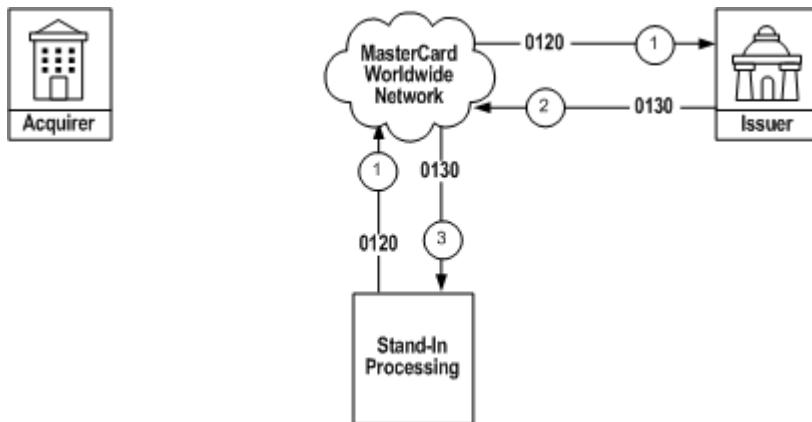
Authorization Request/0100 messages may contain BINs that customers have selected for scoring. For these transactions, issuers create and send Authorization Advice/0120 messages to the RiskFinder scoring system. The RiskFinder scoring system sends to the issuer an Authorization Advice Response/0130 message to acknowledge receipt of the Authorization Advice/0120 message.



1. The issuer initiates an Authorization Advice/0120—Issuer-generated message and sends it to the Authorization Platform. The Authorization Platform forwards the message to the RiskFinder scoring system.
2. The RiskFinder scoring system creates an Authorization Advice Response/0130—System-generated message and sends it to the Authorization Platform. The Authorization Platform forwards the Authorization Advice Response/0130—System-generated message to the issuer to indicate positive receipt of the Authorization Advice/0120—Issuer-generated message.

### **Authorization Advice/0120—System-generated**

When MasterCard responds to an Authorization Request/0100 message on behalf of the issuer, the Authorization Platform generates an authorization response based on the issuer's parameters. The Authorization Platform also generates an Authorization Advice/0120—System-generated message and stores it in a Store-and-Forward (SAF) queue. The Stand-In System will forward advice messages from the SAF queue when the issuer is available.



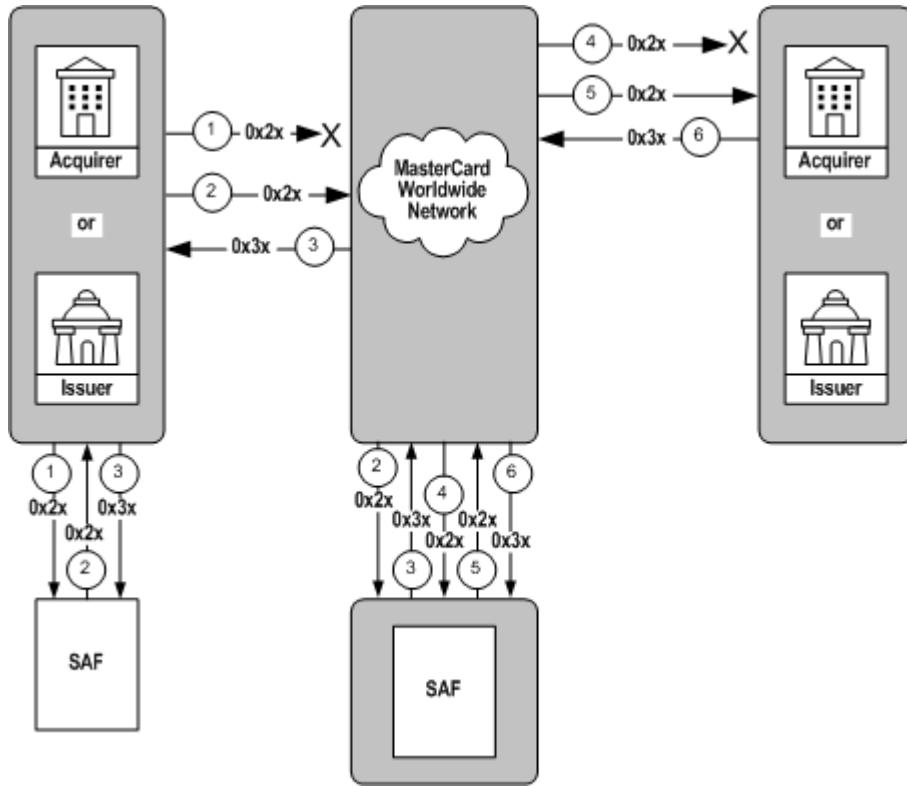
1. Stand-In system processing generates an Authorization Advice/0120—System generated message and sends it to the issuer.
2. The issuer returns an Authorization Advice Response/0130—Issuer-generated message.
3. The Authorization Platform receives the Authorization Advice Response/0130—Issuer-generated to indicate positive receipt of the Authorization Advice/0120—System-generated message.

**NOTE**

**Issuers may differentiate between the acquirer-generated or system-generated Authorization Advice/0120 messages by examining the values in DE 60 (Advice Reason Code).**

## Advice Message Error Condition

This message flow describes the advice message error-condition process.



1. An issuer or acquirer (any customer processing system [CPS]) generates an advice message. If the message cannot be transmitted immediately, it should be stored by an appropriate Store-and-Forward (SAF) facility on the CPS for later transmission to the Authorization Platform.
2. The CPS forwards the advice message to the Authorization Platform.
3. The Authorization Platform returns an appropriate advice response message when it secures the advice message.
4. The Authorization Platform immediately attempts to deliver the transaction to the receiving entity. If the Authorization Platform cannot deliver the message, it stores it at the MasterCard SAF facility for later delivery.
5. The Authorization Platform forwards the advice message to the receiving entity when communication is restored.
6. The receiving entity returns an appropriate advice response message as positive acknowledgement of receipt when it secures the advice message.

## **Message Definitions and Flows**

### **About Message Flows**

---

Not all advice messages flow “through” the Authorization Platform from one CPS to another CPS. For example, the Authorization Platform originates some advice messages and forwards them to a CPS. Similarly, a CPS may initiate some advice messages and forward them to the Authorization Platform as the receiving destination.

## Acquirer Response Acknowledgement/0180 Messages

This message flow ensures control over system error conditions due to technical processing errors or transaction “failures” occurring in the acquirer processing system (APS), the merchant’s device, or both. Specifically, it ensures that responsibility for proper posting and settlement falls to the acquirer. It protects the issuer (and the cardholder) from erroneous debits against their accounts due to incomplete or unsuccessful transactions.

The Authorization Platform provides optional interactive response acknowledgement for Authorization/0100 messages for acquirers. This process is accomplished using Authorization Acknowledgement/0180 messages.

**Acquirers are not required to support Authorization Acknowledgement/0180 messages**, but MasterCard encourages acquirers to select this option and to support these messages. Acquirers may select this option at network configuration time.



1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Authorization Request/0100 message to the issuer.
3. The issuer creates the appropriate Authorization Request Response/0110 message and sends it to the Authorization Platform.
4. The Authorization Platform forwards the Authorization Request Response/0110 message to the acquirer.
5. The acquirer sends an Authorization Acknowledgement/0180 message back to the Authorization Platform, indicating that the acquirer received and secured the preceding Authorization Request Response/0110 message at the application level.

In most cases, the acquirer should send the Authorization Acknowledgement/0180 message to the Authorization Platform:

- Immediately after it secures (or logs) the Authorization Request Response/0110 message
- Before the transaction actually is completed at the point of interaction

An Authorization Acknowledgement/0180 message does not necessarily indicate that the transaction was successfully completed at the point of interaction.

## **Alternate Issuer Host Processing for Online Europe Region Members**

To support customers in the Europe region that route to an alternate issuer host for alternate processing instead of using the Stand-In System, MasterCard offers alternate issuer host processing.

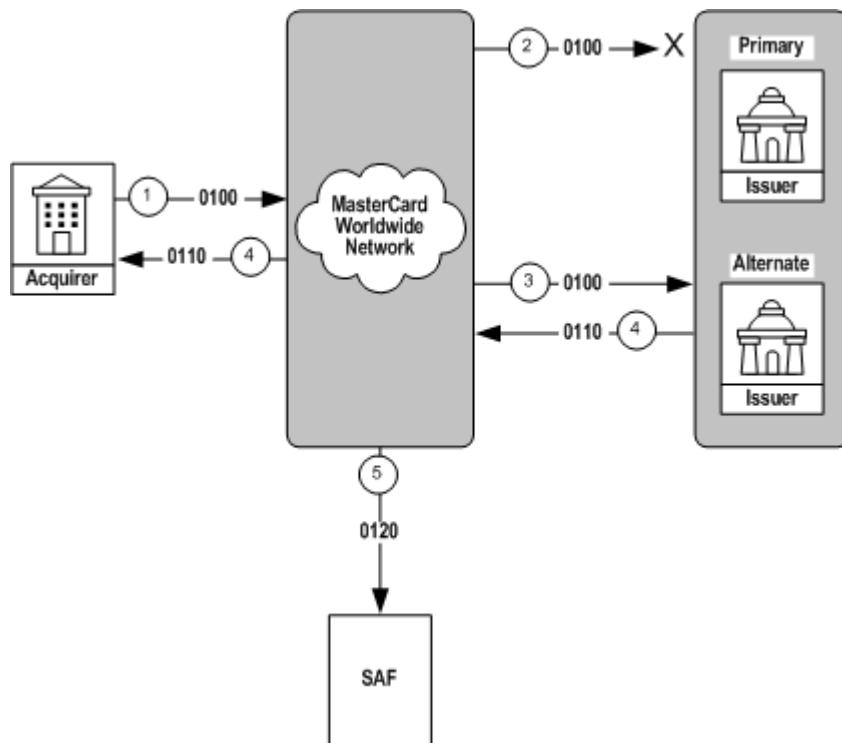
The system routes transactions to the alternate issuer for those issuers that choose to use alternate issuer host processing as their secondary path.

**NOTE**

[\*\*Authorization Message Routing Timers\*\*](#) provides details on time limits.

## Authorization Request/0100—Communication Failure at Issuer (Issuer is not signed in or transaction cannot be delivered)

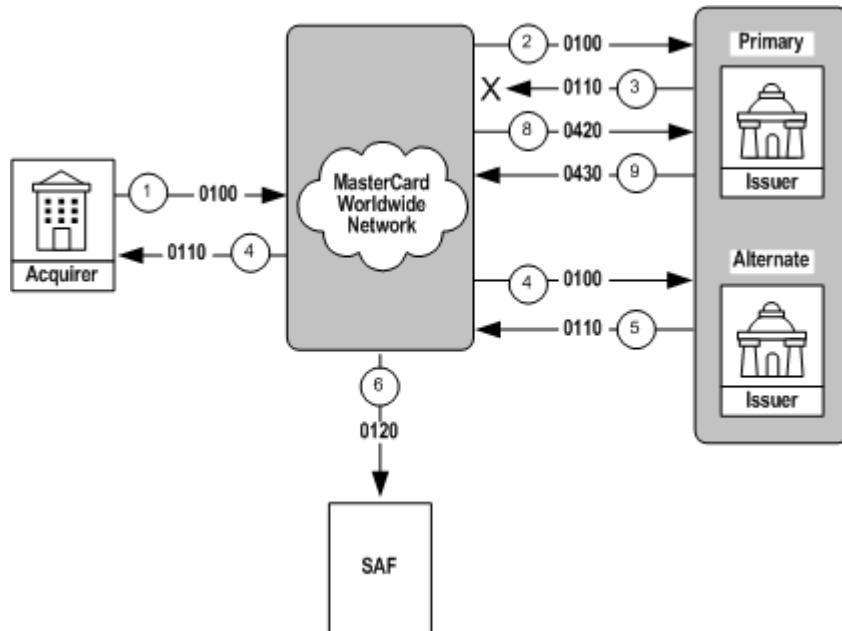
This message flow describes exception processing when the primary issuer is not signed in, the transaction could not be delivered to the primary issuer, or when the primary issuer does not respond with an Authorization Response/0110 message within the time limit defined for the acceptance brand.



1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization Platform.
2. The Authorization Platform attempts to forward the Authorization Request/0100 message to the primary issuer but is unable to complete the message transmission because of a communication link failure or IPS failure.
3. The Authorization Platform immediately sends the Authorization Request/0100 message to the alternate issuer.
4. The alternate issuer generates an appropriate Authorization Request Response/0110 message on the primary issuer's behalf and forwards it to the acquirer.
5. The Authorization Platform generates an Authorization Advice/0120 message and forwards it to the Authorization Platform store-and-forward (SAF) process for later transmission to the primary issuer.

**Authorization Request Response/0110—Alternate Issuer Allowed**

This message flow describes exception processing when communication fails between the Authorization Platform and the issuer processing system (IPS) during an Authorization Request Response/0110 message.

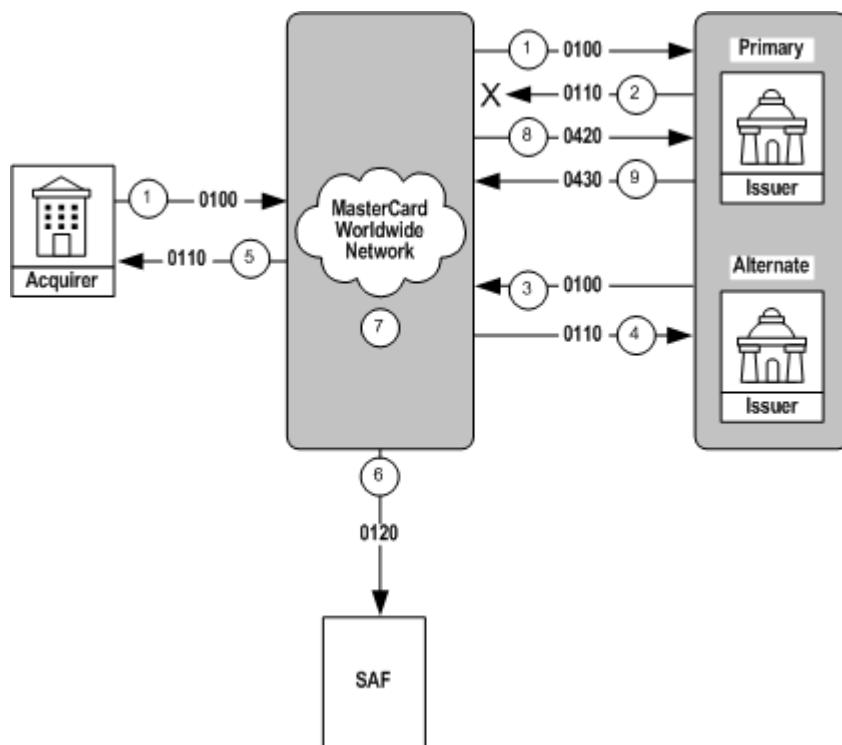


1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Authorization Request/0100 message to the primary issuer.
3. The IPS cannot return the appropriate Authorization Request Response/0110 message because of a communication failure between the IPS and the Authorization Platform.
4. The Authorization Platform detects an expected time-out condition from the primary issuer on the Authorization Request Response/0110 message. If the primary issuer permits alternate issuer processing, the Authorization Platform sends an Authorization Request/0100 message to the alternate issuer host.
5. The alternate issuer generates an appropriate Authorization Request Response/0110 message on the primary issuer's behalf and forwards it to the acquirer.
6. The Authorization Platform generates an Authorization Advice/0120 message and forwards it to the Authorization Platform SAF process for later transmission to the primary issuer.
7. The Authorization Platform does not receive the Authorization Request Response/0110 message from the primary issuer within the response time limits.

- 
8. The Authorization Platform sends a Reversal Advice/0420 message containing the following values to the primary issuer because no issuer response is received:
    - DE 39 (Response Code) = 82 (Time out at issuer)
    - DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) = 402 (Banknet advice: IPS time-out error)
  9. When the primary issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message.

## Authorization Request Response/0110—Not Received within Time Limit

This message flow describes exception processing when no issuer Authorization Request Response/0110 message is received within the time limit after receipt of the Authorization Request/0100 message for transactions that are allowed to be processed by the alternate issuer host.

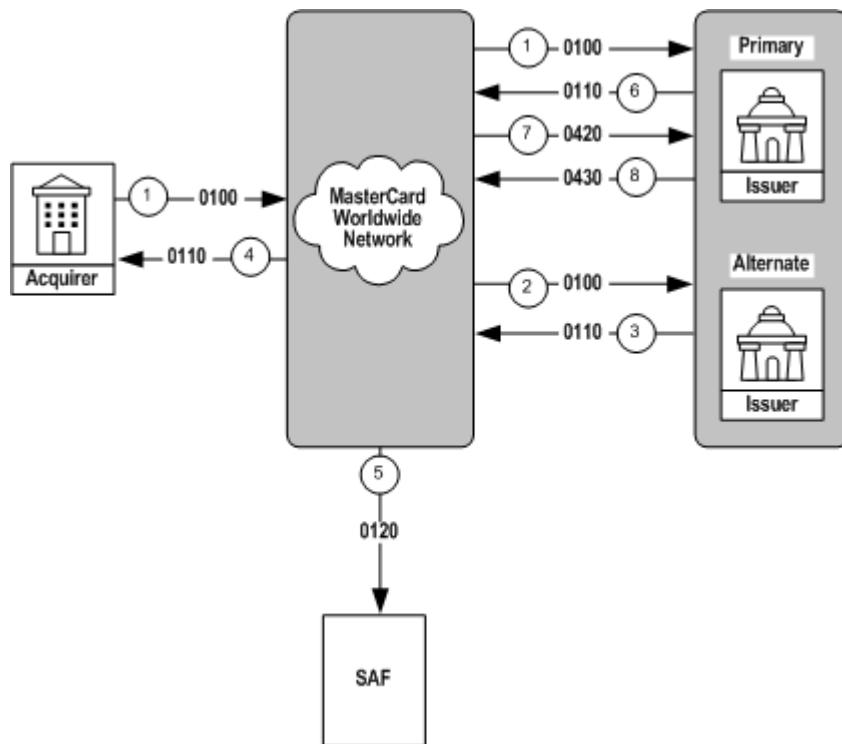


1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization Platform and then the Authorization Platform forwards the Authorization Request/0100 message to the primary issuer.
2. The Authorization Platform does not receive the Authorization Request Response/0110 message from the primary issuer within the time limit.
3. The Authorization Platform sends the Authorization Request/0100 message to the alternate issuer.
4. The alternate issuer forwards the Authorization Request Response/0110 message to the Authorization Platform.
5. The Authorization Platform forwards to the acquirer the Authorization Request Response/0110 message received from the alternate issuer.
6. The Authorization Platform creates an Authorization Advice/0120 message and stores it in a SAF queue for guaranteed delivery to the primary issuer.
7. The Authorization Platform does not receive the Authorization Request Response/0110 message from the primary issuer within the time limit.

- 
8. The Authorization Platform sends a Reversal Advice/0420 message containing the following values to the primary issuer because no issuer response is received:
    - DE 39 (Response Code) = 82 (Time out at issuer)
    - DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) = 402 (Banknet advice: IPS time-out error)
  9. When the primary issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.

## Authorization Request Response/0110—Received within the Time Limit but after Alternate Issuer Response

This message flow describes exception processing when the issuer's Authorization Request Response/0110 message is received within the time limit but after the alternate issuer response.

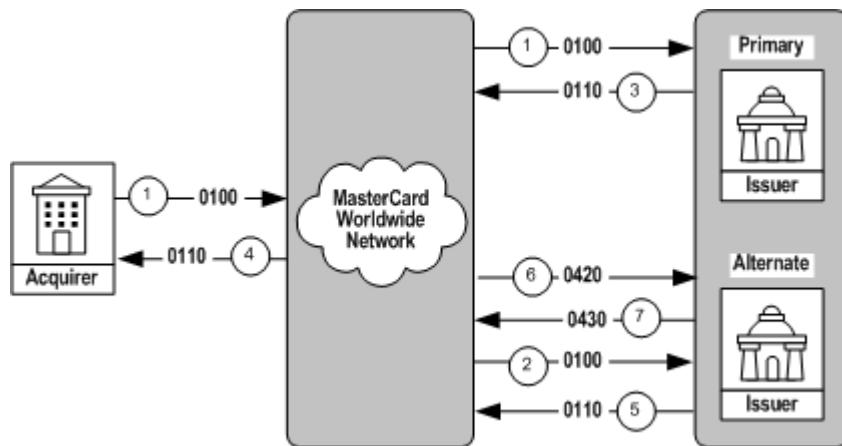


1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization Platform and then the Authorization Platform forwards the Authorization Request/0100 message to the primary issuer.
2. If the Authorization Platform does not receive the Authorization Request Response/0110 message from the primary issuer within the time limit, the Authorization Platform sends the Authorization Request/0100 message to the alternate issuer.
3. The alternate issuer forwards the Authorization Request Response/0110 message to the Authorization Platform.
4. The Authorization Platform sends the alternate issuer Authorization Request Response/0110 message to the acquirer.
5. The Authorization Platform creates an Authorization Advice/0120 message and stores it in a SAF queue for guaranteed delivery to the primary issuer.
6. The primary issuer's Authorization Request Response/0110 message is received within the time limit, but the primary issuer's response is not used because the primary issuer's response was received after the alternate issuer Authorization Request Response/0110 message.

- 
7. The Authorization Platform sends a Reversal Advice/0420 message containing the following values to the primary issuer to reverse the issuer's response that was not used:
    - DE 39 (Response code) = the value from the primary issuer's Authorization Request Response/0110 message
    - DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) = 400 (Banknet advice: APS error; unable to deliver response)
  8. When the primary issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.

## **Authorization Request Response/0110—Received within the Time Limit and before Alternate Issuer Response**

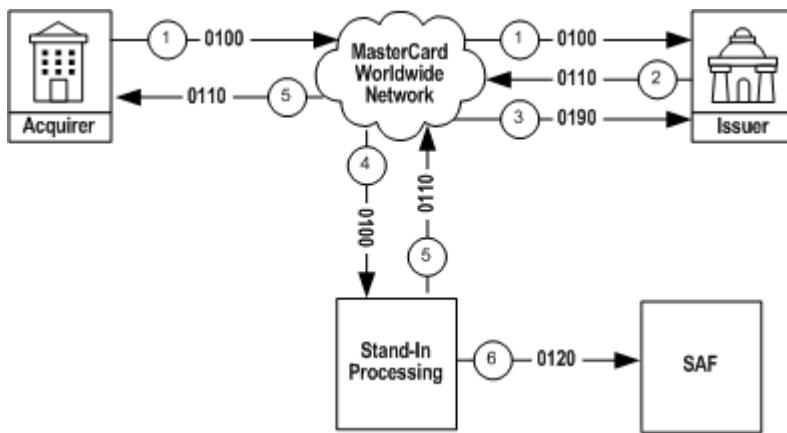
This message flow describes exception processing when the issuer's Authorization Request Response/0110 message is received within the time limit and before the alternate issuer response.



1. The acquirer sends the Authorization Request/0100 message to the Authorization Platform, and the Authorization Platform forwards the Authorization Request/0100 message to the primary issuer.
2. If the Authorization Platform does not receive the Authorization Request Response/0110 message within the time limit from the primary issuer, the Authorization Platform sends the Authorization Request/0100 message to the alternate issuer.
3. The primary issuer sends the Authorization Request Response/0110 message to the Authorization Platform.
4. The Authorization Platform receives the primary issuer's Authorization Request Response/0110 message within the time limit and before the alternate issuer's response and then sends the primary issuer's Authorization Request Response/0110 message to the acquirer.
5. The alternate issuer forwards the Authorization Request Response/0110 message to the Authorization Platform.
6. The Authorization Platform generates the Reversal Advice/0420 message for the alternate issuer to reverse the alternate issuer's response that was not used.
7. When the alternate issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.

## Authorization Response Negative Acknowledgement/0190 (Responding to the Authorization Request Response/0110)

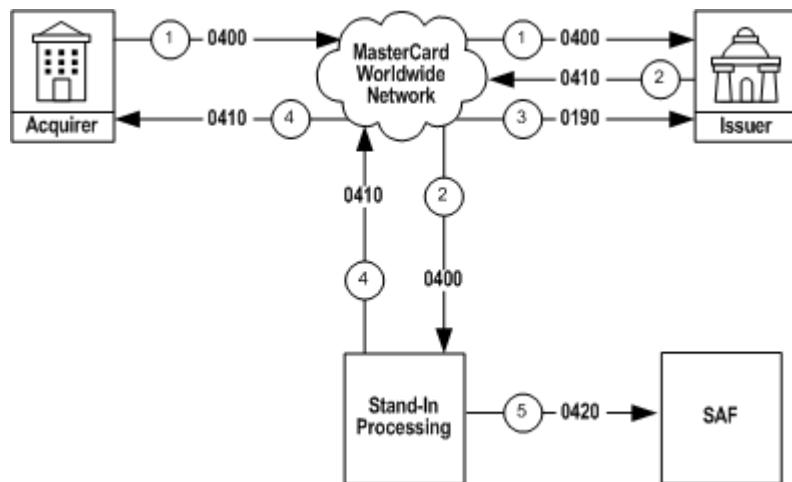
This message flow describes transaction processing when the issuer host generates an invalid or late Authorization Request Response/0110 message, and the Stand-In System processes the transaction and generates a response on behalf of the issuer. The Authorization Platform also sends an Authorization Response Negative Acknowledgement/0190 message to the issuer.



1. The acquirer sends the Authorization Request/0100 message.
2. The issuer generates an invalid or late Authorization Request Response/0110 message.
3. The Authorization Platform sends an Authorization Response Negative Acknowledgement/0190 message to the issuer.
4. The Authorization Platform sends the Authorization Request/0100 message to Stand-In processing.
5. Stand-In processing generates an appropriate Authorization Request Response/0110 message on the issuer's behalf and forwards it to the acquirer.
6. The Stand-In System also generates an Authorization Advice/0120 message and forwards it to the Authorization Platform SAF process for later transmission to the issuer.

## **Authorization Response Negative Acknowledgement/0190 (Responding to the Reversal Request Response/0410)**

This message flow describes transaction processing when the issuer host generates an invalid or late Reversal Request Response/0410 message, and the Authorization Platform processes the transaction and generates a response on behalf of the issuer. The Authorization Platform also sends an Authorization Response Negative Acknowledgement/0190 message to the issuer.



1. The acquirer sends the Reversal Request/0400 message.
2. The issuer generates an invalid or late Reversal Request Response/0410 message and forwards it to the Authorization Platform. The Authorization Platform routes the Reversal Request/0400 to the Stand-In System.
3. The Authorization Platform sends an Authorization Response Negative Acknowledgement/0190 message to the issuer.
4. The Authorization Platform generates the Reversal Request Response/0410 message and sends it to the acquirer.
5. The Stand-In System generates a Reversal Advice/0420 message and forwards it to the Authorization Platform SAF process for later transmission to the issuer.

### **NOTE**

**Members in the Europe region that route to an alternate issuer host for alternate processing instead of the Stand-In System will still receive an Reversal Advice/0420 as described here. Alternate issuer host processing does not send Reversal Request/0400 or Authorization Advice/0120 messages to the alternate host.**

## Issuer File Update Request/0302 and Issuer File Update Request Response/0312

This message flow describes transaction processing of the Issuer File Update Request/0302 message.



1. An issuer initiates an Issuer File Update Request/0302 message.
2. The Authorization Platform performs the requested issuer file update task and issues an Issuer File Update Request Response/0312 message back to the issuer. A Response Indicator field in the Issuer File Update Request Response/0312 message indicates whether the issuer file update was successfully completed.

### NOTE

**The error-condition message process for Issuer File Update/03xx messages are not illustrated. If an issuer unsuccessfully forwards an Issuer File Update Request/0302 message to the Authorization Platform, the issuer should retransmit the message.**

## **Reversal Messages**

Acquirers must send a Reversal Request/0400 message when the acquirer is unable to deliver an issuer's approved Authorization Request Response/0110 to a merchant. Merchants also may request their acquirer's to send a Reversal Request/0400 message to cancel the full or partial amount of the original authorization amount.

The Authorization Platform will not attempt to match the contents of the Reversal Request/0400 message with the contents of the original Authorization Request/0100 message.

### **NOTE**

**The acquirer must send the Reversal Request/0400 message immediately, or as soon as possible, after detecting that an approved Authorization Request Response/0110 message cannot be delivered to a merchant. An approved transaction has DE 39 (Response Code) value of 00 (Approved or completed successfully), 08 (Honor with ID), 10 (Partial Approval), or 87 (Purchase amount only, no cash back allowed).**

**The acquirer must send a Reversal Request/0400 message as a result of an acquirer time-out based on transaction processing rules dictated by the brand. When an acquirer sends a reversal, it is possible that an issuer will receive two reversals for the same authorization request. Issuers must decline subsequent reversal messages using the duplicate transmission response value DE 39 = 94.**

The following message flows describe Stand-In System processing of the Reversal Request/0400 message when:

- The issuer response is received within the time limit
- The issuer response is received after the time limit
- The issuer is signed off
- The issuer response contains errors
- The issuer does not receive the Reversal Request/0400 message

## Reversal Request/0400 and Reversal Request Response/0410

This message flow describes transaction processing of the Reversal Request/0400 and Reversal Request Response/0410 messages.



1. The acquirer initiates a Reversal Request/0400 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Reversal Request/0400 message to the issuer.
3. The issuer generates an appropriate Reversal Request Response/0410 message and sends it to the Authorization Platform.
4. The Authorization Platform forwards the Reversal Request Response/0410 message to the acquirer.

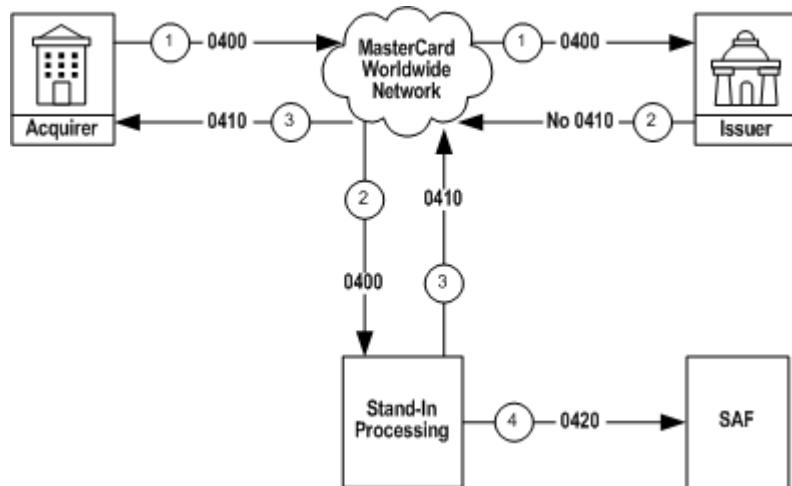
## Message Definitions and Flows

### About Message Flows

---

#### Reversal Request/0400—No Issuer Response Received within the Time Limit

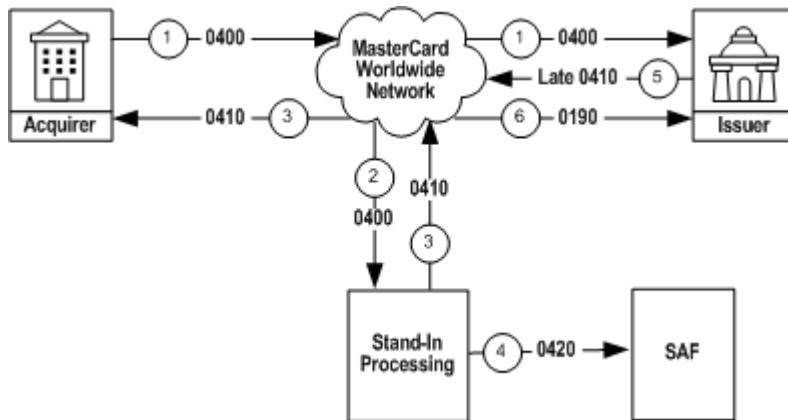
This message flow describes transaction processing of the Reversal Request/0400 message when the issuer response is not received within the time limit.



1. The acquirer sends the Reversal Request/0400 message to the Authorization Platform, and then the Authorization Platform forwards the Reversal Request/0400 message to the issuer.
2. If the Authorization Platform does not receive the issuer's Reversal Request Response/0410 message within the time limit, the Authorization Platform sends the Reversal Request/0400 message to the Stand-In System.
3. The Stand-In System sends the acquirer a Reversal Request Response/0410 message where DE 39 (Response Code) contains the value 00 (Approved or Completed Successfully).
4. The Stand-In System creates a Reversal Advice/0420 message and stores it in a SAF queue for guaranteed delivery to the issuer where:
  - DE 39 = Response Code value from the original Reversal Request/0400 message
  - DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) contains value 402 (Banknet advice: IPS time-out error)

## Reversal Request/0400—Issuer Response Received after the Time Limit

This message flow describes transaction processing when the issuer responds to the Reversal Request/0400 message after the time limit.



1. The acquirer sends the Reversal Request/0400 message to the Authorization Platform, and then the Authorization Platform forwards the Reversal Request/0400 message to the issuer.
2. If the Authorization Platform does not receive the issuer's Reversal Request Response/0410 message within the time limit, the Authorization Platform sends the Reversal Request/0400 message to the Stand-In System.
3. The Stand-In System sends the Reversal Request Response/0410 message containing DE 39, value 00 (Approved or completed successfully) to the acquirer.
4. The Stand-In System creates a Reversal Advice/0420 message and stores it in a SAF queue for guaranteed delivery to the issuer. The Reversal Advice/0420 message contains the following information:
  - DE 39 = Response Code value from the original Reversal Request/0400 message
  - DE 60, subfield 1 = 402 (Banknet advice: IPS time-out error)
5. The Authorization Platform receives the issuer's Reversal Request Response/0410 message after the time limit.
6. The Authorization Platform sends the Authorization Negative Acknowledgement/0190 message containing DE 39, value 68 (Response received late) to indicate it has no record of a corresponding Reversal Request/0400 message.

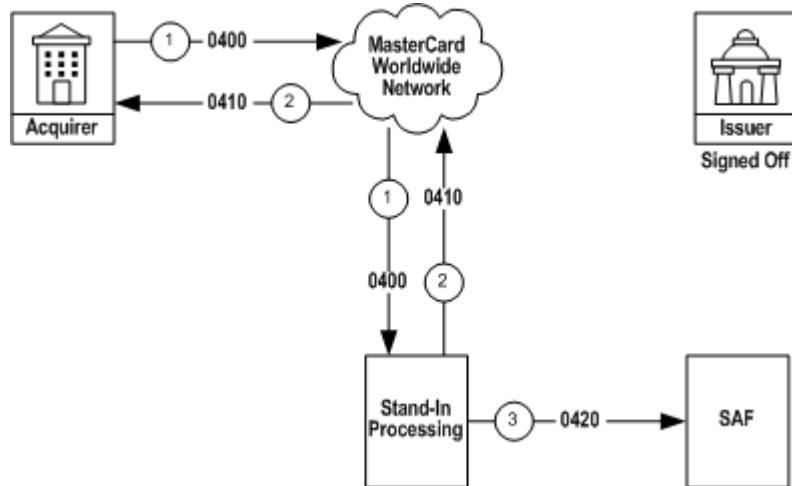
## Message Definitions and Flows

### About Message Flows

---

#### Reversal Request/0400—Issuer Signed Off

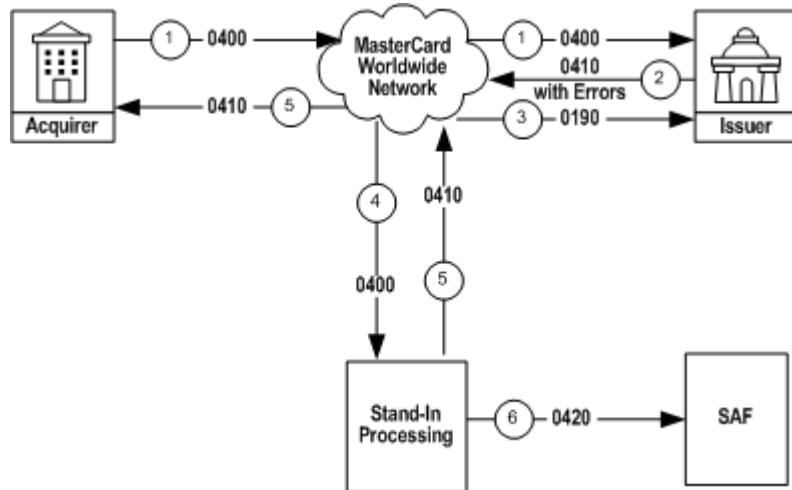
This message flow describes transaction processing when the issuer does not respond to the Reversal Request/0400 message because the issuer is signed off.



1. The acquirer sends the Reversal Request/0400 message to the Authorization Platform, and then the Authorization Platform forwards the Reversal Request/0400 message to the Stand-In System.
2. The Stand-In System sends the Reversal Request Response/0410 message containing DE 39, value 00 (Approved or completed successfully) to the acquirer.
3. The Stand-In System creates a Reversal Advice/0420 message and stores it in a SAF queue for guaranteed delivery to the issuer where:
  - DE 39 = Response Code value from the original Reversal Request/0400 message
  - DE 60, subfield 1 = 403 (Banknet advice: Issuer Signed Out)

## Reversal Request/0400—Issuer Response Contains Errors

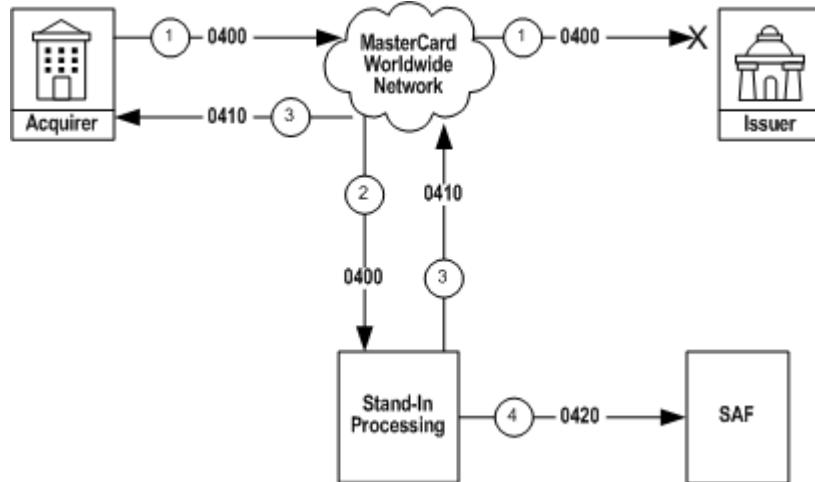
This message flow describes transaction processing when the issuer's response message contains errors.



1. The acquirer sends the Reversal Request/0400 message to the Authorization Platform, and then the Authorization Platform forwards the Reversal Request/0400 message to the issuer.
2. The Authorization Platform receives the issuer's Reversal Request Response/0410 message and the message contains errors.
3. The Stand-In System sends the Reversal Request Response/0410 message containing DE 39, value 00 (Approved or completed successfully) to the acquirer.
4. The Stand-In System creates a Reversal Advice/0420 message and stores it in a SAF queue for guaranteed delivery to the issuer where:
  - DE 39 = Response Code value from the original Reversal Request/0400 message
  - DE 60, subfield 1 = 409 (Banknet advice: Issuer Response Error)
5. The Authorization Platform sends the Authorization Negative Acknowledgement/0190 message containing DE 39, value 30 (Format error) and DE 44 containing the number of the data element in error.
6. The Authorization Platform sends the Reversal Request/0400 message to the Stand-In System.

**Reversal Request/0400—Not Delivered to Issuer**

This message flow describes transaction processing when the issuer does not receive the Reversal Request/0400 message.



1. The acquirer sends the Reversal Request/0400 message to the Authorization Platform and the Authorization Platform is unable to deliver the Reversal Request/0400 message to the issuer.
2. The Authorization Platform sends the Reversal Request/0400 message to the Stand-In System.
3. The Stand-In System sends the Reversal Request Response/0410 message containing DE 39, value 00 (Approved or completed successfully) to the acquirer.
4. The Stand-In System creates a Reversal Advice/0420 message and stores it in a SAF queue for guaranteed delivery to the issuer. The Reversal Advice/0420 message contains the following information:
  - DE 39 = Response Code value from the original Reversal Request/0400 message
  - DE 60, subfield 1 = 413 (Banknet advice: Issuer Undelivered)

## Reversal Request Response/0410—Not Delivered to Acquirer

This message flow describes transaction processing when the acquirer does not receive the Reversal Request Response/0410 message.



1. The acquirer sends the Reversal Request/0400 message to the Authorization Platform, and then the Authorization Platform forwards the Reversal Request/0400 message to the issuer.
2. The Authorization Platform receives the issuer's Reversal Request Response/0410 message.
3. The Authorization Platform cannot deliver the issuer's Reversal Request Response/0410 message to the acquiring host.
4. The Authorization Platform stores the Reversal Request/0400 and Reversal Request Response/0410 messages and takes no additional action.

### NOTE

**The acquirer has the responsibility to resend the Reversal Request/0400 message if the acquirer did not receive a response from the Authorization Platform.**

### **Reversal Advice/0420 and Reversal Advice Response/0430**

This message flow describes transaction processing of the Reversal Advice/0420 and the Reversal Advice/0430 messages.



1. The Authorization Platform sends a Reversal Advice/0420 message to the issuer.
2. The issuer responds to the Authorization Platform with a Reversal Advice Response/0430 message to acknowledge positive receipt of the Reversal Advice/0420 message.

## Administrative Request/0600 and Administrative Request Response/0610

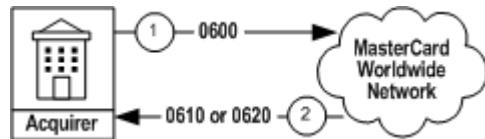
This message flow describes transaction processing of the Administrative Request/0600 and Administrative Request Response/0610 messages.



1. The acquirer initiates an Administrative Request/0600 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Administrative Request/0600 message to the issuer based on the account range contained in DE 2 (PAN).
3. The issuer sends an Administrative Request Response/0610 message to the Authorization Platform.
4. The Authorization Platform forwards the Administrative Request Response/0610 message to the acquirer.

## **Administrative Request/0600, Acquirer Edit Failure**

This message flow describes exception processing when the Authorization Platform determines an acquirer edit failure during processing an Administrative Request/0600 message.



1. The acquirer initiates an Administrative Request/0600 message and sends it to the Authorization Platform.
2. The Authorization Platform edits the Administrative Request/0600 message and detects an acquirer edit failure. As a result, the Authorization Platform notifies the acquirer using the Administrative Request Response/0610 when the Administrative Request/0600 message:
  - is missing mandatory data element
  - contains data attribute error or invalid data value
  - is from ineligible acquirer/processor
  - is sent to ineligible issuerOR  
Administrative Advice/0620 message when the Administrative Request/0600 message:
  - cannot be parsed
  - exceeds the maximum message length of 8k

## Administrative Request/0600, Communication Failure at Issuer

This message flow describes exception processing when communication fails between the issuer and the Authorization Platform during an Administrative Request/0600 message.



1. The acquirer initiates an Administrative Request/0600 message and sends it to the Authorization Platform.
2. The Authorization Platform attempts to forward the Administrative Request/0600 message to the issuer but is unable to complete the message transmission because of a technical problem.
3. As a result, the Authorization Platform sends the acquirer an Administrative Request Response/0610 message containing DE 39 (Response Code), value 92 (Unable to route transaction).

## **Administrative Request Response/0610, Communication Failure at Acquirer**

This message flow describes exception processing when communication fails between the Authorization Platform and the acquirer during an Administrative Request Response/0610 message.



1. The acquirer initiates an Administrative Request/0600 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Administrative Request/0600 message to the issuer based upon the account range contained in DE 2 (Primary Account Number [PAN]).
3. The issuer sends an Administrative Request Response/0610 message to the Authorization Platform.
4. The Authorization Platform attempts to forward the Administrative Request Response/0610 message to the acquirer but is unable to complete the message transmission because of a communication link failure or acquirer failure. As a result, the Authorization Platform logs the undelivered 0610 message and takes no further action. The acquirer host will time out the 0600 message and resend, if appropriate.

## Administrative Request Response/0610, No Issuer Response

This message flow describes exception processing when there is no response from the issuer to the Authorization Platform for an Administrative Request/0600 message.



1. The acquirer initiates an Administrative Request/0600 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Administrative Request/0600 message to the issuer based upon the account range contained in DE 2 (Primary Account Number [PAN]).
3. If the Authorization Platform receives no response from the issuer before the expiration of the response timer, the Authorization Platform sends the acquirer an Administrative Request Response/0610 message containing DE 39 (Response Code), value 91 (Authorization Platform or issuer system inoperative).

## **Administrative Request Response/0610, Late Issuer Response**

This message flow describes exception processing when the Authorization Platform receives a “late” Administrative Request Response/0610 message from the issuer.



1. The acquirer initiates an Administrative Request/0600 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Administrative Request/0600 message to the issuer based upon the account range contained in DE 2 (PAN).
3. If the Authorization Platform receives no response from the issuer before the expiration of the response timer, the Authorization Platform sends the acquirer an Administrative Request Response/0610 message containing DE 39 (Response Code), value 91 (Authorization Platform or issuer system inoperative).
4. If the Authorization Platform receives the issuer's response after expiration of the response timer, the Authorization Platform logs the late issuer 0610 message and takes no further action.

## Administrative Request Response/0610, Issuer Edit Failure

This message flow describes exception processing when the Authorization Platform receives an Administrative Request Response/0610 message that contains an edit failure from the issuer.



1. The acquirer initiates an Administrative Request/0600 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Administrative Request/0600 message to the issuer based upon the account range contained in DE 2 (PAN).
3. The issuer sends an Administrative Request Response/0610 message to the Authorization Platform.
4. The Authorization Platform edits the Administrative Request Response/0610 message and detects an issuer edit failure. As a result, the Authorization Platform notifies the issuer using the Administrative Advice/0620 when the Administrative Request Response/0610 message:
  - cannot be parsed
  - exceeds the maximum message length of 8k
  - is missing mandatory data element
  - contains a data attribute error or invalid data value
5. If the Authorization Platform receives an issuer response containing an edit failure, the Authorization Platform sends the acquirer an Administrative Request Response/0610 message containing DE 39 (Response Code), value 91 (Authorization Platform or issuer system inoperative).

## **Administrative Advice/0620 and Administrative Advice Response/0630**

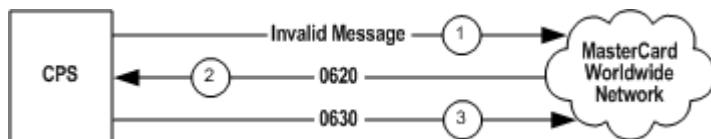
This message flow describes the standard Administrative Advice/06xx message process.



1. A customer processor system (CPS) generates an Administrative Advice/0620 message and forwards it to the Authorization Platform. Note that the CPS may be an issuer, an acquirer, or any other customer processing facility communicating via the Authorization Platform.
2. The Authorization Platform acknowledges receipt of the Administrative Advice/0620 message by returning an Administrative Advice Response/0630 message to the originating CPS.
3. The Authorization Platform forwards the Administrative Advice/0620 message to the receiving destination CPS.
4. The receiving CPS acknowledges receipt of the Administrative Advice/0620 message by returning an Administrative Advice Response/0630 message to the Authorization Platform.

## Administrative Advice/0620 and Administrative Advice Response/0630—Invalid Message, System-generated

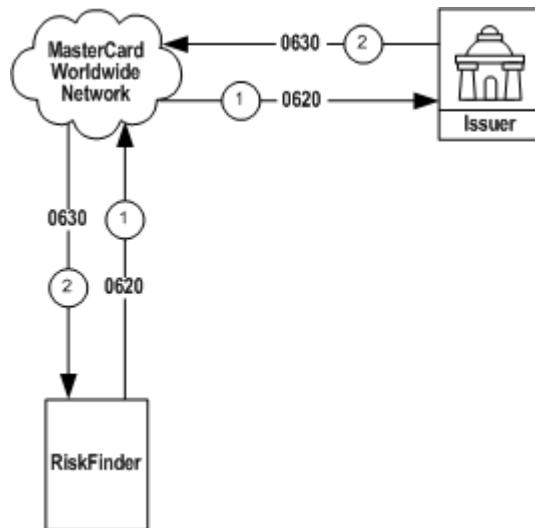
This message flow describes the standard Administrative Advice/06xx invalid message process.



1. A CPS generates an invalid message and forwards it to the Authorization Platform.
2. The Authorization Platform returns an Administrative Advice/0620 message to the CPS, with an appropriate error condition code indicating the point at which the Authorization Platform terminated message parsing or message processing.
3. The CPS acknowledges receipt of the Administrative Advice/0620 message and returns an Administrative Advice Response/0630 message to the Authorization Platform.

## **Administrative Advice/0620 and Administrative Advice Response/0630—RiskFinder, System-generated**

This message flow describes the administrative advice message process used to transmit risk scores generated by the RiskFinder scoring system to an issuer.



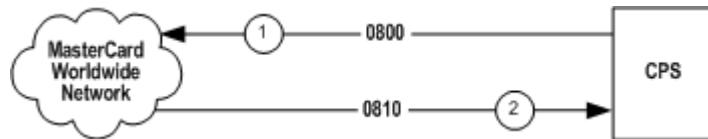
1. The RiskFinder scoring system sends an Administrative Advice/0620 message to the Authorization Platform for delivery to the issuer originating an Authorization Advice/0120—To RiskFinder message.
2. The issuer acknowledges receipt of the Administrative Advice/0620 message and returns an Administrative Advice Response/0630 message to the Authorization Platform for delivery back to the RiskFinder scoring system.

**NOTE**

**Error-condition message flows for Administrative Advice/06xx messages are not illustrated. If a CPS unsuccessfully forwards an Administrative Advice/0620 message to the Authorization Platform, the CPS should retransmit the message.**

## Network Management Request 0800—Sign-On/Sign-Off

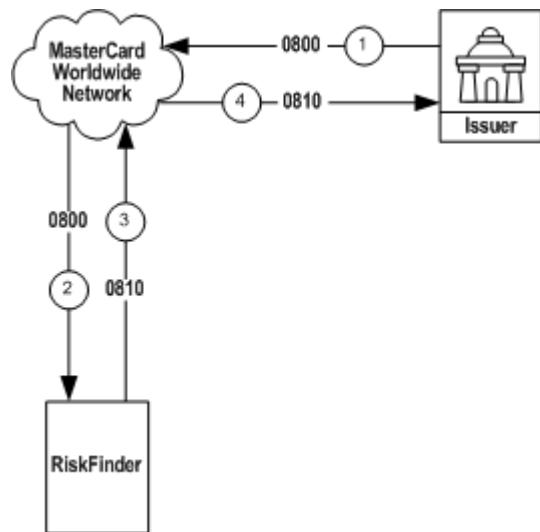
This message flow describes the standard Network Management Request/0800—Sign-On/Sign-Off message to sign on to the MasterCard Worldwide Network or to sign off from the MasterCard Worldwide Network.



1. The customer processing system (CPS) creates a Network Management Request—Sign-On/Sign-Off message and sends it to the Authorization Platform.
2. After receiving the Network Management Request—Sign-On/Sign-off message, the Authorization Platform creates a Network Management Request Response/0810—Sign-On/Sign-off message and sends it to the CPS.

## **Network Management Request/0800—RiskFinder Sign-On/Sign-Off**

This message flow describes the Network Management Request/0800—Sign-On/Sign-Off message sent by the issuer to sign on to or sign off from the RiskFinder™ scoring system.



1. Issuer creates a Network Management Request/0800—RiskFinder Sign-On/Sign-Off message and sends it to the MasterCard Worldwide Network.
2. After receiving the Network Management Request/0800—RiskFinder Sign-On/Sign-Off message, the MasterCard Worldwide Network forwards the Network Management Request/0800—RiskFinder Sign-On/Sign-Off message to RiskFinder.
3. RiskFinder creates an Network Management Request Response/0810—RiskFinder Sign-On/Sign-Off message and forwards it to the MasterCard Worldwide Network.
4. The MasterCard Worldwide Network forwards the Network Management Request Response/0810—RiskFinder Sign-On/Sign-Off message to the issuer.

## Network Management Request/0800—Solicited SAF

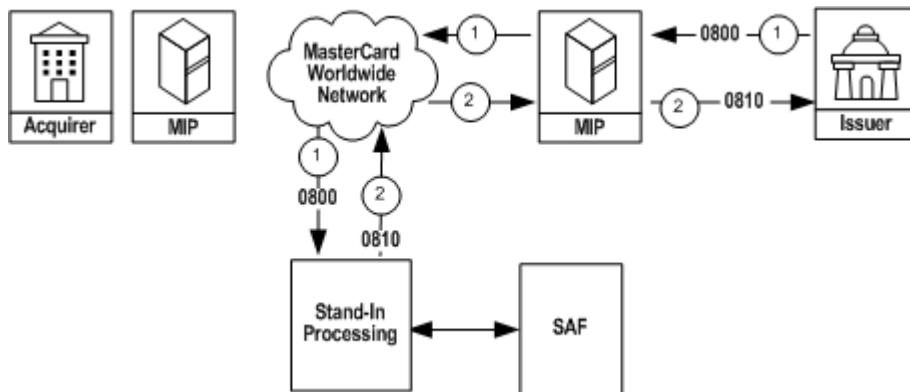
This message flow describes the issuer-initiated (solicited) SAF session using a Network Management Request/0800—SAF Request message.

### NOTE

**MasterCard no longer allows issuers to select the solicited SAF request option. Effective 22 June 2010, SAF participation for all group sign-in entries was changed to U (Unsolicited SAF).**

When an issuer has a large number of SAF records (for example, because of an extended outage), MasterCard can provide SAF records to the issuer using Complex-to-complex (CTC) file transmission.

When MasterCard begins to create the bulk file for transmission, it halts the online transmission of SAF records. This halt prevents MasterCard from distributing duplicate SAF records via an online transmission.



1. The issuer sends a Network Management Request/0800—SAF Request message to request a SAF session. The network management code included in DE 70 (Network Management Information Code) contains value 060 (SAF session request. The request is acknowledged; however, it will not affect SAF processing.)
2. The Stand-In System generates the Network Management Request Response/0810 acknowledgement message. After the Stand-In System responds to the issuer SAF request message, no further processing of the issuer's request is performed by the Stand-In System. All SAF messages are processed unsolicited.

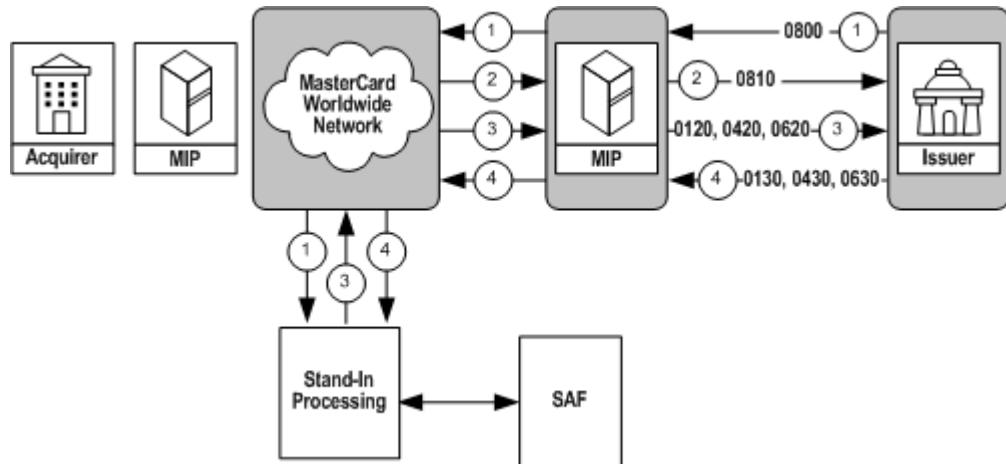
## Message Definitions and Flows

### About Message Flows

---

## Network Management Request/0800—Unsolicited SAF

This message flow describes the unsolicited SAF session with the issuer after the issuer has signed on to the MasterCard Worldwide Network using a Network Management Request/0800—Sign-On/Sign-Off message.



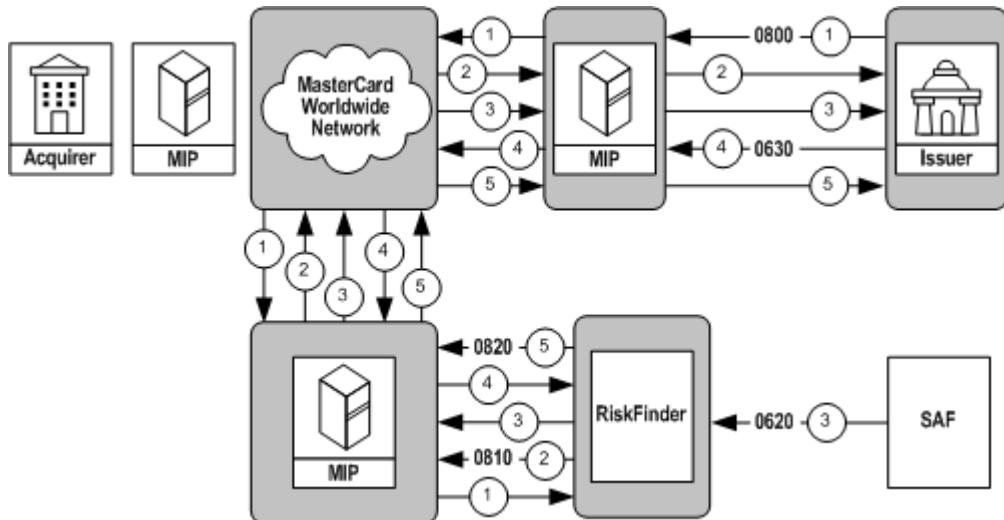
1. The issuer sends a Network Management Request/0800—Sign-On/Sign—Off message to sign on to the MasterCard Worldwide Network.
2. The Authorization Platform forwards a Network Management Request Response/0810 message acknowledging the issuer's sign-on request.
3. The Stand-In System checks for SAF messages in the queue and initiates a SAF session. The SAF process forwards an Authorization Advice/0120, Reversal Advice/0420, or Administrative Advice/0620 message to the issuer. The Stand-In System continues to check for SAF messages periodically as long as the issuer is signed in, and forwards messages if there are any available.
4. The issuer generates an Authorization Advice Response/0130, Reversal Advice Response/0430, or Administrative Advice Response/0630 message. These response messages advise the Stand-In System that the issuer received the previous Authorization Advice/0120, Reversal Advice/0420, or Administrative Advice/0620 message and prompt Stand-In processing to send the next Authorization Advice/0120, Reversal Advice/0420, or Administrative Advice/0620 message.

### NOTE

**Issuers receive SAF messages intermixed with authorization and reversal request messages.**

Network Management Request/0800—RiskFinder SAF

This message flow describes the issuer-initiated SAF session using a Network Management Request/0800—RiskFinder SAF message.



1. The issuer sends a Network Management Request/0800—RiskFinder SAF message to request a SAF session. The network management code included in DE 70 (Network Management Information Code) contains value 070 (Sign-On to RiskFinder by prefix member requests RiskFinder-scored Administrative Advice/0620 messages).
  2. The RiskFinder System generates a Network Management Request Response/0810 acknowledgement message.
  3. The SAF process forwards an Administrative Advice/0620 message to the issuer.
  4. The issuer generates an Administrative Advice Response/0630 message. These response messages advise the RiskFinder System that the issuer received the previous Administrative Advice/0620 message and prompts the RiskFinder System to send the next Administrative Advice/0620 message.

Each time the RiskFinder System receives a 0630 message, RiskFinder sends the issuer the next message. If the RiskFinder System does not receive an 0630 message within three minutes, RiskFinder assumes the issuer did not receive the previous message and ends the SAF session.

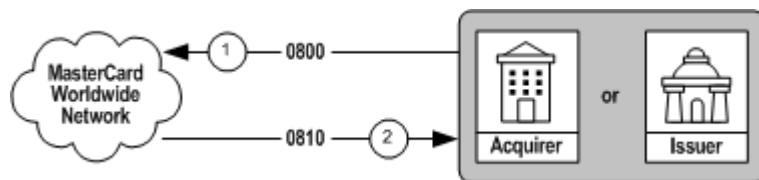
- When there are no more Administrative Advice/0620 messages in the queue, the RiskFinder System generates a Network Management Advice/0820 message containing DE 70, value 072 (End of file encountered for RiskFinder SAF traffic).

## **Network Management Request/0800—Network Connection Status, Member-generated**

This message flow describes transaction processing of the Network Management Request/0800—Network Connection Status, Member-generated message.

Members should send the Network Management Request/0800 message with DE 70 (Network Management Information Code) is 270 (Network Connection Status—echo test) when they want to investigate the status of their MasterCard Worldwide Network connection to MasterCard instead of using a repeat sign on message.

MasterCard will respond with a Network Management Request Response/0810 message containing DE 70, value 270 indicating positive acknowledgement of the Network Management Request/0800 message.



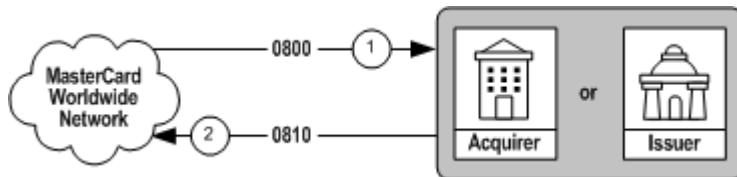
1. The customer sends a Network Management Request/0800—Network Connection Status, Member-generated message where DE 70 is 270 to the Authorization Platform to verify the customer's connection to the MasterCard Worldwide Network.
2. The Authorization Platform responds with a Network Management Request Response/0810—Network Connection Status, System-generated message to confirm that the connection is active.

## Network Management Request/0800—Network Connection Status, System-generated

This message flow describes transaction processing of the Network Management Request/0800—Network Connection Status, System-generated message.

Members that request MasterCard to periodically check the status of their connection to the MasterCard Worldwide Network will receive the Network Management Request/0800 message with DE 70 (Network Management Information Code) is 270 (Network Connection Status—echo test) from MasterCard.

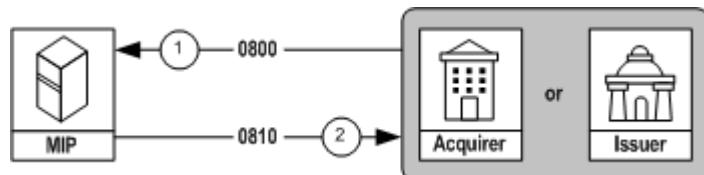
A customer must respond with a Network Management Request Response/0810 message containing DE 70, value 270 to indicate positive acknowledgement of the Network Management Request/0800 message.



1. The Authorization Platform sends a Network Management Request/0800—Network Connection Status, System-generated message where DE 70 is 270 to the customer to verify the customer's connection to the MasterCard Worldwide Network.
2. The customer responds with a Network Management Request Response/0810—Network Connection Status, Member-generated message to confirm that the connection is active.

## **Network Management Request/0800—Host Session Activation/Deactivation**

This message flow describes transaction processing of the Network Management Request/0800—Host Session Activation/Deactivation message.



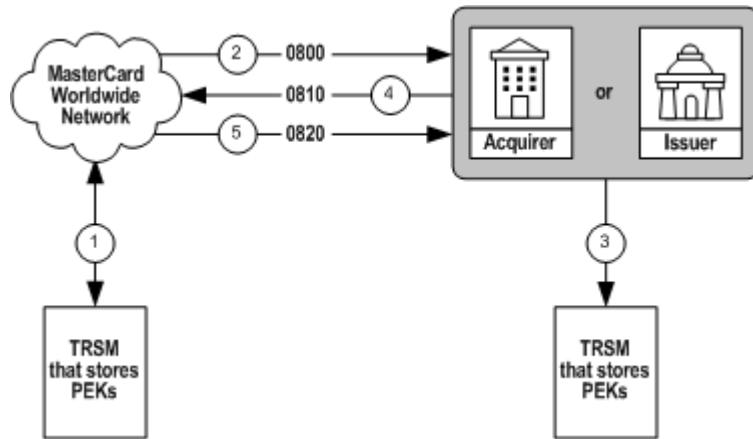
1. The customer sends a Network Management Request/0800—Host Session Activation/Deactivation message where DE 70 (Network Management Information Code) contains either a value of 081 (Host session activation) or 082 (Host session deactivation) to identify session activation or session deactivation to the MasterCard interface processor (MIP).
2. The MIP responds with a Network Management Request Response/0810—Host Session Activation/Deactivation message containing DE 39 (Response Code), value 00 (Approved or completed successfully).

**NOTE**

**The Dynamic PIN Key (PEK) service is not available for use by customers in the Europe region that use MasterCard Worldwide Network PIN Processing services. The Dynamic PIN Key service is available to members outside the Europe region that use Single Message System PIN Processing services.**

## Network Management Request/0800—PEK Exchange Authorization Platform-Initiated

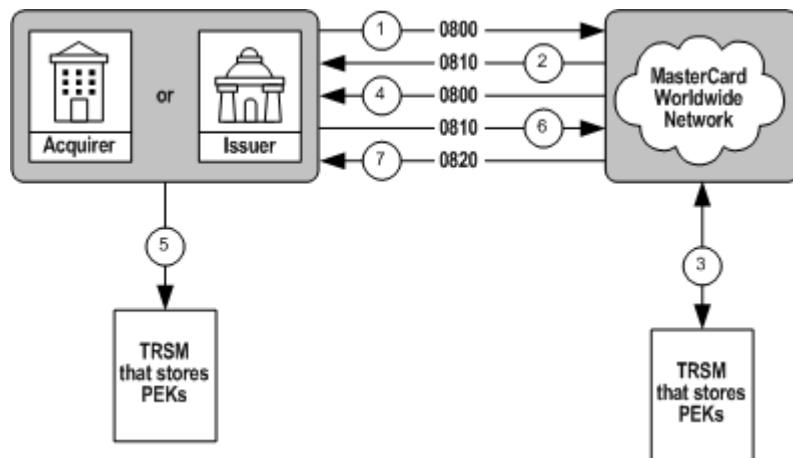
This message flow describes transaction processing as it exchanges new PEKs with the customer every 24 hours or every 2,500 transactions, whichever occurs first.



1. The pre-determined time or number of transactions has passed for exchanging a new PEK. The Authorization Platform uses the Key Encryption Key (KEK) on the tamper-resistant security module (TRSM) to encrypt the new PEK.
2. The Authorization Platform sends a Network Management Request/0800—PEK Exchange message containing the PEK. The message contains the new PEK (encrypted using the KEK) in DE 48 and the customer ID in DE 2 (Primary Account Number [PAN]). The customer uses the PEK for PIN translation in subsequent Authorization Request/0100 messages.
3. The customer stores the new PEK on its TRSM.
4. The customer sends a Network Management Request Response/0810—PEK Exchange message to the Authorization Platform acknowledging receipt of the Network Management Request/0800—PEK Exchange message exchanging the PEK. If the message does not contain DE 39 (Response Code) with the value 00 (Approved or completed successfully), the Authorization Platform sends another Network Management Request/0800—PEK Exchange message.
5. The Authorization Platform sends a Network Management Advice/0820—PEK Exchange message to notify the customer that the new PEK is active and operational. Subsequent Authorization Request/0100 messages must use the new PEK to translate the PIN data in DE 52 (Personal ID Number [PIN] Data).

## Network Management Request/0800—PEK Exchange Member-Initiated

Customers must be capable of sending a Network Management Request/0800—PEK Exchange—Member-initiated message to the Authorization Platform requesting a new PEK. The Authorization Platform immediately initiates a PEK exchange with the customer identified in DE 33 (Forwarding Institution ID Code) of the Network Management Request/0800—PEK Exchange—On Demand message. The customer should use this feature when systems problems occur and a re-synchronization of the PEK is necessary.



1. The customer determines there is a problem with its PEK and sends a Network Management Request/0800—PEK Exchange—On Demand message to the Authorization Platform requesting a new PEK.
2. The Authorization Platform responds with a Network Management Request Response/0810—PEK Exchange—On Demand message.
3. The Authorization Platform uses the KEK on its TRSM to encrypt the new PEK.
4. The Authorization Platform sends a Network Management Request/0800—PEK Exchange message containing the new PEK. The message contains the new PEK (encrypted using the KEK) in DE 48 and the associated ID of the customer, identified in DE 2 (Primary Account Number [PAN]). The customer uses the PEK for PIN encryption in subsequent Authorization Request/0100 messages.
5. The customer stores the new PEK on its TRSM.
6. The customer sends a Network Management Request Response/0810—PEK Exchange message to the Authorization Platform acknowledging receipt of the Network Management Request/0800—PEK Exchange message exchanging the PEK. If the message does not contain DE 39 (Response Code) with the value 00 (Approved or completed successfully), the Authorization Platform sends another Network Management Request/0800—PEK Exchange message.

7. The Authorization Platform sends a Network Management Advice/0820—PEK Exchange message to the customer notifying it that the new PEK is active and operational. Subsequent Authorization Request/0100 messages must use the new PEK to translate the PIN in DE 52.

**NOTE**

**Error-condition message flows for Network Management/08xx messages are not illustrated. If an APS or IPS unsuccessfully forwards a Network Management/08xx message to the Authorization Platform, the APS or IPS should retransmit the message.**

---

## Chapter 3 Message Layouts

*This section describes the required, conditional, optional, or Authorization Platform-provided data element layouts for all messages that the Authorization Platform supports.*

---

Authorization Request/0100 .....	3-1
Authorization Request Response/0110.....	3-5
Authorization Advice/0120—Acquirer-generated.....	3-9
Authorization Advice/0120—Issuer-generated.....	3-13
Authorization Advice/0120—System-generated .....	3-16
Authorization Advice Response/0130—Issuer-generated (Responding to a System-generated 0120 from SAF) .....	3-19
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120).....	3-21
Authorization Advice Response/0130—System-generated (Responding to an Acquirer-generated 0120).....	3-24
Authorization Advice Response/0130—System-generated (Responding to an Issuer-generated 0120).....	3-26
Authorization Response Acknowledgement/0180.....	3-28
Authorization Response Negative Acknowledgement/0190.....	3-29
Issuer File Update Request/0302.....	3-30
Issuer File Update Request Response/0312 .....	3-31
Reversal Request/0400 .....	3-32
Reversal Request Response/0410 .....	3-37
Reversal Advice/0420 .....	3-40
Reversal Advice Response/0430.....	3-44
Administrative Request/0600.....	3-46
Administrative Request Response/0610 .....	3-48
Administrative Advice/0620—System-generated .....	3-50
Administrative Advice/0620—Member-generated .....	3-52
Administrative Advice Response/0630 .....	3-53
Network Management Request/0800—Sign-On/Sign-Off .....	3-54
Network Management Request/0800—RiskFinder SAF Request .....	3-56
Network Management Request/0800—Network Connection Status, Member-generated .....	3-57
Network Management Request/0800—Network Connection Status, System-generated .....	3-58
Network Management Request/0800—Host Session Activation/Deactivation.....	3-59

## **Message Layouts**

---

Network Management Request/0800—PEK Exchange.....	3-60
Network Management Request/0800—PEK Exchange On Demand.....	3-61
Network Management Request Response/0810—Sign-On/Sign-Off .....	3-62
Network Management Request Response/0810—RiskFinder SAF Request .....	3-63
Network Management Request Response/0810—Network Connection Status, Member-generated.....	3-64
Network Management Request Response/0810—Network Connection Status, System-generated.....	3-65
Network Management Request Response/0810—Host Session Activation/Deactivation .....	3-66
Network Management Request Response/0810—PEK Exchange .....	3-67
Network Management Request Response/0810—PEK Exchange-On Demand.....	3-68
Network Management Advice/0820—RiskFinder SAF End of File .....	3-69
Network Management Advice/0820—PEK Exchange .....	3-70

## Authorization Request/0100

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	M	•	M	Constant—0100 (Authorization Request).
- Bit Map, Primary	M	•	M	
1 Bit Map, Secondary	C	•	C	Required data element if DE 65–DE 128 are present in the message.
2 Primary Account Number (PAN)	M	•	M	
3 Processing Code	M	•	M	
4 Amount, Transaction	M	•	M	Transaction amount, in the acquirer's currency, at the point of interaction.
5 Amount, Settlement	•	X	C	Transaction amount, in the reporting currency, as specified within individual MasterCard programs and services; the Authorization Platform provides DE 5 if the issuer chooses to receive settlement amount-related data elements.
6 Amount, Cardholder Billing	•	X	M	Transaction amount in the issuer currency. The Authorization Platform provides this data element.
7 Transmission Date and Time	M	•	M	Transaction time stamp; UTC date and time that this transaction was entered into the interchange.
9 Conversion Rate, Settlement	•	X	C	The Authorization Platform provides DE 9 if the issuer chooses to receive settlement amount-related data elements.
10 Conversion Rate, Cardholder Billing	•	X	M	The Authorization Platform provides DE 10 with the rate used to convert the transaction currency to the cardholder billing currency. If the acquirer and issuer currency are the same, this value will be 61000000.
11 Systems Trace Audit Number (STAN)	M	•	M	
12 Time, Local Transaction	C	•	C	Used in all customer-related reports and statements, if available. Required for ATM, Chip, and POS card-read transactions. Required for MasterCard Hosted Mobile Phone Top-up transactions.

## Message Layouts

### Authorization Request/0100

Data Element ID and Name	Org	Sys	Dst	Comments
13 Date, Local Transaction	C	•	C	Used in all customer-related reports and statements, if available. Required for ATM, Chip, and POS card-read transactions. Required for MasterCard Hosted Mobile Phone Top-up transactions.
14 Date, Expiration	C	•	C	
15 Date, Settlement	•	X	M	The acquirer omits this data element, and the Authorization Platform inserts it and forwards it to the issuer.
16 Date, Conversion	•	X	M	Currency conversion rate file effective date. The Authorization Platform provides this data element.
18 Merchant Type	M	•	M	Refer to the <i>Quick Reference Booklet</i> for a listing of MCCs.
20 Primary Account Number (PAN) Country Code	C	•	C	
22 Point-of-Service (POS) Entry Mode	M	•	M	
23 Card Sequence Number	C	•	C	Conditional data for chip transactions.
26 Point-of-Service (POS) Personal ID Number (PIN) Capture Code	C	•	C	
28 Amount, Transaction Fee	C	•	C	Must contain fee amount, if applied.
32 Acquiring Institution ID Code	M	•	M	
33 Forwarding Institution ID Code	C	•	C	
35 Track 2 Data	C	X	C	Required if the transaction entry point captured Track 2 data. Required for ATM transactions. For Maestro transactions, such as e-commerce, the Authorization Platform creates Track 2 data if it is not provided by the acquirer.
37 Retrieval Reference Number	C	•	C	Required for ATM, Chip and POS card-read transactions.
41 Card Acceptor Terminal ID	C	•	C	Required for ATM transactions.
42 Card Acceptor ID Code	C	•	C	Mandatory for POS transaction types containing DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), values 00 (Purchase), 09 (Purchase with Cash Back) and 28 (Payment Transaction).

**Message Layouts**  
**Authorization Request/0100**

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
43 Card Acceptor Name and Location	C	•	C	Required for Chip and POS card-read transactions. Required for MasterCard Hosted Mobile Phone Top-up transactions.
45 Track 1 Data	C	•	C	Required if the transaction entry point captured track 1 data.
48 Additional Data—Private Use	M	X	M	Contains applicable subelement data.
49 Currency Code, Transaction	M	•	M	
50 Currency Code, Settlement	•	X	C	The Authorization Platform provides DE 50 if the issuer chooses to receive settlement amount-related data elements.
51 Currency Code, Cardholder Billing	•	X	M	The Authorization Platform provides this data element.
52 Personal ID Number (PIN) Data	C	X	C	Required for ATM transactions.
53 Security-Related Control information	C	X	C	Required for acquirers using the Authorization Platform to perform PIN translation services. Acquirers provide DE 53 to identify the PIN Block Format and key used for PIN encryption.  The Authorization Platform provides issuers that perform PIN translation services using the Authorization Platform the PIN Block Format and key that was used by MasterCard to encrypt the PIN before sending the Authorization Request/0100 to the issuer.
54 Additional Amounts	C	X	C	The Authorization Platform will forward the occurrence of each DE 54 amount type provided by the acquirer in the acquirer's currency and will provide an additional occurrence of each DE 54 amount type in the issuer's currency.
55 Integrated Circuit Card (ICC) System-Related Data	C	•	C	Conditional data for chip-based transactions.
61 Point-of-Service (POS) Data	M	•	M	
62 Intermediate Network Facility (INF) Data	O	•	O	
63 Network Data	•	X	M	
112 Additional Data—National Use	C	•	C	Contains applicable subelement data.
120 Record Data	C	X	C	

## Message Layouts

### Authorization Request/0100

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
124 Member-defined Data	O	•	C	May contain customer-defined data; required for MasterCard® <i>MoneySend</i> ™ transactions.
125 New PIN Data	C	X	C	Must be present for all PIN change transactions; otherwise not present
127 Private Data	O	X	•	Private data for message initiator's use.

## Authorization Request Response/0110

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	M	•	M	Constant—0110 (Authorization Request Response).
- Bit Map, Primary	M	•	M	
1 Bit Map, Secondary	C	•	C	Mandatory if DE 65–DE 128 are present in the message.
2 Primary Account Number (PAN)	ME	•	ME	Must be the same value as in the original Authorization Request/0100.
3 Processing Code	ME	•	ME	Must be the same value as in the original Authorization Request/0100.
4 Amount, Transaction	CE	X	M	Must be the same value as in the original Authorization Request/0100 except when DE 39 contains value 10 (Partial approval) or value 87 (Purchase Amount Only—No Cash Back Allowed).
5 Amount, Settlement	CE	X	C	Must be the same value as in the original Authorization Request/0100, if present, except when DE 39 contains value 10 (Partial approval) or value 87 (Purchase Amount Only—No Cash Back Allowed). The Authorization Platform provides this data element if the acquirer chooses to receive settlement amount-related data elements. <sup>1</sup>
6 Amount, Cardholder Billing	C	•	C	Must be the same value as in the original Authorization Request/0100, except when DE 39 contains value 10 (Partial approval) or value 87 (Purchase Amount Only—No Cash Back Allowed). <sup>1</sup>
7 Transmission Date and Time	ME	•	ME	Must be the same value as in the original Authorization Request/0100.
9 Conversion Rate, Settlement	CE	X	C	Must be the same value as in the original Authorization Request/0100, if present. The Authorization Platform provides this data element if the acquirer chooses to receive settlement amount-related data elements. <sup>1</sup>

---

1. This data will be present, as defined, except when the Authorization Platform has declined an Authorization Request/0100 message and was unable to complete currency conversion processing.

## Message Layouts

### Authorization Request Response/0110

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
10 Conversion Rate, Cardholder Billing	C	•	C	Must be the same value as in the original Authorization Request/0100. <sup>1</sup>
11 Systems Trace Audit Number (STAN)	ME	•	ME	Must be the same value as in the original Authorization Request/0100.
15 Date, Settlement	ME	•	ME	Must be the same value as in the original Authorization Request/0100.
16 Date, Conversion	C	•	C	Must be the same value as in the original Authorization Request/0100. <sup>1</sup>
20 Primary Account Number (PAN) Country Code	CE	•	CE	Must be the same value as in the original Authorization Request/0100, if present.
28 Amount, Transaction Fee	CE	X	CE	Must be the same value as in the original Authorization Request/0100, if present.
32 Acquiring Institution ID Code	ME	•	ME	Must be the same value as in the original Authorization Request/0100.
33 Forwarding Institution ID Code	CE	•	CE	Must be the same value as in the original Authorization Request/0100, if present.
37 Retrieval Reference Number	CE	•	CE	Must be the same value as in the original Authorization Request/0100, if present.
38 Authorization ID Response	C	•	C	Response ID that the authorizing institution or agent assigned for approved requests.
39 Response Code	M	•	M	Contains message-specific values. See the data element details for list of values by message type. <sup>2</sup>
41 Card Acceptor Terminal ID	CE	•	CE	Must be the same value as in the original Authorization Request/0100, if present.
44 Additional Response Data	C	•	C	May be used for referral phone numbers in denied transactions, or cardholder ID information in approved transactions.
48 Additional Data—Private Use	C	•	C	Contains applicable subelement data.
49 Currency Code, Transaction	ME	•	ME	Must be the same value as in the original Authorization Request/0100.

2. Issuers responding with DE 39 (Response Code), value 10 (Partial approval) or value 87 (Purchase amount only, no cash back allowed) will not be required to echo DE 4 (Amount, Transaction) in the Authorization Request Response/0110. Likewise, if DE 5 (Amount, Settlement) was present in the Authorization Request/0100 to the issuer, the issuer will not be required to echo DE 5 in the Authorization Request Response/0110 when responding with DE 39, value 10 or value 87. The issuer will provide the partial approval amount in DE 6 (Amount, Cardholder Billing).

**Message Layouts**  
**Authorization Request Response/0110**

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
50 Currency Code, Settlement	CE	X	C	Must be the same value as in the original Authorization Request/0100, if present. The Authorization Platform provides this data element if the acquirer chooses to receive settlement amount-related data elements. <sup>1</sup>
51 Currency Code, Cardholder Billing	C	•	C	Must be the same value as in the original Authorization Request/0100. <sup>1</sup>
54 Additional Amounts	C	X	C	The Authorization Platform will forward the occurrence of each DE 54 amount type as provided by the issuer in the issuer's currency and will provide an additional occurrence of each DE 54 amount type in the acquirer's currency.
55 Integrated Circuit Card (ICC) System-Related Data	C	•	C	Conditional data for chip-based transactions.
62 Intermediate Network Facility (INF) Data	CE	•	CE	Must be the same value as in the original Authorization Request/0100 message, if present.
63 Network Data	ME	•	ME	Must be the same value as in the original Authorization Request/0100.
102 Account ID-1	C	•	C	May contain cardholder "from" account number.
103 Account ID-2	C	•	C	May contain cardholder "to" account number.
112 Additional Data—National Use	C	•	C	Contains applicable subelement data.
120 Record Data	CE	•	CE	Must be the same value as in the original Authorization Request/0100 message, if present.
121 Authorizing Agent ID Code	C	•	C	Contains the MasterCard customer ID of an alternate authorizer, if authorized by other than the issuer or issuer's primary authorizer.
123 Receipt Free Text	O	X	C	Optional for issuers. Present for acquirers if provided by the issuer. If not supported by the acquirer, the Authorization Platform removes DE 123 from the message.
<b>NOTE</b>				
<b>Applicable only to Swedish Domestic Authorization Switching Service (SASS).</b>				

## Message Layouts

### Authorization Request Response/0110

---

Data Element ID and Name		Org	Sys	Dst	Comments
124	Member-defined Data	C	•	C	May contain issuer-defined data.
127	Private Data	O	X	CE	Private data for message initiator's use. The Authorization Platform will echo DE 127 from the original Authorization Request/0100, if present.

## Authorization Advice/0120—Acquirer-generated

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTD)	M	•	M	Constant—0120 (Authorization Advice).
- Bit Map, Primary	M	•	M	
1 Bit Map, Secondary	C	•	C	Mandatory if DE 65–DE 128 are present in the message.
2 Primary Account Number (PAN)	M	•	M	Must be the same value as in the original Authorization Request/0100.
3 Processing Code	M	•	M	Must be the same value as in the original Authorization Request/0100.
4 Amount, Transaction	M	•	M	Must be the same value as in the original Authorization Request/0100 unless the message is submitted to complete a pre-authorized transaction.
5 Amount, Settlement	•	X	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
6 Amount, Cardholder Billing	•	X	M	The Authorization Platform provides this data element.
7 Transmission Date and Time	M	•	M	Must be the same value as in the original Authorization Request/0100.
9 Conversion Rate, Settlement	•	X	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
10 Conversion Rate, Cardholder Billing	•	X	M	The Authorization Platform provides this data element.
11 Systems Trace Audit Number (STAN)	M	•	M	Must be the same value as in the original Authorization Request/0100.
12 Time, Local Transaction	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
13 Date, Local Transaction	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
14 Date, Expiration	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
15 Date, Settlement	•	X	M	The Authorization Platform provides this data element.

## Message Layouts

### Authorization Advice/0120—Acquirer-generated

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
16 Date, Conversion	•	X	M	The Authorization Platform provides this data element.
18 Merchant Type	M	•	M	Must be the same value as in the original Authorization Request/0100.
20 Primary Account Number (PAN) Country Code	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
22 Point-of-Service (POS) Entry Mode	M	•	M	Must be the same value as in the original Authorization Request/0100.
23 Card Sequence Number	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
26 Point-of-Service (POS) Personal ID Number (PIN) Capture Code	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
32 Acquiring Institution ID Code	M	•	M	Must be the same value as in the original Authorization Request/0100.
33 Forwarding Institution ID Code	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
35 Track 2 Data	O	•	O	Must be the same value as in the original Authorization Request/0100, if present.
37 Retrieval Reference Number	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
38 Authorization ID Response	C	•	C	Must be the same value as in the original Authorization Request Response/0110 provided by the acquirer, if present.
39 Response Code	M	•	M	Must be either the same value as in the original Authorization Request Response/0110 or a value provided by the acquirer if the acquirer or merchant processed and approved the transaction.
41 Card Acceptor Terminal ID	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
42 Card Acceptor ID Code	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
43 Card Acceptor Name and Location	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
44 Additional Response Data	C	•	C	Must be the same value as in the original Authorization Request Response/0110, if present.
45 Track 1 Data	O	•	O	Must be the same value as in the original Authorization Request/0100, if present.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
48 Additional Data—Private Use	M	X	M	Contains applicable subelement data.
49 Currency Code, Transaction	M	•	M	Must be the same value as in the original Authorization Request/0100.
50 Currency Code, Settlement	•	X	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
51 Currency Code, Cardholder Billing	•	X	M	The Authorization Platform provides this data element.
54 Additional Amounts	C	X	C	Must be the same value as in the original Authorization Request/0100, if present. The Authorization Platform will forward the occurrence of each DE 54 amount type provided by the acquirer in the acquirer's currency and will provide an additional occurrence of each DE 54 amount type in the issuer's currency.
55 Integrated Circuit Card (ICC) System-Related Data	C	•	C	Must be the same value as in the original Authorization Request/0100, if present.
60 Advice Reason Code	M	•	M	DE 60, subfield 1 (Advice Reason Code) must contain the value 190 (APS approved) or value 191 (Acquirer Processing System [APS] Completed Authorization Transaction).
61 Point-of-Service (POS) Data	M	•	M	Must be the same value as in the original Authorization Request/0100.
62 Intermediate Network Facility (INF) Data	O	•	O	Must be the same value as in the original Authorization Request/0100, if present.
63 Network Data	•	X	M	The Authorization Platform provides this data element.
102 Account ID-1	C	•	C	Must be the same value as in the original Authorization Request Response/0110, if present.
103 Account ID-2	C	•	C	Must be the same value as in the original Authorization Request Response/0110, if present.
121 Authorizing Agent ID Code	C	•	C	Must be the MasterCard assigned customer ID of the authorizing entity, if present. Must be the same value as in the original Authorization Request Response/0110.

## Message Layouts

### Authorization Advice/0120—Acquirer-generated

---

Data Element ID and Name		Org	Sys	Dst	Comments
124	Member-defined Data	C	•	C	May contain acquirer-defined data.
127	Private Data	O	X	•	Private data for message initiator's use.

## Authorization Advice/0120—Issuer-generated

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	M	M	•	Constant—0120 (Authorization Advice).
- Bit Map, Primary	M	M	•	
1 Bit Map, Secondary	C	C	•	Mandatory if DE 65–DE 128 are present in the message.
2 Primary Account Number (PAN)	M	M	•	Must be the same value as in the original Authorization Request/0100 message.
3 Processing Code	M	M	•	Must be the same value as in the original Authorization Request/0100 message.
4 Amount, Transaction	M	M	•	Must be the same value as in the original Authorization Request/0100 message or the partial approval amount or purchase only approval amount.
5 Amount, Settlement	M	M	•	Must be the same value as in the original Authorization Request/0100 message or the partial approval amount or purchase only approval amount, if present.
6 Amount, Cardholder Billing	M	M	•	Must be the same value as in the original Authorization Request/0100 message or the partial approval amount or purchase only approval amount.
7 Transmission Date and Time	M	M	•	Must be the same value as in the original Authorization Request/0100 message.
9 Conversion Rate, Settlement	M	M	•	Must be the same value as in the original Authorization Request/0100 message.
10 Conversion Rate, Cardholder Billing	M	M	•	Must be the same value as in the original Authorization Request/0100 message.
11 Systems Trace Audit Number (STAN)	M	M	•	Must be the same value as in the original Authorization Request/0100 message.
12 Time, Local Transaction	C	C	•	Must be the same value as in the original Authorization Request/0100 message, if present.
13 Date, Local Transaction	C	C	•	Must be the same value as in the original Authorization Request/0100 message, if present.
14 Date, Expiration	C	C	•	Must be the same value as in the original Authorization Request/0100 message, if present.

## Message Layouts

### Authorization Advice/0120—Issuer-generated

Data Element ID and Name	Org	Sys	Dst	Comments
15 Date, Settlement	M	M	•	Must be the same value as in the original Authorization Request/0100 message, if present.
16 Date, Conversion	M	M	•	Must be the same value as in the original Authorization Request/0100 message.
18 Merchant Type	M	M	•	Must be the same value as in the original Authorization Request/0100.
20 Primary Account Number (PAN) Country Code	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
22 Point-of-Service (POS) Entry Mode	M	M	•	Must be the same value as in the original Authorization Request/0100.
23 Card Sequence Number	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
26 Point-of-Service (POS) Personal ID Number (PIN) Capture Code	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
32 Acquiring Institution ID Code	M	M	•	Must be the same value as in the original Authorization Request/0100.
33 Forwarding Institution ID Code	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
35 Track 2 Data	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
37 Retrieval Reference Number	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
38 Authorization ID Response	C	C	•	Must be the same value as in the original Authorization Request Response/0110, if present.
39 Response Code	M	M	•	Must be the same value as in the original Authorization Request Response/0110.
41 Card Acceptor Terminal ID	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
42 Card Acceptor ID Code	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
43 Card Acceptor Name and Location	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
44 Additional Response Data	C	C	•	Must be the same value as in the original Authorization Request Response/0110, if present.
45 Track 1 Data	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
48 Additional Data—Private Use	M	M	•	Contains applicable subelement data.
49 Currency Code, Transaction	M	M	•	Must be the same value as in the original Authorization Request/0100.
50 Currency Code, Settlement	M	M	•	Must be the same value as in the original Authorization Request/0100, if present.
51 Currency Code, Cardholder Billing	M	M	•	Must be the same value as in the original Authorization Request/0100.
54 Additional Amounts	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
55 Integrated Circuit Card (ICC) System-Related Data	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
60 Advice Reason Code	M	M	•	Specifies reason for this Authorization Advice/0120. 6500030 = for member-generated transactions
61 Point-of-Service (POS) Data	M	M	•	Must be the same value as in the original Authorization Request/0100.
62 Intermediate Network Facility (INF) Data	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
63 Network Data	M	M	•	Must be the same value as in the original Authorization Request/0100.
102 Account ID-1	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
103 Account ID-2	C	C	•	Must be the same value as in the original Authorization Request/0100, if present.
112 Additional Data—National Use	C	C	•	Contains applicable subelement data.
121 Authorizing Agent ID Code	C	C	•	Must be the issuer customer ID if the issuer authorized the request; otherwise, must be the same value as in the Authorization Advice/0120—System-generated message for MasterCard processed authorizations.

## Message Layouts

### Authorization Advice/0120—System-generated

---

## Authorization Advice/0120—System-generated

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	•	M	M	Constant—0120 (Authorization Advice).
- Bit Map, Primary	•	M	M	
1 Bit Map, Secondary	•	C	C	Mandatory if DE 65–DE 128 are present in the message.
2 Primary Account Number (PAN)	•	M	M	Must be the same value as in the original Authorization Request/0100.
3 Processing Code	•	M	M	Must be the same value as in the original Authorization Request/0100.
4 Amount, Transaction	•	M	M	Must be the same value as in the original Authorization Request/0100.
5 Amount, Settlement	•	C	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
6 Amount, Cardholder Billing	•	M	M	The Authorization Platform provides this data element.
7 Transmission Date and Time	•	M	M	Must be the same value as in the original Authorization Request/0100.
9 Conversion Rate, Settlement	•	C	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
10 Conversion Rate, Cardholder Billing	•	M	M	The Authorization Platform provides this data element.
11 Systems Trace Audit Number (STAN)	•	M	M	Must be the same value as in the original Authorization Request/0100.
12 Time, Local Transaction	•	C	C	Must be the same value as in the original Authorization Request/0100, if present.
13 Date, Local Transaction	•	C	C	Must be the same value as in the original Authorization Request/0100, if present.
14 Date, Expiration	•	C	C	Must be the same value as in the original Authorization Request/0100, if present.
15 Date, Settlement	•	M	M	The Authorization Platform provides this data element.
16 Date, Conversion	•	M	M	The Authorization Platform provides this data element.

<b>Data Element ID and Name</b>		<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
18 Merchant Type	•	M	M		Must be the same value as in the original Authorization Request/0100.
20 Primary Account Number (PAN) Country Code	•	C	C		Must be the same value as in the original Authorization Request/0100, if present.
22 Point-of-Service (POS) Entry Mode	•	M	M		Must be the same value as in the original Authorization Request/0100.
23 Card Sequence Number	•	C	C		Must be the same value as in the original Authorization Request/0100, if present.
26 Point-of-Service (POS) Personal ID Number (PIN) Capture Code	•	C	C		Must be the same value as in the original Authorization Request/0100, if present.
28 Amount, Transaction Fee	•	C	C		Must contain the same value as the original Authorization Request/0100 message, if present.
32 Acquiring Institution ID Code	•	M	M		Must be the same value as in the original Authorization Request/0100.
33 Forwarding Institution ID Code	•	C	C		Must be the same value as in the original Authorization Request/0100, if present.
35 Track 2 Data	•	C	C		Must be the same value as in the original Authorization Request/0100, if present.
37 Retrieval Reference Number	•	C	C		Must be the same value as in the original Authorization Request/0100, if present.
38 Authorization ID Response	•	C	C		Must be the same value as in the original Authorization Request Response/0110, if present.
39 Response Code	•	M	M		Must be the same value as in the original Authorization Request Response/0110.
41 Card Acceptor Terminal ID	•	C	C		Must be the same value as in the original Authorization Request/0100, if present.
42 Card Acceptor ID Code	•	C	C		Must be the same value as in the original Authorization Request/0100, if present.
43 Card Acceptor Name and Location	•	C	C		Must be the same value as in the original Authorization Request/0100, if present.
44 Additional Response Data	•	C	C		Must be the same value as in the original Authorization Request Response/0110, if present.
45 Track 1 Data	•	C	C		Must be the same value as in the original Authorization Request/0100, if present.
48 Additional Data—Private Use	•	M	M		Contains applicable subelement data.

## Message Layouts

### Authorization Advice/0120—System-generated

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
49 Currency Code, Transaction	•	M	M	Must be the same value as in the original Authorization Request/0100.
50 Currency Code, Settlement	•	C	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
51 Currency Code, Cardholder Billing	•	M	M	The Authorization Platform provides this data element.
54 Additional Amounts	•	C	C	Must be the same value as in the original Authorization Request/0100, if present.
55 Integrated Circuit Card (ICC) System-Related Data	•	C	C	Must be the same value as in the original Authorization Request/0100, if present.
60 Advice Reason Code	•	M	M	Specifies reason for this Authorization Advice/0120.
61 Point-of-Service (POS) Data	•	M	M	Must be the same value as in the original Authorization Request/0100.
62 Intermediate Network Facility (INF) Data	•	C	C	Must be the same value as in the original Authorization Request/0100, if present.
63 Banknet Data	•	M	M	Must be the same value as in the original Authorization Request/0100. The Authorization Platform provides this data element, if required.
102 Account ID-1	•	C	C	Must be the same value as in the original Authorization Request Response/0110, if present.
103 Account ID-2	•	C	C	Must be the same value as in the original Authorization Request Response/0110, if present.
121 Authorizing Agent ID Code	•	C	C	Must be the same value as in the original Authorization Request Response/0110, if present.
124 Member-defined Data	•	C	C	Must be the same value as in the original Authorization Request/0100, if present.

## Authorization Advice Response/0130—Issuer-generated (Responding to a System-generated 0120 from SAF)

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	M	M	•	Constant—0130 (Authorization Advice Response).
- Bit Map, Primary	M	M	•	
1 Bit Map, Secondary	C	C	•	Must be the same value as in the Authorization Advice/0120, if present.
2 Primary Account Number (PAN)	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
3 Processing Code	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
4 Amount, Transaction	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
5 Amount, Settlement	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
6 Amount, Cardholder Billing	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
7 Transmission Date and Time	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
9 Conversion Rate, Settlement	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
10 Conversion Rate, Cardholder Billing	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
11 Systems Trace Audit Number (STAN)	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
15 Date, Settlement	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
16 Date, Conversion	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
20 Primary Account Number (PAN) Country Code	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
23 Card Sequence Number	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
28 Amount, Transaction Fee	CE	CE	•	Must be the same value as in the original Authorization Advice/0120 message, if present.

## Message Layouts

### Authorization Advice Response/0130—Issuer-generated (Responding to a System-generated 0120 from SAF)

Data Element ID and Name		Org	Sys	Dst	Comments
32	Acquiring Institution ID Code	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
33	Forwarding Institution ID Code	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
37	Retrieval Reference Number	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
39	Response Code	M	M	•	For more detail, refer to the data element definition for DE 39.
41	Card Acceptor Terminal ID	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
44	Additional Response Data	C	C	•	May contain additional response information for certain error conditions in original Authorization Advice/0120.
49	Currency Code, Transaction	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
50	Currency Code, Settlement	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
51	Currency Code, Cardholder Billing	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
62	Intermediate Network Facility (INF) Data	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
63	Network Data	ME	ME	•	Must be the same value as in the Authorization Advice/0120.

## Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
- Message Type Identifier (MTI)		M	•	M	Constant—0130 (Authorization Advice Response).
- Bit Map, Primary		M	•	M	
1	Bit Map, Secondary	C	•	C	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
2	Primary Account Number (PAN)	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
3	Processing Code	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
4	Amount, Transaction	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
5	Amount, Settlement	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
6	Amount, Cardholder Billing	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
7	Transmission Date and Time	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
9	Conversion Rate, Settlement	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
10	Conversion Rate, Cardholder Billing	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
11	Systems Trace Audit Number (STAN)	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.

## Message Layouts

### Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)

Data Element ID and Name	Org	Sys	Dst	Comments
15 Date, Settlement	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
16 Date, Conversion	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
20 Primary Account Number (PAN) Country Code	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
23 Card Sequence Number	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
32 Acquiring Institution ID Code	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
33 Forwarding Institution ID Code	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
37 Retrieval Reference Number	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
39 Response Code	M	•	M	Response Code for the Authorization Advice Response/0130. For values, refer to DE 39 Response Code
41 Card Acceptor Terminal ID	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
44 Additional Response Data	CE	•	CE	May contain additional response information for certain error conditions in original Authorization Advice/0120—Acquirer-generated, if present.
48 Additional Data—Private Use	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
49 Currency Code, Transaction	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.

## Message Layouts

### Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)

Data Element ID and Name	Org	Sys	Dst	Comments
50 Currency Code, Settlement	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
51 Currency Code, Cardholder Billing	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
62 Intermediate Network Facility (INF) Data	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
63 Network Data	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
127 Private Data	CE	X	CE	Private data for message originator's use. The Authorization Platform will echo in DE 127 from the original Authorization Advice/0120—Acquirer-generated, if present.

**Message Layouts****Authorization Advice Response/0130—System-generated (Responding to an Acquirer-generated 0120)****Authorization Advice Response/0130—System-generated (Responding to an Acquirer-generated 0120)**

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	M	M	•	Constant—0130 (Authorization Advice Response).
- Bit Map, Primary	M	M	•	
1 Bit Map, Secondary	C	C	•	Must be the same value as in the Authorization Advice/0120, if present.
2 Primary Account Number (PAN)	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
3 Processing Code	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
4 Amount, Transaction	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
5 Amount, Settlement	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
6 Amount, Cardholder Billing	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
7 Transmission Date and Time	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
9 Conversion Rate, Settlement	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
10 Conversion Rate, Cardholder Billing	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
11 Systems Trace Audit Number (STAN)	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
15 Date, Settlement	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
16 Date, Conversion	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
20 Primary Account Number (PAN) Country Code	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
23 Card Sequence Number	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
28 Amount, Transaction Fee	CE	CE	•	Must be the same value as in the original Authorization Advice/0120 message, if present.

**Authorization Advice Response/0130—System-generated (Responding to an Acquirer-generated 0120)**

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
32 Acquiring Institution ID Code	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
33 Forwarding Institution ID Code	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
37 Retrieval Reference Number	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
39 Response Code	M	M	•	For more detail, refer to the data element definition for DE 39.
41 Card Acceptor Terminal ID	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
44 Additional Response Data	C	C	•	May contain additional response information for certain error conditions in original Authorization Advice/0120.
48 Additional Data—Private Use	ME	•	ME	Must be the same value as in the Authorization Advice/0120—Acquirer-generated.
49 Currency Code, Transaction	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
50 Currency Code, Settlement	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
51 Currency Code, Cardholder Billing	ME	ME	•	Must be the same value as in the Authorization Advice/0120.
62 Intermediate Network Facility (INF) Data	CE	CE	•	Must be the same value as in the Authorization Advice/0120, if present.
63 Network Data	ME	ME	•	Must be the same value as in the Authorization Advice/0120.

## Message Layouts

### Authorization Advice Response/0130—System-generated (Responding to an Issuer-generated 0120)

---

## Authorization Advice Response/0130—System-generated (Responding to an Issuer-generated 0120)

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	M	M	Constant—0130 (Authorization Advice Response).
-	Bit Map, Primary	•	M	M	
1	Bit Map, Secondary	•	C	C	Must be the same value as in the Authorization Advice/0120—Issuer-generated, if present.
2	Primary Account Number (PAN)	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.
3	Processing Code	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.
4	Amount, Transaction	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.
5	Amount, Settlement	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.
6	Amount, Cardholder Billing	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.
7	Transmission Date and Time	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.
9	Conversion Rate, Settlement	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.
10	Conversion Rate, Cardholder Billing	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.
11	Systems Trace Audit Number (STAN)	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.
15	Date, Settlement	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.

## Authorization Advice Response/0130—System-generated (Responding to an Issuer-generated 0120)

Data Element ID and Name		Org	Sys	Dst	Comments
16 Date, Conversion	•	ME	ME		Must be the same value as in the Authorization Advice/0120—Issuer-generated.
20 Primary Account Number (PAN) Country Code	•	CE	CE		Must be the same value as in the Authorization Advice/0120—Issuer-generated, if present.
23 Card Sequence Number	•	CE	CE		Must be the same value as in the Authorization Advice/0120—Issuer-generated, if present.
32 Acquiring Institution ID Code	•	ME	ME		Must be the same value as in the Authorization Advice/0120—Issuer-generated.
33 Forwarding Institution ID Code	•	CE	CE		Must be the same value as in the Authorization Advice/0120—Issuer-generated, if present.
37 Retrieval Reference Number	•	CE	CE		Must be the same value as in the Authorization Advice/0120—Issuer-generated, if present.
39 Response Code	•	M	M		Response Code for this Authorization Advice Response/0130.
41 Card Acceptor Terminal ID	•	CE	CE		Must be the same value as in the Authorization Advice/0120—Issuer-generated, if present.
44 Additional Response Data	•	X	C		May contain additional response information for certain error conditions in original Authorization Advice/0120—Issuer-generated.
49 Currency Code, Transaction	•	ME	ME		Must be the same value as in the Authorization Advice/0120—Issuer-generated.
50 Currency Code, Settlement	•	ME	ME		Must be the same value as in the Authorization Advice/0120—Issuer-generated.
51 Currency Code, Cardholder Billing	•	ME	ME		Must be the same value as in the Authorization Advice/0120—Issuer-generated.
62 Intermediate Network Facility (INF) Data	•	CE	CE		Must be the same value as in the Authorization Advice/0120—Issuer-generated, if present.
63 Network Data	•	X	M		The Authorization Platform provides this data element, if required.

## Message Layouts

### Authorization Response Acknowledgement/0180

---

## Authorization Response Acknowledgement/0180

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
- Message Type Identifier (MTI)		M	M	•	Constant—0180 (Authorization Response Acknowledgement).
- Bit Map, Primary		M	M	•	
1	Bit Map, Secondary	C	C	•	Mandatory if DE 65–DE 128 are present in the message.
7	Transmission Date and Time	ME	ME	•	Must be the same value as in the original Authorization Request Response/0110.
11	Systems Trace Audit Number (STAN)	ME	ME	•	Must be the same value as in the original Authorization Request Response/0110.
39	Response Code	M	M	•	Must be 00 to indicate positive “Response Acknowledgement.”
63	Network Data	ME	ME	•	Must be the same value as in the original Authorization Request Response/0110.
127	Private Data	CE	CE	•	Private data for message initiator’s use.

## Authorization Response Negative Acknowledgement/0190

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	•	M	M	Constant—0190 (Authorization Response Negative Acknowledgement).
- Bit Map, Primary	•	M	M	
1 Bit Map, Secondary	•	C	C	Required data element if DE 65–DE 128 are present in the message.
7 Transmission Date and Time	•	ME	ME	Must be the same value as in the original Authorization Request Response/0110 or Reversal Request Response/0410.
11 Systems Trace Audit Number (STAN)	•	ME	ME	Must be the same value as in the original Authorization Request Response/0110 or Reversal Request Response/0410.
39 Response Code	•	M	M	Indicates specific reason for this “Negative Response Acknowledgement.”
44 Additional Response Data	•	C	C	For a listing of values, refer to this data element definition in the “Data Element Definitions” chapter.
63 Network Data	•	ME	ME	Must be the same value as in the original Authorization Request Response/0110 or Reversal Request Response/0410.
127 Private Data	•	X	CE	Must be the same value as in the original Authorization Request Response/0110 or Reversal Request Response/0410

## Message Layouts

### Issuer File Update Request/0302

---

## Issuer File Update Request/0302

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
- Message Type Identifier (MTI)		M	M	•	Constant—0302 (Issuer File Update Request).
- Bit Map, Primary		M	M	•	Mandatory.
1	Bit Map, Secondary	M	M	•	Mandatory.
2	Primary Account Number (PAN)	C	C	•	May contain PAN information if required for this Issuer File Update Request/0302.
7	Transmission Date and Time	M	M	•	Transaction time stamp; UTC date and time that this transaction was entered into interchange.
11	Systems Trace Audit Number (STAN)	M	M	•	Transaction trace number; must be unique value for transaction initiator within each UTC day.
33	Forwarding Institution ID Code	M	M	•	MasterCard-assigned customer ID code. Identifies the institution submitting this file maintenance request.
63	Network Data	•	M	•	Authorization Platform transaction ID code; MasterCard provides this data as a unique identifier for this Issuer File Update Request/0302.
91	Issuer File Update Code	M	M	•	Issuer File Update function code.
96	Message Security Code	M	M	•	Issuer File Update “password” or security code used to authenticate Issuer File Update permissions. Data must be provided in EBCDIC hexadecimal format.
101	File Name	M	M	•	Name of file the issuer is maintaining or accessing.
120	Record Data	C	C	•	Contains the specific Issuer File Update detail record data.
127	Private Data	O	X	•	Private use data element, available for message initiator's optional use.

## Issuer File Update Request Response/0312

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>		<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
-	Message Type Identifier (MTI)	•	M	M	Constant—0312 (Issuer File Update Request Response).
-	Bit Map, Primary	•	M	M	Mandatory.
1	Bit Map, Secondary	•	M	M	Mandatory.
2	Primary Account Number (PAN)	•	CE	CE	Must be the same value as in the original Issuer File Update Request/0302, if present.
7	Transmission Date and Time	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302.
11	Systems Trace Audit Number (STAN)	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302.
33	Forwarding Institution ID Code	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302, if present.
39	Response Code	•	M	M	Indicates disposition of Issuer File Update Request/0302.
44	Additional Response Data	•	C	C	May contain additional response information, based on DE 39.
63	Network Data	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302.
91	Issuer File Update Code	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302.
96	Message Security Code	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302.
101	File Name	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302.
120	Record Data	•	C	C	This data element is used to return file inquiry and rejects records associated with reject responses. Refer to the data element definition for DE 120.
122	Additional Record Data	•	C	C	This data element is used to return additional data resulting from a file inquiry.
127	Private Data	•	X	CE	Must be the same value as in the original Issuer File Update Request/0302, if present.

## Message Layouts

### Reversal Request/0400

---

## Reversal Request/0400

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	M	•	M	Constant—0400 (Reversal Request).
- Bit Map, Primary	M	•	M	Mandatory.
1 Bit Map, Secondary	M	•	M	Mandatory.
2 Primary Account Number (PAN)	M	•	M	Must be the same value as in the original Authorization Request/0100 message.
3 Processing Code	M	•	M	Must be the same value as in the original Authorization Request/0100 message.
4 Amount, Transaction	M	•	M	Must be the same value as in the original Authorization Request/0100 message. On a partial approval or purchase only approval, must be the same as the Authorization Request Response/0110 message. Must be a value other than all zeros.
5 Amount, Settlement	•	X	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements. This value may be different from the Authorization Request/0100 message if the currency conversion rate used by the Authorization Platform has changed between the time the original Authorization Request/0100 message was processed and the time the Reversal Request/0400 message is processed by the Authorization Platform.
6 Amount, Cardholder Billing	•	X	M	The Authorization Platform provides this data element. This value may be different from the Authorization Request/0100 message if the currency conversion rate used by the Authorization Platform has changed between the time the original Authorization Request/0100 message was processed and the time the Reversal Request/0400 message is processed by the Authorization Platform.
7 Transmission Date and Time	M	•	M	Transaction time stamp; UTC date and time that this transaction was entered into interchange.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
9 Conversion Rate, Settlement	•	X	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
10 Conversion Rate, Cardholder Billing	•	X	M	The Authorization Platform provides this data element. This value may be different from the Authorization Request/0100 message if the currency conversion rate used by the Authorization Platform has changed between the time the original Authorization Request/0100 message was processed and the time the Reversal Request/0400 message is processed by the Authorization Platform.
11 Systems Trace Audit Number (STAN)	M	•	M	Transaction trace number; must be unique value for transaction initiator within each UTC day.
12 Time, Local Transaction	C	•	C	Must be the same value as in the original Authorization Request/0100 message, if present.
13 Date, Local Transaction	C	•	C	Must be the same value as in the original Authorization Request/0100 message, if present.
14 Date, Expiration	C	•	C	Must be the same value as in the original Authorization Request/0100 message, if present.
15 Date, Settlement	•	X	M	The Authorization Platform provides this data element.
16 Date, Conversion	•	X	M	The Authorization Platform provides this data element.
18 Merchant Type	M	•	M	Must be the same value as in the original Authorization Request/0100 message.
20 Primary Account Number (PAN) Country Code	C	•	C	Must be the same value as in the original Authorization Request/0100 message, if present.
22 Point-of-Service (POS) Entry Mode	M	•	M	Must be the same value as in the original Authorization Request/0100 message.
23 Card Sequence Number	C	•	C	Must be the same value as in the original Authorization Request/0100 message, if present.

## Message Layouts

### Reversal Request/0400

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
28 Amount, Transaction Fee	C	X	C	Must be the same value as in the original Authorization Request/0100 message, if present.
32 Acquiring Institution ID Code	M	•	M	Must be the same value as in the original Authorization Request/0100 message.
33 Forwarding Institution ID Code	C	•	C	Must be the same value as in the original Authorization Request/0100 message, if present.
37 Retrieval Reference Number	C	•	C	Must be the same value as in the original Authorization Request/0100 message, if present.
38 Authorization ID Response	C	•	C	Must be the same value as in the original Authorization Request Response/0110 message if present.
39 Response Code	M	•	M	Must be the same value as in the original Authorization Request Response/0110 message or it may contain value 06, 17, 32, or 68.
41 Card Acceptor Terminal ID	C	•	C	Must be the same value as in the original Authorization Request/0100 message, if present.
42 Card Acceptor ID Code	C	•	C	Must be the same value as in the original Authorization Request/0100 message, if present.
43 Card Acceptor Name/Location	C	•	C	Must be the same value as in the original Authorization Request/0100 message, if present.
48 Additional Data—Private Use	M	X	M	Must contain the transaction category code (TCC) from the original Authorization Request/0100. Subelement 58 (ATM Additional Data) and subelement 77 (Payment Transaction Type Indicator) may be present based on the usage condition defined for each of these subelements in the Data Element Definitions.

Data Element ID and Name	Org	Sys	Dst	Comments
				<p>May also contain the following DE 48 subelements for Visa issuers:</p> <ul style="list-style-type: none"> <li>• 36 (Visa Defined Data [Visa Only])</li> <li>• 42 (Electronic Commerce Indicators)</li> <li>• 43 (Universal Cardholder Authentication Field [UCAF])</li> <li>• 44 (Visa 3-D Secure Electronic Commerce Transaction Identifier [XID]—Visa Only)</li> <li>• 90 (Custom Payment Service Request—Visa Only)</li> <li>• 91 (Custom Payment Service Request Transaction ID—Visa Only)</li> <li>• 94 (Commercial Card Inquiry Request—Visa Only)</li> <li>• 96 (Visa Market-Specific Data Identifier—Visa Only)</li> </ul>
<b>NOTE</b>				
				<p><b>DE 48 subelements not specifically referenced in the Reversal Request/0400 message layout but submitted by an acquirer in the Reversal Request/0400 message will not be forwarded by the Authorization Platform to the issuer or returned to the acquirer.</b></p>
49 Currency Code, Transaction	M	•	M	Must be the same value as in the original Authorization Request/0100 message.
50 Currency Code, Settlement	•	X	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
51 Currency Code, Cardholder Billing	•	X	M	The Authorization Platform provides this data element.
54 Additional Amounts	C	X	C	Must be the same value as in the original Authorization Request/0100 message. This data element will only be passed to the issuer when DE 54, subfield 2, contains the value 40. The Authorization Platform will forward occurrences of this amount type in both the acquirer's currency and the issuer's currency.

## Message Layouts

### Reversal Request/0400

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
61 Point-of-Service (POS) Data	M	•	M	Must be the same value as in the original Authorization Request/0100 message.
62 Intermediate Network Facility (INF) Data	O	•	O	If present in an original Authorization Request/0100 message, may be present in subsequent Reversal Request/0400.
63 Network Data	•	X	M	The Authorization Platform provides this data element.
90 Original Data Elements	M	•	M	Contains certain data elements from the original Authorization Request/0100 message.
95 Replacement Amounts	C	X	C	If this data element is provided by an acquirer in a <b>full reversal</b> message, it must contain all zeros to indicate a full reversal. If this data element is provided by an acquirer in a <b>partial reversal</b> message, it must contain a value other than all zeros to indicate a partial reversal.
112 Additional Data—National Use	C	•	C	Contains applicable subelement data.
124 Member-defined Data	O	•	C	Member-defined data element, available for message initiator and recipient optional use.
127 Private Data	O	X	•	Private use data element, available for message initiator's optional use.

## Reversal Request Response/0410

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>		<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)		M	•	M	Constant—0410 (Reversal Request Response)
- Bit Map, Primary		M	•	M	Mandatory
1	Bit Map, Secondary	M	•	M	Mandatory
2	Primary Account Number (PAN)	ME	•	ME	Must be the same value as in the original Reversal Request/0400 message.
3	Processing Code	ME	•	ME	Must be the same value as in the original Reversal Request/0400 message.
4	Amount, Transaction	ME	•	ME	Must be the same value as in the original Reversal Request/0400 message.
5	Amount, Settlement	CE	X	C	Must be the same value as in the original Reversal Request/0400 message, if present. The Authorization Platform provides this data element if the acquirer chooses to receive settlement amount-related data elements. <sup>3</sup>
6	Amount, Cardholder Billing	C	•	C	Must be the same value as in the original Reversal Request/0400 message. <sup>3</sup>
7	Transmission Date and Time	ME	•	ME	Must be the same value as in the original Reversal Request/0400 message.
9	Conversion Rate, Settlement	CE	X	C	Must be the same value as in the original Reversal Request/0400 message, if present. The Authorization Platform provides this data element if the acquirer chooses to receive settlement amount-related data elements. <sup>3</sup>
10	Conversion Rate, Cardholder Billing	C	X	C	Must be the same value as in the original Reversal Request/0400 message. <sup>3</sup>

---

3. This data will be present, as defined, except when the Authorization Platform has declined an Authorization Request/0100 message and was unable to complete currency conversion processing.

## Message Layouts

### Reversal Request Response/0410

Data Element ID and Name	Org	Sys	Dst	Comments
11 Systems Trace Audit Number	ME	•	ME	Must be the same value as in the original Reversal Request/0400 message.
15 Date, Settlement	ME	X	M	Must be the same value as in the original Reversal Request/0400 message.
16 Date, Conversion	C	X	C	Must be the same value as in the original Reversal Request/0400 message. <sup>3</sup>
20 Primary Account Number (PAN) Country Code	CE	•	CE	Must be the same value as in the original Reversal Request/0400 message, if present.
28 Amount, Transaction Fee	CE	X	CE	Must contain the same value as in the original Reversal Request/0400 message, if present.
32 Acquiring Institution ID Code	ME	•	ME	Must be the same value as in the original Reversal Request/0400 message.
33 Forwarding Institution ID Code	CE	•	CE	Must be the same value as in the original Reversal Request/0400 message, if present.
37 Retrieval Reference Number	CE	•	CE	Must be the same value as in the original Reversal Request/0400 message, if present.
39 Response Code	M	•	M	Must be present in the Reversal Request Response/0410 message. Defines the disposition of a previous message or an action taken as a result of receipt of a previous message.
41 Card Acceptor Terminal ID	CE	•	CE	Must be the same value as in the original Reversal Request/0400 message, if present.
44 Additional Response Data	C	•	C	Contains additional response data.
48 Additional Data—Private Use	ME	•	ME	Must be the same value as in the original Reversal Request/0400 message.
49 Currency Code, Transaction	ME	•	ME	Must be the same value as in the original Reversal Request/0400 message.

**Message Layouts**  
**Reversal Request Response/0410**

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
50 Currency Code, Settlement	CE	X	C	Must be the same value as in the original Reversal Request/0400 message, if present. The Authorization Platform provides this data element if the acquirer chooses to receive settlement amount-related data elements. <sup>3</sup>
51 Currency Code, Cardholder Billing	C	•	C	Must be the same value as in the original Reversal Request/0400 message. <sup>3</sup>
62 Intermediate Network Facility (INF) Data	CE	•	CE	Must be the same value as in the original Reversal Request/0400 message, if present.
63 Network Data	ME	X	M	Must be the same value as in the original Reversal Request/0400 message.
90 Original Data Elements	ME	•	ME	Must be the same value as in the original Reversal Request/0400 message.
95 Replacement Amounts	CE	X	C	Must be the same value as in the original Reversal Request/0400 message, if present.
112 Additional Data—National Use	C	•	C	Contains applicable subelement data.
121 Authorizing Agent ID Code	C	•	C	Contains the MasterCard member ID of an alternate authorizer (Stand-In), that performed Dual Message System processing on-behalf of an issuer or issuer's primary authorizer.
124 Member-defined Data	O	•	C	May contain member-defined data.
127 Private Data	O	X	CE	Private data for message initiator's use.

## Message Layouts

### Reversal Advice/0420

---

## Reversal Advice/0420

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	•	M	M	Constant—0420 (Reversal Advice).
- Bit Map, Primary	•	M	M	Mandatory.
1 Bit Map, Secondary	•	M	M	Mandatory.
2 Primary Account Number (PAN)	•	M	M	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message.
3 Processing Code	•	M	M	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message.
4 Amount, Transaction	•	M	M	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 (except for a partial approval or purchase only approval). For a partial approval or purchase only approval, must be the same value as the Authorization Request Response/0110.
5 Amount, Settlement	•	C	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
6 Amount, Cardholder Billing	•	M	M	The Authorization Platform provides this data element.
7 Transmission Date and Time	•	M	M	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message.
9 Conversion Rate, Settlement	•	C	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
10 Conversion Rate, Cardholder Billing	•	M	M	The Authorization Platform provides this data element.
11 Systems Trace Audit Number (STAN)	•	M	M	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message.
13 Date, Local Transaction	•	C	C	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message, if present.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
15 Date, Settlement	•	M	M	The Authorization Platform provides this data element.
16 Date, Conversion	•	M	M	The Authorization Platform provides this data element.
20 Primary Account Number (PAN) Country Code	•	C	C	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message, if present.
22 Point-of-Service (POS) Entry Mode	•	M	M	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message.
28 Amount, Transaction Fee	•	C	C	Must contain the same value as in the original Authorization Request/0100 or Reversal Request/0400 message, if present.
32 Acquiring Institution ID Code	•	M	M	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message.
33 Forwarding Institution ID Code	•	C	C	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message, if present.
37 Retrieval Reference Number	•	C	C	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message, if present.
38 Authorization ID Response	•	C	C	Must be the same value as in the original Authorization Request Response/0110 or Reversal Request Response/0410 message, if present.
39 Response Code	•	C	C	Must be the same value as in the original Authorization Request Response/0110. Otherwise, value 82, if no Authorization Request Response/0110 or Reversal Request Response/0410 is received. When provided in response to Reversal Request/0400 messages processed by the Authorization Platform on behalf of the issuer, will contain the value from the original Reversal Request/0400 message.

## Message Layouts

### Reversal Advice/0420

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
43 Card Acceptor Name/Location	•	C	C	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message, if present.
48 Additional Data—Private Use	•	M	M	Must contain the transaction category code (TCC) from the original Authorization Request/0100 or Reversal Request/0400 message.
49 Currency Code, Transaction	•	M	M	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message.
50 Currency Code, Settlement	•	C	C	The Authorization Platform provides this data element if the issuer chooses to receive settlement amount-related data elements.
51 Currency Code, Cardholder Billing	•	M	M	The Authorization Platform provides this data element.
54 Additional Amounts	•	C	C	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message or the original Authorization Request Response/0110 or Reversal Request Response/0410 message.
60 Advice Reason Code	•	M	M	Indicates exact purpose of the Reversal Advice/0420.
62 Intermediate Network Facility (INF) Data	•	C	C	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message, if present.
63 Network Data	•	M	M	The Authorization Platform provides this data element.
90 Original Data Elements	•	M	M	Must be present when the Authorization Platform reverses a Reversal Request/0400 message.
95 Replacement Amounts	•	C	C	If this data element is provided by the acquirer in a partial reversal message, it must be included in the subsequent Reversal Advice/0420 message.

Data Element ID and Name	Org	Sys	Dst	Comments
121 Authorizing Agent ID Code	•	C	C	Must be the same value as in the original Authorization Request Response/0110 or Reversal Request Response/0410 message, if present.
127 Private Data	•	X	CE	Must be the same value as in the original Authorization Request/0100 or Reversal Request/0400 message, if present.

## Message Layouts

### Reversal Advice Response/0430

---

## Reversal Advice Response/0430

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	M	•	Constant—0430 (Reversal Advice Response)
-	Bit Map, Primary	M	M	•	Mandatory.
1	Bit Map, Secondary	M	M	•	Mandatory.
2	Primary Account Number (PAN)	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
3	Processing Code	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
4	Amount, Transaction	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
5	Amount, Settlement	CE	CE	•	Must be the same value as in the original Reversal Advice/0420 message, if present.
6	Amount, Cardholder Billing	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
7	Transmission Date and Time	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
9	Conversion Rate, Settlement	CE	CE	•	Must be the same value as in the original Reversal Advice/0420 message, if present.
10	Conversion Rate, Cardholder Billing	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
11	Systems Trace Audit Number	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
15	Date, Settlement	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
16	Date, Conversion	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.

**Message Layouts**  
**Reversal Advice Response/0430**

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
20 Primary Account Number (PAN) Country Code	CE	CE	•	Must be the same value as in the original Reversal Advice/0420 message, if present.
28 Amount, Transaction Fee	CE	CE	•	Must be the same value as in the original Reversal Advice/0420 message, if present.
32 Acquiring Institution ID Code	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
33 Forwarding Institution ID Code	CE	CE	•	Must be the same value as in the original Reversal Advice/0420 message, if present.
37 Retrieval Reference Number	CE	CE	•	Must be the same value as in the original Reversal Advice/0420 message, if present.
39 Response Code	M	M	•	Must be present in the Reversal Advice Response/0430 message.
44 Additional Response Data	C	C	•	Contains additional response data.
49 Currency Code, Transaction	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
50 Currency Code, Settlement	CE	CE	•	Must be the same value as in the original Reversal Advice/0420 message, if present.
51 Currency Code, Cardholder Billing	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
62 Intermediate Network Facility (INF) Data	CE	CE	•	Must be the same value as in the original Reversal Advice/0420 message, if present.
63 Network Data	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
90 Original Data Elements	ME	ME	•	Must be the same value as in the original Reversal Advice/0420 message.
95 Replacement Amounts	CE	CE	•	Must be the same value as in the original Reversal Advice/0420 message, if present.
127 Private Data	CE	CE	•	Must be the same value as in the original Reversal Advice/0420 message, if present.

## Message Layouts

### Administrative Request/0600

---

## Administrative Request/0600

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	M	•	M	Constant—0600 (Administrative Request).
- Bit Map, Primary	M	•	M	Mandatory.
1 Bit Map, Secondary	M	•	M	Mandatory.
2 Primary Account Number (PAN)	M	•	M	Identifies the receiver of the Administrative Request/0600.
7 Transmission Date and Time	M	•	M	Transaction time stamp; UTC date and time that this transaction was entered into the interchange.
11 Systems Trace Audit Number (STAN)	M	•	M	Transaction trace number; must be a unique value for the message initiator within each UTC day
32 Acquiring Institution ID Code	M	•	M	Identifies the acquirer of the Administrative Request/0600.
33 Forwarding Institution ID Code	C	•	C	Identifies the acquirer processor of the Administrative Request/0600 message, if present.
41 Card Acceptor Terminal ID	O	•	O	Identifies the merchant terminal ID, if present.
42 Card Acceptor ID Code	O	•	O	Identifies the merchant ID, if present.
43 Card Acceptor Name and Location	O	•	O	Contains the merchant name and address, if present.
60 Advice Reason Code	M	•	M	Indicates specific type of message.
62 Intermediate Network Facility (INF) Data	O	•	O	May contain message initiator network trace information.
63 Network Data		•	X	Contains the Banknet Reference Number that the Authorization Platform provides as a unique transaction ID.
113 Reserved for National Use	C	•	C	Contains customer information.
114 Reserved for National Use	C	•	C	Contains customer information.
115 Reserved for National Use	C	•	C	Contains customer information.
116 Reserved for National Use	C	•	C	Contains customer information.
117 Reserved for National Use	C	•	C	Contains customer information.

**Message Layouts**  
**Administrative Request/0600**

---

<b>Data Element ID and Name</b>		<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
118	Reserved for National Use	C	•	C	Contains customer information.
119	Reserved for National Use	C	•	C	Contains customer information.
127	Private Data	O	X	•	May contain message initiator information.

## Message Layouts

### Administrative Request Response/0610

---

## Administrative Request Response/0610

Following is the list of the data elements applicable to this message.

Date Element ID and Name	Org	Sys	Dst	Comments
- Message Type Identifier (MTI)	M	•	M	Constant—0610 (Administrative Request Response).
- Bit Map, Primary	M	•	M	Mandatory.
1 Bit Map, Secondary	M	•	M	Mandatory.
2 Primary Account Number (PAN)	ME	•	ME	Must be the same value as in the original Administrative Request/0600.
7 Transmission Date and Time	ME	•	ME	Must be the same value as in the original Administrative Request/0600.
11 Systems Trace Audit Number (STAN)	ME	•	ME	Must be the same value as in the original Administrative Request/0600.
32 Acquiring Institution ID Code	ME	•	ME	Must be the same value as in the original Administrative Request/0600.
33 Forwarding Institution ID Code	CE	•	CE	Must be the same value as in the original Administrative Request/0600, if present.
39 Response Code	M	•	M	Indicates the disposition of the original Administrative Request/0600.
41 Card Acceptor Terminal ID	CE	•	CE	Must be the same value as in the original Administrative Request/0600, if present.
42 Card Acceptor ID Code	CE	•	CE	Must be the same value from the original Administrative Request/0600, if present.
43 Card Acceptor Name/Location	CE	•	CE	Must be the same value from the original Administrative Request/0600, if present.
44 Additional Response Data	C	•	C	May contain additional error code information.
60 Advice Reason Code	ME	•	ME	Must be the same value from the original Administrative Request/0600.
62 Intermediate Network Facility (INF) Data	CE	•	CE	Must be the same value as in the original Administrative Request/0600, if present.
63 Network Data	ME	•	ME	Must be the same value as in the original Administrative Request/0600.
113 Reserved for National Use	C	•	C	Contains customer information.
114 Reserved for National Use	C	•	C	Contains customer information.
115 Reserved for National Use	C	•	C	Contains customer information.

Date Element ID and Name	Org	Sys	Dst	Comments
116 Reserved for National Use	C	•	C	Contains customer information.
117 Reserved for National Use	C	•	C	Contains customer information.
118 Reserved for National Use	C	•	C	Contains customer information.
119 Reserved for National Use	C	•	C	Contains customer information.
127 Private Data	•	X	CE	May contain message initiator information.

## Message Layouts

### Administrative Advice/0620—System-generated

---

## Administrative Advice/0620—System-generated

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	•	M	M	Constant—0620 (Administrative Advice).
- Bit Map, Primary	•	M	M	Mandatory.
1 Bit Map, Secondary	•	M	M	Mandatory.
7 Transmission Date and Time	•	M	M	Transaction time stamp; UTC date and time that this transaction was entered into interchange.
11 Systems Trace Audit Number (STAN)	•	M	M	Transaction trace number; must be unique value for transaction initiator within each UTC day.
33 Forwarding Institution ID Code	•	M	M	Identifies the customer, institution, or Authorization Platform facility originating this Administrative Advice/0620. Value 003200 indicates RiskFinder generated the message.
48 Additional Data—Private Use	•	C	C	If DE 60 = 600, DE 48 will not be present in the message. If DE 60 = 650, DE 48 will contain the TCC and also may contain data for subelements 83, 87, 88, and 89 if they were present in a RiskFinder Authorization Advice/0120 message.
60 Advice Reason Code	•	M	M	Indicates specific type of message.
62 Intermediate Network Facility (INF) Data	•	C	C	If DE 60 = 600, INF data in the Administrative Advice/0620 contains MCBN620060000xxx, where xxx is the MIP ID. This data must be returned in an Administrative Advice Response/0630. If DE 60 = 650, INF data in the Administrative Advice/0620 contains the value RISK, and it must be returned in an Administrative Advice Response/0630.
63 Network Data	•	M	M	Contains the Banknet Reference Number that the Authorization Platform provides as a unique transaction ID.
100 Receiving Institution ID Code	•	M	M	Identifies the customer, institution, or Authorization Platform facility that will receive this Administrative Advice/0620.

Data Element ID and Name	Org	Sys	Dst	Comments
120 Record Data	•	C	C	If DE 60 = 600, contains rejected message. If DE 60 = 650, contains RiskFinder scoring information.
127 Private Data	•	O	O	Private use data element, available for optional use by message initiator.

## Message Layouts

### Administrative Advice/0620—Member-generated

---

## Administrative Advice/0620—Member-generated

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	•	M	Constant—0620 (Administrative Advice).
-	Bit Map, Primary	M	•	M	Mandatory.
1	Bit Map, Secondary	M	•	M	Mandatory.
7	Transmission Date and Time	M	•	M	Transaction time stamp; UTC date and time that this transaction was entered into interchange.
11	Systems Trace Audit Number (STAN)	M	•	M	Transaction trace number; must be unique value for transaction initiator within each UTC day.
33	Forwarding Institution ID Code	M	•	M	Identifies the customer, institution, or Authorization Platform facility originating this Administrative Advice/0620.
48	Additional Data—Private Use	C	•	C	This data element is not applicable to this message when used for Administrative textual message transmittal.
60	Advice Reason Code	M	•	M	Must contain value 650 to indicate Administrative textual message transmittal.
62	Intermediate Network Facility (INF) Data	C	•	C	Contains “acquiring network trace information” that intermediate network facilities (INFs) may require to quickly and accurately route Administrative Advice/0620 messages back to the originating institution.
63	Network Data	M	•	M	Contains the Banknet Reference Number that the Authorization Platform provides as a unique transaction ID.
100	Receiving Institution ID Code	M	•	M	Identifies the customer, institution, or Authorization Platform facility that will receive this Administrative Advice/0620.
120	Record Data	C	•	C	Contains textual message. May contain name, address, or interoffice routing information; free text format; used as an aid to insure that administration message is forwarded to a specific individual.
127	Private Data	O	X	•	Private use data element, available for optional use by message initiator.

## Administrative Advice Response/0630

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>		<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
-	Message Type Identifier (MTI)	M	M	•	Constant—0630 (Administrative Advice Response).
-	Bit Map, Primary	M	M	•	Mandatory.
1	Bit Map, Secondary	M	M	•	Mandatory.
7	Transmission Date and Time	ME	ME	•	Must be the same value from the original Administrative Advice/0620.
11	Systems Trace Audit Number (STAN)	ME	ME	•	Must be the same value from the original Administrative Advice/0620.
33	Forwarding Institution ID	ME	ME	•	Must be the same value from the original Administrative Advice/0620.
39	Response Code	M	M	•	Indicates the disposition of the original Administrative Advice/0620.
44	Additional Response Data	C	C	•	May contain the additional error code information depending on the value in DE 39.
62	Intermediate Network Facility (INF) Data	CE	CE	•	Must be the same value as in the original Administrative Advice/0620 if present.
63	Network Data	ME	ME	•	Must be the same value as in the original Administrative Advice/0620.
100	Receiving Institution ID Code	ME	ME	•	Must be the same value as in the original Administrative Advice/0620.
127	Private Data	•	X	CE	Private use data element, available for optional use by message initiator.

## Message Layouts

### Network Management Request/0800—Sign-On/Sign-Off

---

## Network Management Request/0800—Sign-On/Sign-Off

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	M	•	Constant—0800 (Network Management Request).
-	Bit Map, Primary	M	M	•	Mandatory.
1	Bit Map, Secondary	M	M	•	Mandatory.
2	Primary Account Number (PAN)	M	M	•	Must contain PAN prefix for “sign-on/off by prefix” functions; must contain MasterCard Group Sign-on for “group sign-on/off” functions or both the MasterCard Group Sign-on followed by the card prefix for a prefix sign-on/sign-off within a particular group.
7	Transmission Date and Time	M	M	•	Transaction time stamp; contains UTC date and time that this transaction was entered into interchange.
11	Systems Trace Audit Number (STAN)	M	M	•	Transaction trace number; must be unique value for transaction indicator within each UTC day.
20	Primary Account Number (PAN) Country Code	C	C	•	Country Code is required if DE 2 contains a BIN beginning with 59.
33	Forwarding Institution ID Code	M	M	•	Identifies the customer, institution, or Authorization Platform facility originating this Network Management Request/0800.
53	Security-Related Control Information	C	C	•	Issuers performing their own PIN validation and issuers participating in the PIN validation in Stand-In service must provide the PIN Key Index Number to be used for PIN translation.
63	Network Data	•	X	•	Authorization Platform transaction ID code that the Authorization Platform provides as a unique identifier for this transaction.
70	Network Management Information Code	M	M	•	Indicates the specific purpose of this message. Refer to the DE 70 data element definition for a list of applicable values by message type.
94	Service Indicator	M	M	•	For values applicable to the Network Management/0800 message, refer to this data element details in the “Data Element Definitions” chapter.

**Message Layouts****Network Management Request/0800—Sign-On/Sign-Off**

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
96      Message Security Code	M	M	•	Contains the MasterCard customer “password” security code, allowing access to the Authorization Platform network by a CPS or INF processor. Data must be provided in EBCDIC hexadecimal format.
127     Private Data	O	X	•	Private use data element, available for optional use by message initiator.

---

## Message Layouts

### Network Management Request/0800—RiskFinder SAF Request

---

# Network Management Request/0800—RiskFinder SAF Request

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	M	M	•	Constant—0800 (Network Management Request).
- Bit Map, Primary	M	M	•	Mandatory.
1 Bit Map, Secondary	M	M	•	Mandatory.
2 Primary Account Number (PAN)	M	M	•	Must contain PAN prefix for “sign-on/off by prefix” functions; must contain the MasterCard Group Sign-on for “group sign-on/off” functions.
7 Transmission Date and Time	M	M	•	Transaction time stamp; contains UTC date and time that this transaction was entered into interchange.
11 Systems Trace Audit Number (STAN)	M	M	•	Transaction trace number; must be unique value for transaction indicator within each UTC day.
20 Primary Account Number (PAN) Country Code	C	C	•	Country Code is required if DE 2 contains a BIN beginning with 59.
33 Forwarding Institution ID Code	M	M	•	Identifies the customer, institution, or Authorization Platform facility originating this Network Management Request/0800.
63 Network Data	•	X	•	Authorization Platform transaction ID code that the Authorization Platform provides as a unique identifier for this transaction.
70 Network Management Information Code	M	M	•	Indicates the specific purpose of this message. Refer to the DE 70 data element definition for a list of applicable values by message type.
94 Service Indicator	M	M	•	For values applicable to the Network Management/0800 message, refer to this data element details in the “Data Element Definitions” chapter.
96 Message Security Code	M	M	•	Contains the MasterCard customer “password” security code, allowing access to the Authorization Platform network by a CPS or INF processor. Data must be in EBCDIC hexadecimal format
127 Private Data	O	X	•	Private use data element, available for optional use by message initiator.

## Network Management Request/0800—Network Connection Status, Member-generated

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>		<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
-	Message Type Identifier (MTI)	M	M	•	Constant—0800 (Network Management Request).
-	Bit Map, Primary	M	M	•	Mandatory.
1	Bit Map, Secondary	M	M	•	Mandatory.
2	Primary Account Number (PAN)	M	M	•	Group Sign-on ID for which the network connection status is being requested.
7	Transmission Date and Time	M	M	•	Transaction time stamp; contains UTC date and time that this transaction was entered into interchange.
11	Systems Trace Audit Number (STAN)	M	M	•	Transaction trace number; must be unique value for transaction indicator within each UTC day.
33	Forwarding Institution ID Code	M	M	•	Identifies the customer, institution, or Authorization Platform facility originating this Network Management Request/0800.
63	Network Data	•	X	•	Authorization Platform transaction ID code that the Authorization Platform provides as a unique identifier for this transaction.
70	Network Management Information Code	M	M	•	Indicates the specific purpose of this message. Refer to the DE 70 data element definition for a list of applicable values by message type.

## Message Layouts

### Network Management Request/0800—Network Connection Status, System-generated

---

## Network Management Request/0800—Network Connection Status, System-generated

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	M	M	Constant—0800 (Network Management Request).
-	Bit Map, Primary	•	M	M	Mandatory.
1	Bit Map, Secondary	•	M	M	Mandatory.
2	Primary Account Number (PAN)	•	M	M	Group Sign-on ID for which the Authorization Platform is requesting the network connection status.
7	Transmission Date and Time	•	M	M	Transaction time stamp; contains UTC date and time that this transaction was entered into interchange.
11	Systems Trace Audit Number (STAN)	•	M	M	Transaction trace number; must be unique value for transaction indicator within each UTC day.
33	Forwarding Institution ID Code	•	M	M	Identifies the Authorization Platform facility originating this Network Management Request/0800.
63	Network Data	•	X	M	Authorization Platform transaction ID code that the Authorization Platform provides as a unique identifier for this transaction.
70	Network Management Information Code	•	M	M	Indicates the specific purpose of this message. Refer to for a list of applicable values by message type.

## Network Management Request/0800—Host Session Activation/Deactivation

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	M	•	Constant—0800 (Network Management Request).
-	Bit Map, Primary	M	M	•	Mandatory.
1	Bit Map, Secondary	M	M	•	Mandatory.
2	Primary Account Number (PAN)	M	M	•	Group Sign-on ID for which the network connection status is being requested.
7	Transmission Date and Time	M	M	•	Transaction time stamp; contains UTC date and time that this transaction was entered into interchange.
11	Systems Trace Audit Number (STAN)	M	M	•	Transaction trace number; must be unique value for transaction indicator within each UTC day.
33	Forwarding Institution ID Code	M	M	•	Identifies the customer, institution, or Authorization Platform facility originating this Network Management Request/0800.
70	Network Management Information Code	M	M	•	Indicates the specific purpose of this message. Refer to for a list of applicable values by message type.

## Message Layouts

### Network Management Request/0800—PEK Exchange

---

## Network Management Request/0800—PEK Exchange

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
- Message Type Identifier (MTI)		•	M	M	Constant—0800 (Network Management Request).
- Bit Map, Primary		•	M	M	Mandatory.
1	Bit Map, Secondary	•	M	M	Mandatory.
2	Primary Account Number (PAN)	•	M	M	Member Group ID of the member receiving the working key exchange; the Authorization Platform uses this to route the message to the appropriate issuer or acquirer.
7	Transmission Date and Time	•	M	M	Date and time that this message is transmitted; specified in UTC date and time format.
11	Systems Trace Audit Number (STAN)	•	M	M	Transaction trace number; must be unique value for all messages associated with a given transaction within each UTC day.
33	Forwarding Institution ID Code	•	M	M	Constant—002202; identifies the Authorization Platform.
48	Additional Data—Private Use	•	M	M	Key Exchange Data Block for key change function; the KEK is used to encrypt the PEK.
63	Network Data	•	M	M	Authorization Platform provides this data element; which includes a Banknet Reference Number for this transaction.
70	Network Management Information Code	•	M	M	Indicates the specific purpose of this Network Management Request/0800 as follows: 161 = Encryption key exchange request

## Network Management Request/0800—PEK Exchange On Demand

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>		<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)		M	M	•	Constant—0800 (Network Management Request).
- Bit Map, Primary		M	M	•	Mandatory.
1 Bit Map, Secondary		M	M	•	Mandatory.
2 Primary Account Number (PAN)		M	M	•	Member Group ID of the member requesting the working key exchange.
7 Transmission Date and Time		M	M	•	Date and time that this message is transmitted; specified in UTC date and time format.
11 Systems Trace Audit Number (STAN)		M	M	•	Transaction trace number; must be unique value for all messages associated with a given transaction within each UTC day.
33 Forwarding Institution ID Code		M	M	•	ID of the member originating this message; must be the same value as DE 2.
63 Network Data		•	M	•	Authorization Platform provides this data element; which includes a Banknet Reference Number for this transaction.
70 Network Management Information Code		M	M	•	Indicates the specific purpose of this Network Management Request/0800 as follows: 162 = Solicitation for key exchange request
127 Private Data		O	X	•	Private use data element, available for optional use by message initiator; this data is not passed to the Authorization Platform.

## Message Layouts

### Network Management Request Response/0810—Sign-On/Sign-Off

---

# Network Management Request Response/0810—Sign-On/Sign-Off

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	M	M	Constant—0810 (Network Management Request Response).
-	Bit Map, Primary	•	M	M	Mandatory.
1	Bit Map, Secondary	•	M	M	Mandatory.
2	Primary Account Number (PAN)	•	ME	ME	Must be the same value as in the original Network Management Request/0800—Sign-On/Sign-Off.
7	Transmission Date and Time	•	ME	ME	Must be the same value as in the original Network Management Request/0800—Sign-On/Sign-Off.
11	Systems Trace Audit Number (STAN)	•	ME	ME	Must be the same value as in the original Network Management Request/0800—Sign-On/Sign-Off.
33	Forwarding Institution ID Code	•	ME	ME	Must be the same value as in the original Network Management Request/0800—Sign-On/Sign-Off.
39	Response Code	•	M	M	Indicates disposition of original Network Management Request/0800—Sign-On/Sign-Off.
44	Additional Response Data	•	C	C	May be present to provide additional information about message error conditions when the value in DE 39 is 30.
63	Network Data	•	ME	ME	Must be the same value as in the original Network Management Request/0800—Sign-On/Sign-Off.
70	Network Management Information Code	•	ME	ME	Must be the same value as in the original Network Management Request/0800—Sign-On/Sign-Off.
127	Private Data	•	X	CE	Must be the same value as in the original Network Management Request/0800—Sign-On/Sign-Off.

## Network Management Request Response/0810—RiskFinder SAF Request

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	•	M	M	Constant—0810 (Network Management Request Response).
- Bit Map, Primary	•	M	M	Mandatory.
1 Bit Map, Secondary	•	M	M	Mandatory.
2 Primary Account Number (PAN)	•	ME	ME	Must be the same value as in the original Network Management Request/0800—Riskfinder SAF Request.
7 Transmission Date and Time	•	ME	ME	Must be the same value as in the original Network Management Request/0800—Riskfinder SAF Request.
11 Systems Trace Audit Number (STAN)	•	ME	ME	Must be the same value as in the original Network Management Request/0800—RiskFinder SAF Request.
33 Forwarding Institution ID Code	•	ME	ME	Must be the same value as in the original Network Management Request/0800—RiskFinder SAF Request.
39 Response Code	•	M	M	Indicates disposition of original Network Management Request/0800—RiskFinder SAF Request.
44 Additional Response Data	•	C	C	May be present to provide additional information about message error conditions when the value in DE 39 is 30.
63 Network Data	•	ME	ME	Must be the same value as in the original Network Management Request/0800—RiskFinder SAF Request.
70 Network Management Information Code	•	ME	ME	Must be the same value as in the original Network Management Request/0800—RiskFinder SAF Request.
127 Private Data	•	X	CE	Must be the same value as in the original Network Management Request/0800—RiskFinder SAF Request.

## Message Layouts

### Network Management Request Response/0810—Network Connection Status, Member-generated

---

## Network Management Request Response/0810—Network Connection Status, Member-generated

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	M	•	Constant—0810 (Network Management Request Response).
-	Bit Map, Primary	M	M	•	Mandatory.
1	Bit Map, Secondary	M	M	•	Mandatory.
2	Primary Account Number (PAN)	ME	ME	•	The Member Group ID. Must be the same value as in the original Network Management Request/0800.
7	Transmission Date and Time	ME	ME	•	Must be the same value as in the original Network Management Request/0800.
11	Systems Trace Audit Number (STAN)	ME	ME	•	Must be the same value as in the original Network Management Request/0800.
33	Forwarding Institution ID Code	ME	ME	•	Must be the same value as in the original Network Management Request/0800.
39	Response Code	M	M	•	Indicates disposition of original Network Management Request/0800.
63	Network Data	ME	ME	•	Must be the same value as in the original Network Management Request/0800.
70	Network Management Information Code	ME	ME	•	Must be the same value as in the original Network Management Request/0800.

## Network Management Request Response/0810—Network Connection Status, System-generated

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	•	M	M	Constant—0810 (Network Management Request Response).
- Bit Map, Primary	•	M	M	Mandatory.
1 Bit Map, Secondary	•	M	M	Mandatory.
2 Primary Account Number (PAN)	•	ME	ME	The Member Group ID. Must be the same value as in the original Network Management Request/0800.
7 Transmission Date and Time	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
11 Systems Trace Audit Number (STAN)	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
33 Forwarding Institution ID Code	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
39 Response Code	•	M	M	Indicates disposition of original Network Management Request/0800.
44 Additional Response Data	•	C	C	May be present to provide additional information about message error conditions when the value in DE 39 is 30.
63 Network Data	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
70 Network Management Information Code	•	ME	ME	Must be the same value as in the original Network Management Request/0800.

## Message Layouts

### Network Management Request Response/0810—Host Session Activation/Deactivation

---

## Network Management Request Response/0810—Host Session Activation/Deactivation

Following is the list of the data elements applicable to this message.

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	M	M	Constant—0810 (Network Management Request Response).
-	Bit Map, Primary	•	M	M	Mandatory.
1	Bit Map, Secondary	•	M	M	Mandatory.
2	Primary Account Number (PAN)	•	ME	ME	The Member Group ID. Must be the same value as in the original Network Management Request/0800.
7	Transmission Date and Time	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
11	Systems Trace Audit Number (STAN)	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
33	Forwarding Institution ID Code	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
39	Response Code	•	M	M	Indicates disposition of original Network Management Request/0800.
44	Additional Response Data	•	C	C	May be present to provide additional information about message error conditions when the value in DE 39 is 30.
70	Network Management Information Code	•	ME	ME	Must be the same value as in the original Network Management Request/0800.

## Network Management Request Response/0810—PEK Exchange

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	M	M	•	Constant—0810 (Network Management Request Response).
- Bit Map, Primary	M	M	•	Mandatory.
1 Bit Map, Secondary	M	M	•	Mandatory.
2 Primary Account Number (PAN)	ME	ME	•	The Member Group ID. Must be the same value as in the original Network Management Request/0800.
7 Transmission Date and Time	ME	ME	•	Must be the same value as in the original Network Management Request/0800.
11 Systems Trace Audit Number (STAN)	ME	ME	•	Must be the same value as in the original Network Management Request/0800.
33 Forwarding Institution ID Code	ME	ME	•	Must be the same value as in the original Network Management Request/0800.
39 Response Code	M	M	•	Indicates disposition of original Network Management Request/0800.
44 Additional Response Data	C	C	•	May be present to provide additional information on message error conditions when the value in DE 39 is 30.
48 Additional Data—Private Use	ME	ME	•	Must be the same value as in the original Network Management Request/0800.
63 Network Data	ME	ME	•	Must be the same value as in the original Network Management Request/0800.
70 Network Management Information Code	ME	ME	•	Must be the same value as in the original Network Management Request/0800.

## Message Layouts

### Network Management Request Response/0810—PEK Exchange-On Demand

---

# Network Management Request Response/0810—PEK Exchange-On Demand

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	•	M	M	Constant—0810 (Network Management Request Response).
- Bit Map, Primary	•	M	M	Mandatory.
1 Bit Map, Secondary	•	M	M	Mandatory.
2 Primary Account Number (PAN)	•	ME	ME	The Member Group ID. Must be the same value as in the original Network Management Request/0800.
7 Transmission Date and Time	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
11 Systems Trace Audit Number (STAN)	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
33 Forwarding Institution ID Code	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
39 Response Code	•	M	M	Indicates disposition of original Network Management Request/0800.
44 Additional Response Data	•	C	C	May be present to provide additional information on message error conditions when the value in DE 39 is 30.
63 Network Data	•	ME	ME	Must be the same value as in the original Network Management Request/0800.
70 Network Management Information Code	•	ME	ME	Must be the same value as in the original Network Management Request/0800.

## Network Management Advice/0820—RiskFinder SAF End of File

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>		<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
-	Message Type Identifier (MTI)	•	M	M	Constant—0820 (Network Management Advice).
-	Bit Map, Primary	•	M	M	Mandatory.
1	Bit Map, Secondary	•	M	M	Mandatory.
7	Transmission Date and Time	•	M	M	Transaction time stamp; UTC date and time that this transaction was entered into interchange.
11	Systems Trace Audit Number (STAN)	•	M	M	Transaction trace number; must be unique value for transaction initiator within each UTC day.
33	Forwarding Institution ID Code	•	M	M	Contains the MasterCard customer ID number of CPS, INF, or Authorization Platform facility originating this message.
48	Additional Data—Private Use	•	C	C	
63	Network Data	•	M	M	Authorization Platform transaction ID code that the Authorization Platform provides as a unique identifier for this transaction.
70	Network Management Information Code	•	M	M	Indicates the specific purpose of this Network Management Advice/0820. Valid value is 072.

## Message Layouts

### Network Management Advice/0820—PEK Exchange

---

## Network Management Advice/0820—PEK Exchange

Following is the list of the data elements applicable to this message.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	•	M	M	Constant—0820 (Network Management Advice).
- Bit Map, Primary	•	M	M	Mandatory.
1 Bit Map, Secondary	•	M	M	Mandatory.
2 Primary Account Number (PAN)	•	M	M	Member Group ID of the member receiving this working key exchange; the Authorization Platform uses this data to route the transaction to the appropriate issuer or acquirer.
7 Transmission Date and Time	•	M	M	Date and time that this message is transmitted; specified in UTC date and time format.
11 Systems Trace Audit Number (STAN)	•	M	M	Transaction trace number; must be unique value for all messages associated with a given transaction within each UTC day.
33 Forwarding Institution ID Code	•	M	M	Constant—002202; identifies the Authorization Platform.
48 Additional Data—Private Use	•	M	M	Key Exchange Data Block for key exchange function; the communication key is used to encrypt the working key.
63 Network Data	•	M	M	Authorization Platform provides this data element; which includes a Banknet Reference Number for this transaction.
70 Network Management Information Code	•	M	M	Indicates the specific purpose of this Network Management Advice/0820 as follows: 161 = Encryption key exchange request

---

## Chapter 4 Data Element Definitions

*This section provides data element (DE) detail definitions of all data elements used in Authorization Platform application messages.*

---

Data Element Layout.....	4-1
Subelement Layout .....	4-1
Subfield Layout .....	4-2
Position Layout .....	4-2
List of Data Elements (Numeric Order).....	4-2
List of Data Elements (Alphabetic Order) .....	4-7
Message Type Identifier.....	4-11
Message Types and Applicable Program or Service .....	4-14
About Primary and Secondary Bit Maps .....	4-15
Primary Bit Map.....	4-16
DE 1—Bit Map, Secondary .....	4-18
DE 2—Primary Account Number (PAN) .....	4-20
About Primary Account Number.....	4-23
DE 3—Processing Code .....	4-24
Subfield 1—Cardholder Transaction Type Code.....	4-25
Subfield 2—Cardholder "From Account" Type Code .....	4-27
Subfield 3—Cardholder "To Account" Type Code .....	4-28
DE 4—Amount, Transaction .....	4-28
DE 5—Amount, Settlement .....	4-31
DE 6—Amount, Cardholder Billing.....	4-32
DE 7—Transmission Date and Time .....	4-34
Subfield 1—Date.....	4-36
Subfield 2—Time .....	4-36
DE 8—Amount, Cardholder Billing Fee.....	4-37
DE 9—Conversion Rate, Settlement.....	4-37
Subfield 1—Decimal Indicator.....	4-38
Subfield 2—Conversion Rate .....	4-39
DE 10—Conversion Rate, Cardholder Billing.....	4-39
Subfield 1—Decimal Indicator.....	4-40
Subfield 2—Cardholder Billing Conversion Rate .....	4-41
DE 11—System Trace Audit Number (STAN).....	4-41

## Data Element Definitions

---

DE 12—Time, Local Transaction.....	4-43
DE 13—Date, Local Transaction .....	4-44
DE 14—Date, Expiration.....	4-45
DE 15—Date, Settlement .....	4-46
DE 16—Date, Conversion .....	4-48
DE 17—Date, Capture .....	4-49
DE 18—Merchant Type.....	4-49
DE 19—Acquiring Institution Country Code.....	4-51
DE 20—Primary Account Number (PAN) Country Code.....	4-51
DE 21—Forwarding Institution Country Code .....	4-53
DE 22—Point-of-Service (POS) Entry Mode.....	4-53
Subfield 1—POS Terminal PAN Entry Mode .....	4-54
Subfield 2—POS Terminal PIN Entry Mode.....	4-56
Authorization Platform Edits .....	4-57
MasterCard Electronic Card Transactions .....	4-57
Chip Transactions .....	4-57
Magnetic Stripe or Chip-Read Transactions for MasterCard Electronic Card.....	4-59
DE 23—Card Sequence Number.....	4-60
DE 24—Network International ID .....	4-61
DE 25—Point-of-Service (POS) Condition Code.....	4-62
DE 26—Point-of-Service (POS) Personal ID Number (PIN) Capture Code.....	4-62
DE 27—Authorization ID Response Length.....	4-63
DE 28—Amount, Transaction Fee.....	4-64
Subfield 1—Debit/Credit Indicator .....	4-65
Subfield 2—Amount.....	4-66
DE 29—Amount, Settlement Fee .....	4-66
Subfield 1—Debit/Credit Indicator .....	4-66
Subfield 2—Amount.....	4-67
DE 30—Amount, Transaction Processing Fee .....	4-67
Subfield 1—Debit/Credit Indicator .....	4-68
Subfield 2—Amount.....	4-68
DE 31—Amount, Settlement Processing Fee.....	4-68
Subfield 1—Debit/Credit Indicator .....	4-69
Subfield 2—Amount.....	4-69
DE 32—Acquiring Institution ID Code.....	4-69
DE 33—Forwarding Institution ID Code.....	4-71
DE 34—Primary Account Number (PAN), Extended.....	4-73

---

DE 35—Track 2 Data .....	4-74
DE 36—Track 3 Data .....	4-76
DE 37—Retrieval Reference Number .....	4-76
Subfield 1—Transaction Date and Initiator Discretionary Data .....	4-78
Subfield 2—Terminal Transaction Number .....	4-78
DE 38—Authorization ID Response .....	4-79
DE 39—Response Code .....	4-80
Authorization Request Response/0110 Response Codes .....	4-82
Authorization Advice/0120 Response Codes .....	4-84
Authorization Advice Response/0130 Response Codes .....	4-86
Authorization Advice Response/0180 Response Codes .....	4-87
Authorization Negative Acknowledgement/0190 Response Codes .....	4-87
Issuer File Update Request Response/0312 Response Codes .....	4-87
Reversal Request/0400 Message Response Codes .....	4-87
Reversal Request Response/0410 Response Codes .....	4-89
Reversal Advice/0420 Response Codes .....	4-90
Reversal Advice Response/0430 Message and Administrative Advice Response/0630 Response Codes .....	4-92
Administrative Request Response/0610 Response Codes .....	4-93
Network Management Request Response/0810 Response Codes .....	4-93
DE 40—Service Restriction Code .....	4-94
DE 41—Card Acceptor Terminal ID .....	4-94
DE 42—Card Acceptor ID Code .....	4-96
DE 43—Card Acceptor Name/Location for All Transactions .....	4-97
Subfield 1—Merchant Name ("Doing Business As" name) .....	4-98
Subfield 2—Space .....	4-99
Subfield 3—Merchant's City .....	4-99
Subfield 4—Space .....	4-99
Subfield 5—Merchant's State (or Country Code, if not U.S.) .....	4-100
DE 43—Card Acceptor Name/Location for ATM Transactions .....	4-100
Subfield 1—ATM Owning Institution or Terminal/Merchant Address or Both .....	4-101
Subfield 2—Space .....	4-101
Subfield 3—ATM or Merchant Location City .....	4-102
Subfield 4—Space .....	4-102
Subfield 5—ATM or Merchant State, Province, or Country Code Location .....	4-102
DE 43—Card Acceptor Name/Location for Bankcard-Activated Public Phones .....	4-103
Subfield 1—Abbreviation "TEL" .....	4-104
Subfield 2—Phone Number Dialed .....	4-104

## Data Element Definitions

---

Subfield 3—Abbreviation "M" .....	4-105
Subfield 4—Call Duration .....	4-105
Subfield 5—Space .....	4-105
Subfield 6—Call Origin City .....	4-106
Subfield 7—Space .....	4-106
Subfield 8—Call Origin State or Country Code .....	4-106
DE 44—Additional Response Data .....	4-107
DE 44 Values by Program or Service .....	4-108
DE 45—Track 1 Data .....	4-110
DE 46—Expanded Additional Amounts .....	4-112
DE 47—Additional Data—National Use .....	4-112
DE 48—Additional Data—Private Use .....	4-113
DE 48 Transaction Category Code .....	4-114
DE 48 Subelement Encoding Scheme in Authorization Request/0100 Messages .....	4-115
DE 48 Subelement Encoding Scheme in Network Management Messages .....	4-116
List of DE 48 Subelements .....	4-116
Subelement 10—Encrypted PIN Block Key .....	4-120
Subelement 11—Key Exchange Block Data (Single-Length Keys) .....	4-120
Subelement 11—Key Exchange Block Data (Double-Length Keys) .....	4-121
Subelement 11—Key Exchange Block Data (Triple-Length Keys) .....	4-123
Subelement 12—Routing Indicator .....	4-124
Subelement 13—MasterCard Hosted Mobile Phone Top-up Request Data .....	4-125
Subfield 1—Mobile Phone Number .....	4-125
Subfield 2—Mobile Phone Service Provider Name .....	4-126
Subelement 15—Authorization System Advice Date and Time .....	4-126
Subfield 1—Date .....	4-127
Subfield 2—Time .....	4-127
Subelement 16—Processor Pseudo ICA .....	4-127
Subelement 20—Cardholder Verification Method .....	4-128
Subelement 23—Payment Initiation Channel .....	4-129
Subfield 1—Device Type .....	4-129
Subelement 25—MasterCard Cash Program Data .....	4-130
Subfield 01—Message Identifier .....	4-130
Subelement 32—MasterCard Assigned ID .....	4-131
Subelement 33—PAN Mapping File Information .....	4-132
Subelement 33 Encoding Scheme .....	4-133
Subfield 1—Account Number Indicator .....	4-134
Subfield 2—Account Number .....	4-134

---

Subfield 3—Expiration Date .....	4-135
Subfield 4—Product Code .....	4-135
Subelement 34—Dynamic CVC 3 ATC Information .....	4-136
Subfield 1—ATC Value.....	4-137
Subfield 2—ATC Discrepancy Value .....	4-137
Subfield 3—ATC Discrepancy Indicator.....	4-137
Subelement 34 Subfield Data Examples.....	4-138
Subelement 35— <i>PayPass</i> Non-Card Form Factor Request/Response .....	4-139
Subelement 36—Visa Defined Data (Visa Only).....	4-140
Subfield 1—Merchant Verification Value.....	4-141
Subelement 38—Account Category.....	4-141
Subelement 39—Expert Monitoring Compromised Account Service Information.....	4-142
Subelement 40—Electronic Commerce Merchant/Cardholder Certificate Serial Number (Visa Only) .....	4-144
Subfield 1—Merchant Certificate Serial Number.....	4-145
Subfield 2—Cardholder Certificate Serial Number.....	4-145
Subelement 41—Electronic Commerce Certificate Qualifying Information.....	4-146
Subfield 1—Reserved for Future Use.....	4-147
Subfield 2—Reserved for Future Use.....	4-147
Subfield 3—Reserved for Future Use.....	4-147
Subfield 4—Reserved for Future Use.....	4-147
Subfield 5—Reserved for Future Use.....	4-147
Subfield 6—Reserved for Future Use.....	4-148
Subfield 7—Reserved for Future Use.....	4-148
Subfield 8—Reserved for Future Use.....	4-148
Subfield 9—Reserved for Future Use.....	4-148
Subfield 10—Reserved for Future Use .....	4-149
Subfield 11—Citizen ID .....	4-149
Subfield 12—Reserved for Future Use .....	4-149
Subfield 13—Reserved for Future Use .....	4-149
Subfield 14—Reserved for Future Use .....	4-150
Subfield 15—Reserved for Future Use .....	4-150
Subfield 16—Reserved for Future Use .....	4-150
Subfield 17—Reserved for Future Use .....	4-150
Subfield 18—Reserved for Future Use .....	4-151
Subelement 42—Electronic Commerce Indicators .....	4-151
Subfield 1—Electronic Commerce Security Level Indicator and UCAF Collection Indicator .....	4-152
Subelement 43—Universal Cardholder Authentication Field (UCAF) .....	4-153

## Data Element Definitions

---

Subelement 43—3-D Secure for MasterCard SecureCode .....	4-154
Subelement 43—Static AAV for Maestro or MasterCard Advance Registration Program .....	4-155
Subelement 43—Secure Electronic Commerce Verification Service (Visa Only) .....	4-156
Subelement 44—Visa 3-D Secure Electronic Commerce Transaction Identifier (XID) (Visa Only) .....	4-156
Subelement 45—Visa 3-D Secure Electronic Commerce Transaction Response Code (Visa Only) .....	4-157
Subelement 46—Card-Level Result (Visa Only) .....	4-158
Subelement 47—MasterCard Payment Gateway Transaction Indicator.....	4-159
Subelement 48—Mobile Program Indicators.....	4-160
Subfield 1—Remote Payments Program Type Identifier.....	4-161
Subfield 2—Reserved for Future Use.....	4-161
Subfield 3—Mobile Phone Number.....	4-161
Subfield 4—Convenience Fee.....	4-162
Subelement 51—Merchant On-behalf Services .....	4-162
Subfield 1—Merchant On-behalf [OB] Service .....	4-163
Subfield 2—Merchant On-behalf [OB] Result 1.....	4-163
Valid Subfield 1 and Subfield 2 Value Combinations .....	4-164
Subfield 3—Additional Information .....	4-164
Subelement 55—Merchant Fraud Scoring Data.....	4-165
Subfield 1—Merchant Fraud Score .....	4-165
Subfield 2—Merchant Score Reason Code .....	4-166
Subfield 3—Reserved for Future Use.....	4-166
Subfield 4—Reserved for Future Use .....	4-167
Subfield 5—Reserved for Future Use .....	4-167
Subelement 58—ATM Additional Data.....	4-168
Subfield 1—ATM Time .....	4-168
Subfield 2—ATM Date .....	4-168
Subfield 3—Watermark .....	4-169
Subfield 4—Mark 1 .....	4-169
Subfield 5—Mark 2 .....	4-170
Subfield 6—Mark 3 .....	4-170
Subfield 7—Card Swallowed Status .....	4-171
Subfield 8—Posting Date .....	4-171
Subelement 61—POS Data Extended Condition Codes .....	4-171
Subfield 1—Partial Approval Terminal Support Indicator.....	4-172
Subfield 2—Purchase Amount Only Terminal Support Indicator.....	4-172
Subfield 3—Real-time Substantiation Indicator .....	4-173

---

Subfield 4—Merchant Transaction Fraud Scoring Indicator .....	4-173
Subfield 5—Reserved for Future Use.....	4-174
Subelement 63—Trace ID .....	4-174
Subelement 64—Transit Program.....	4-176
Subfield 1—Transit Transaction Type Indicator.....	4-176
Subfield 2—Transportation Mode Indicator .....	4-177
Subelement 71—On-behalf Services.....	4-178
Subfield 1—On-behalf (OB) Service.....	4-179
Subfield 2—On-behalf Result 1.....	4-179
Subfield 3—On-behalf Result 2.....	4-181
Valid Subfield 1 and Subfield 2 Value Combinations .....	4-182
Subelement 72—Issuer Chip Authentication.....	4-182
Subelement 74—Additional Processing Information.....	4-183
Subfield 1—Processing Indicator .....	4-184
Subfield 2—Processing Information.....	4-185
Valid Subfield 1 and Subfield 2 Value Combinations .....	4-185
Subelement 75—Fraud Scoring Data .....	4-186
Subfield 1—Fraud Score .....	4-186
Subfield 2—Score Reason Code.....	4-187
Subfield 3—Rules Adjusted Score .....	4-187
Subfield 4—Rules Reason Code 1.....	4-188
Subfield 5—Rules Reason Code 2.....	4-188
Subelement 76—MasterCard Electronic Acceptance Indicator.....	4-189
Subelement 77—Payment Transaction Type Indicator .....	4-190
Subelement 78—U.S. Deferred Billing Indicator (Visa Only).....	4-191
Subelement 79—Chip CVR/TVR Bit Error Results.....	4-192
Subfield 1—CVR or TVR Identifier.....	4-193
Subfield 2—Byte ID .....	4-194
Subfield 3—Byte Identifier.....	4-194
Subfield 4—Value of Bit in Error .....	4-194
Subelement 80—PIN Service Code .....	4-195
Subelement 82—Address Verification Service Request .....	4-196
Subelement 83—Address Verification Service Response.....	4-196
Subelement 84—Merchant Advice Code.....	4-198
Subelement 84—Visa Response Codes (Visa Only).....	4-198
Subelement 85—U.S. Existing Debt Indicator (Visa Only).....	4-199
Subelement 86—Relationship Participant Indicator (Visa Only) .....	4-200
Subelement 87—Card Validation Code Result .....	4-200

## Data Element Definitions

---

Subelement 87—CVV2 Response (Visa Only) .....	4-202
Subelement 88—Magnetic Stripe Compliance Status Indicator .....	4-202
Subelement 89—Magnetic Stripe Compliance Error Indicator .....	4-203
Subelement 90—Lodging and Auto Rental Indicator .....	4-204
Subelement 90—Custom Payment Service Request (Visa Only) .....	4-205
Subelement 90—Custom Payment Service Request Response (Visa Only) .....	4-206
Subelement 91—Acquirer Reference Data (American Express Only) .....	4-207
Subelement 91—Custom Payment Service Request Transaction ID (Visa Only) .....	4-207
Subelement 91—Custom Payment Service Response Transaction ID (Visa Only) .....	4-208
Subelement 92—CVC 2 .....	4-209
Subelement 92—CVV2 Data (Visa Only) .....	4-210
Subelement 93—Fleet Card ID Request Data (Visa Only) .....	4-211
Subfield 1—Fleet Card ID Request Indicator .....	4-212
Subfield 2—Optional Free-form Informational Text .....	4-212
Subelement 94—Commercial Card Inquiry Request (Visa Only) .....	4-212
Subelement 94—Commercial Card Inquiry Response (Visa Only) .....	4-213
Subelement 95—MasterCard Promotion Code .....	4-214
Subelement 95—American Express Customer ID Number (American Express Only) .....	4-215
Subelement 96—Visa Market-Specific Data Identifier (Visa Only) .....	4-215
Subelement 97—Prestigious Properties Indicator (Visa Only) .....	4-216
Subelement 98—MasterCard Corporate Fleet Card ID/Driver Number .....	4-217
Subelement 99—MasterCard Corporate Fleet Card Vehicle Number .....	4-218
DE 48—Authorization Platform Edits .....	4-219
DE 48, TCC .....	4-219
DE 48, TCC and DE 3 .....	4-219
DE 48, Subelement 32 .....	4-220
DE 48, Subelement 35 .....	4-221
DE 48, Subelement 38 .....	4-222
DE 48, Subelement 42 and Subelement 43 .....	4-223
DE 48, Subelement 43 (Static AAV for Maestro or MasterCard Advance Registration Program) .....	4-224
DE 48, Subelement 42 and DE 61 .....	4-225
DE 48, Subelement 61 .....	4-226
DE 48, Subelement 78 .....	4-227
DE 48, Subelement 82 .....	4-228
DE 48, Subelement 86 .....	4-228
DE 48, in Authorization Request Response .....	4-228
DE 49—Currency Code, Transaction .....	4-228

---

DE 50—Currency Code, Settlement .....	4-229
DE 51—Currency Code, Cardholder Billing.....	4-231
DE 52—Personal ID Number (PIN) Data .....	4-232
DE 53—Security-Related Control Information.....	4-233
Subfield 1—PIN Security Type Code .....	4-234
Subfield 2—PIN Encryption Type Code .....	4-234
Subfield 3—PIN Block Format Code .....	4-235
Subfield 4—PIN Key Index Number.....	4-235
Subfield 5—Reserved for Future Use .....	4-235
Subfield 6—Reserved for Future Use .....	4-236
DE 54—Additional Amounts.....	4-236
Subfield 1—Account Type .....	4-238
Subfield 2—Amount Type .....	4-238
Subfield 3—Currency Code .....	4-239
Subfield 4—Amount.....	4-239
DE 55—Integrated Circuit Card (ICC) System-Related Data.....	4-240
DE 55—Subelement Encoding Scheme .....	4-240
DE 55—Subelements .....	4-241
DE 55—Authorization Platform Edits.....	4-244
DE 56—Reserved for ISO Use .....	4-246
DE 57—DE 59—Reserved for National Use.....	4-247
DE 60—Advice Reason Code.....	4-247
Subfield 1—Advice Reason Code .....	4-248
DE 60, Subfield 1 Values, in Authorization Advice/0120 .....	4-248
DE 60, Authorization Advice/0120 Edits .....	4-249
DE 60, Subfield 1 Values, in Reversal Advice/0420.....	4-250
DE 60, Subfield 1 Values, in Administrative Request/0600 .....	4-250
DE 60, Subfield 1 Values, in Administrative Request Response/0610 .....	4-250
DE 60, Subfield 1 Values, in Administrative Advice/0620 .....	4-251
Subfield 2—Advice Detail Code.....	4-251
DE 60, Subfield 2 Values, in Authorization Advice/0120—Issuer-generated.....	4-252
DE 60, Subfield 2 Values, in Authorization Advice/0120—System-generated .....	4-252
DE 60, Subfield 2 Values, in Administrative Advice/0620 .....	4-253
DE 60, Subfield 2 Values, in Customer Service Messages .....	4-253
DE 60, Subfield 2 Values, in CVC 3 Validation.....	4-253
DE 60, Subfield 2 Values, in MasterCard inControl Service.....	4-254
DE 60, Subfield 2 Values, in M/Chip On-Behalf Services .....	4-254
DE 60, Subfield 2 Values, in Pay with Rewards .....	4-255

## Data Element Definitions

---

DE 60, Subfield 2 Values, in PIN Validation.....	4-255
DE 60, Subfield 2 Values, in Private Label Processing .....	4-255
DE 60, Subfield 2 Values, in TCC, CAT Level, and Promotion Code in Failed Parameter Combinations (country-specific) .....	4-256
DE 60, Subfield 2 Values, in TCC, CAT Level, and Promotion Code in Failed Parameter Combinations (global) .....	4-256
DE 60, Subfield 2 Values, in MCC, CAT Level, and Promotion Code in Failed Parameter Combinations (country-specific) .....	4-257
DE 60, Subfield 2 Values, in MCC and Promotion Code in Failed Parameter Combinations (country-specific) .....	4-257
DE 60, Subfield 2 Values, in MCC and Promotion Code in Failed Parameter Combinations (global) .....	4-258
DE 60, Subfield 2 Values, in TCC and Promotion Code in Failed Parameter Combinations (country-specific) .....	4-258
DE 60, Subfield 2 Values, in TCC and Promotion Code in Failed Parameter Combinations (global) .....	4-259
DE 60, Subfield 2 Values, in MCC and CAT Level in Failed Parameter Combinations (country-specific).....	4-259
DE 60, Subfield 2 Values, in MCC and CAT Level in Failed Parameter Combinations (global) .....	4-260
DE 60, Subfield 2 Values, in TCC and CAT Level in Failed Parameter Combinations (country-specific) .....	4-260
DE 60, Subfield 2 Values, in TCC and CAT Level in Failed Parameter Combinations (global) .....	4-261
DE 60, Subfield 2 Values, in MCC in Failed Parameter Combinations (country-specific).....	4-261
DE 60, Subfield 2 Values, in MCC in Failed Parameter Combinations (global).....	4-262
DE 60, Subfield 2 Values, in TCC in Failed Parameter Combinations (country-specific) .....	4-262
DE 60, Subfield 2 Values, in TCC in Failed Parameter Combinations (global).....	4-263
DE 60, Subfield 2 Values, in Miscellaneous Processing .....	4-263
Subfield 3—Advice Detail Text.....	4-264
DE 61—Point-of-Service (POS) Data.....	4-264
Subfield 1—POS Terminal Attendance .....	4-265
Subfield 2—Reserved for Future Use .....	4-265
Subfield 3—POS Terminal Location.....	4-266
Subfield 4—POS Cardholder Presence .....	4-266
Subfield 5—POS Card Presence.....	4-267
Subfield 6—POS Card Capture Capabilities .....	4-267
Subfield 7—POS Transaction Status .....	4-267
Subfield 8—POS Transaction Security.....	4-268

---

Subfield 9—Reserved for Future Use .....	4-268
Subfield 10—Cardholder-Activated Terminal Level.....	4-269
Subfield 11—POS Card Data Terminal Input Capability Indicator .....	4-269
Subfield 12—POS Authorization Life Cycle.....	4-270
Subfield 13—POS Country Code .....	4-271
Subfield 14—POS Postal Code.....	4-271
Authorization Platform Edits .....	4-272
DE 62—Intermediate Network Facility (INF) Data .....	4-274
DE 63—Network Data .....	4-276
Subfield 1—Financial Network Code .....	4-277
Subfield 2—Banknet Reference Number .....	4-287
DE 64—Message Authentication Code.....	4-287
DE 65—Bit Map, Extended .....	4-288
DE 66—Settlement Code .....	4-288
DE 67—Extended Payment Code .....	4-289
DE 68—Receiving Institution Country Code .....	4-289
DE 69—Settlement Institution Country Code.....	4-289
DE 70—Network Management Information Code .....	4-290
Network Management Request/0800—Sign-On/Sign-Off .....	4-291
Network Management Request/0800—RiskFinder SAF Request .....	4-292
Network Management Advice/0820—RiskFinder SAF End of File .....	4-293
Network Management Request/0800—Network Connection Status, Member-generated .....	4-293
Network Management Request/0800—Network Connection Status, System-generated .....	4-293
Network Management Request/0800—Host Session Activation/Deactivation.....	4-293
Network Management Request/0800—PEK Exchange.....	4-294
Network Managment Request/0800—PEK Exchange-On Demand.....	4-294
DE 71—Message Number .....	4-294
DE 72—Message Number Last .....	4-294
DE 73—Date, Action.....	4-295
DE 74—Credits, Number .....	4-295
DE 75—Credits, Reversal Number .....	4-296
DE 76—Debits, Number .....	4-296
DE 77—Debits, Reversal Number .....	4-296
DE 78—Transfers, Number .....	4-297
DE 79—Transfers, Reversal Number .....	4-297

## Data Element Definitions

---

DE 80—Inquiries, Number.....	4-298
DE 81—Authorizations, Number.....	4-298
DE 82—Credits, Processing Fee Amount .....	4-298
DE 83—Credits, Transaction Fee Amount.....	4-299
DE 84—Debits, Processing Fee Amount.....	4-299
DE 85—Debits, Transaction Fee Amount.....	4-300
DE 86—Credits, Amount.....	4-300
DE 87—Credits, Reversal Amount .....	4-300
DE 88—Debits, Amount.....	4-301
DE 89—Debits, Reversal Amount .....	4-301
DE 90—Original Data Elements.....	4-302
Subfield 1—Original Message Type Identifier .....	4-302
Subfield 2—Original DE 11 (Systems Trace Audit Number) .....	4-303
Subfield 3—Original DE 7 (Transmission Date and Time).....	4-303
Subfield 4—Original DE 32 (Acquiring Institution ID Code) .....	4-304
Subfield 5—Original DE 33 (Forwarding Institution ID Code) .....	4-304
DE 91—Issuer File Update Code .....	4-304
DE 92—File Security Code.....	4-305
DE 93—Response Indicator .....	4-305
DE 94—Service Indicator.....	4-306
Subfield 1—Reserved for Future Use .....	4-306
Subfield 2—Acquirer/Issuer Indicator.....	4-307
Subfield 3—Address Data Indicator .....	4-307
DE 95—Replacement Amounts.....	4-308
Subfield 1—Actual Amount, Transaction .....	4-309
Subfield 2—Actual Amount, Settlement .....	4-310
Subfield 3—Actual Amount, Cardholder Billing.....	4-310
Subfield 4—Zero Fill.....	4-310
DE 96—Message Security Code .....	4-311
DE 97—Amount, Net Settlement.....	4-311
Subfield 1—Debit/Credit Indicator .....	4-312
Subfield 2—Amount.....	4-312
DE 98—Payee .....	4-312
DE 99—Settlement Institution ID Code .....	4-313
DE 100—Receiving Institution ID Code .....	4-313
DE 101—File Name .....	4-314
DE 102—Account ID 1 .....	4-315

---

DE 103—Account ID 2 .....	4-316
DE 104—Transaction Description .....	4-317
DE 105—DE 111—Reserved for Future Use .....	4-317
DE 112—Additional Data, National Use .....	4-317
DE 112—Encoding Scheme .....	4-318
Cuotas—Payment Transactions .....	4-319
Subelement 001—Installment Payment Data .....	4-319
Subelement 003—Installment Payment Response Data .....	4-321
Subelement 027—ATM Credit Card Cash Advance Installments .....	4-322
Subfield 1—Transaction Type .....	4-322
Subfield 2—Requested Number of Installments .....	4-323
Subfield 3—Approved Number of Installments .....	4-323
Subfield 4—Installment Amount .....	4-323
Subfield 5—Total Transaction Amount .....	4-324
Subfield 6—Yearly Interest Rate .....	4-324
Subfield 7—Currency Code .....	4-324
Subfield 8—Member-defined Data .....	4-325
Subfield 9—Member-defined Data .....	4-325
Mexcta—PaymentTransactions .....	4-325
Subelement 004—Credit Line Usage Fee (CLUF) .....	4-325
Subelement 005—Issuing Bank Name (AKA Doing Business As [DBA]) .....	4-326
Subelement 006—Financial Institution ID (FIID) .....	4-326
Subelement 007—Installment Payment Data .....	4-327
Subelement 008—Installment Payment Response Data .....	4-328
Parcelas—Payment Transactions .....	4-328
Subelement 001—Installment Payment Data .....	4-329
Subelement 002—Installment Payment Response Data .....	4-329
Percta—Payment Transactions .....	4-330
Subelement 007—Installment Payment Data .....	4-330
Subelement 008—Installment Payment Response Data .....	4-331
Philippines—Payment Transactions .....	4-332
Subelement 009—Installment Payment Data .....	4-332
UK Domestic Maestro Transactions .....	4-333
Subelement 001—Reason Online Code .....	4-333
Subelement 002—Retailer Classification Code .....	4-334
DE 113—Reserved for National Use .....	4-335
Generic Data, Administrative Request/0600 Message .....	4-336
Banking Data, Administrative Request/0600 Message .....	4-338

## Data Element Definitions

---

DE 114—Reserved for National Use .....	4-338
Consumer Application Request Data Administrative Request/0600 Message .....	4-339
Consumer Status Inquiry or Preapproved Offer Inquiry Data Administrative Request/0600 Message .....	4-341
Consumer Account Maintenance Data Administrative Request/0600 Message .....	4-342
Consumer Application Response Data Administrative Request Response/0610 Message .....	4-345
Consumer Account Maintenance Data Administrative Request Response/0610 Message .....	4-347
DE 115—Reserved for National Use .....	4-351
Business Application Request Data Administrative Request/0600 Message .....	4-352
Business Application Status Inquiry Data or Business Preapproved Offer Inquiry Data Administrative Request/0600 Message .....	4-354
Business Account Maintenance Data Administrative Request/0600 Message .....	4-354
Business Application Response Data Administrative Request Response/0610 Message .....	4-357
Business Account Maintenance Data Administrative Request Response/0610 Message .....	4-359
DE 116—Reserved For National Use .....	4-364
Consumer User Lookup Inquiry Data Administrative Request/0600 .....	4-365
Consumer Account Lookup Inquiry Data Administrative Request/0600 Message .....	4-365
Consumer Account Lookup Response Data Administrative Request Response/0610 Message .....	4-366
DE 117—Reserved for National Use .....	4-368
Business User Lookup Inquiry Data Administrative Request/0600 Message .....	4-369
Business Account Lookup Inquiry Data Administrative Request/0600 Message .....	4-369
Business Account Lookup Response Data Administrative Request Response/0610 Message .....	4-370
DE 118—Reserved for National Use .....	4-372
Authorized User Data Administrative Request/0600 Message .....	4-373
Trade Reference Data Administrative Request/0600 Message .....	4-373
Authorized User Response Data Administrative Request Response/0610 Message .....	4-374
DE 119—Reserved for National Use .....	4-375
Using DE 113–119 in Administrative 06xx Messages .....	4-376
DE 120—Record Data .....	4-379
Subfield 01—AVS Service Indicator 1 .....	4-380
Subfield 02—AVS Service Indicator 2 .....	4-380
Subfield 03—AVS Service Indicator 3 .....	4-381
Subfield 04—AVS Service Indicator 4 .....	4-382
Online File Maintenance .....	4-382

---

MCC102—Stand-In Account File.....	4-383
MCC103—Electronic Warning Bulletin File.....	4-385
MCC104—Local Stoplist File .....	4-387
MCC105—Recurring Payment Cancellation Service File .....	4-391
DE 120 When Blocking Recurring Payments.....	4-392
MCC106—PAN Mapping File .....	4-393
MCC107—Enhanced Value File.....	4-395
MCC108—Product Graduation File .....	4-398
MCC109— <i>PayPass</i> Application Transaction Counter File .....	4-400
DE 120 Error Codes .....	4-402
MCC102 Error Codes.....	4-402
MCC103 Error Codes.....	4-402
MCC104 Error Codes.....	4-403
MCC105 Error Codes.....	4-404
MCC106 Error Codes.....	4-405
MCC107 Error Codes.....	4-407
MCC108 Error Codes.....	4-408
MCC109 Error Codes.....	4-410
DE 121—Authorizing Agent ID Code .....	4-411
DE 122—Additional Record Data.....	4-412
DE 123—Receipt Free Text.....	4-413
DE 124—Member-defined Data .....	4-414
DE 124—Member-defined Data (General Use).....	4-414
DE 124—Member-defined Data ( <i>MoneySend</i> Only) .....	4-416
DE 124—Member-defined Data (Brazil Maestro Only).....	4-416
Subfield 1—Unique Reference Number.....	4-416
Subfield 2—Sender/Payer/User ID .....	4-417
Subfield 3—Sender/Payer Address .....	4-417
Subfield 4—Reserved For Future Use .....	4-418
Subfield 6—Discretionary Message on Sales Slip Supported .....	4-418
Subfield 7—Discretionary Message on Sales Slip Code .....	4-419
Subfield 8—Discretionary Message on Sales Slip Content .....	4-419
Subfield 9—Phoneshop (Phone Company ID) .....	4-419
Subfield 10—Phoneshop (Cell Phone Number) .....	4-420
Subfield 11—Phoneshop (Message Security Code) .....	4-420
Subfield 12—Merchant CNPJ Number .....	4-420
Subfield 13—Total Annual Effective Cost .....	4-421
DE 125—New PIN Data.....	4-421

## **Data Element Definitions**

---

DE 126—Private Data .....	4-422
DE 127—Private Data .....	4-422
DE 128—Message Authentication Code.....	4-424

## Data Element Layout

Following is the data element structure for describing data elements. Value and Application Note information is omitted from the data element attributes of those data elements not currently used in Authorization Platform messages.

Attribute	Description
Length of Length Field:	2 or 3 if variable in length
Data Representation:	Annotation and data length (fixed or variable in length)
Data Field:	Contents of subelement, subfields or N/A
Subfields:	Indicates number of subelements, subfields or N/A
Justification:	Left, Right, or N/A
<b>Usage</b>	
Following is the usage of DE xx (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:	Org      Sys      Dst
Message types applicable and the entities involved in the message.	•      •      •
<b>Values</b>	
Valid values and name of each value listed.	
<b>Application Notes</b>	
Specific application notes, conditions, and cross-edits where applicable.	

## Subelement Layout

Following is the subelement structure for describing data element subelements.

Attribute	Description
Subelement ID:	Subelement identifier
Length of Length Field:	2 or 3 if variable in length
Data Representation:	Annotation and data length (fixed or variable in length)
Data Field:	Contents of subfields
Subfields:	Indicates number of subfields
Justification:	See "Subfields" (may be subfield specific)
<b>Usage</b>	

## Data Element Definitions

### Subfield Layout

---

Following is the usage of subelement XX (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Org	Sys	Dst
-----	-----	-----

List of message types that use this data element and usage.

•	•	•
---	---	---

#### Values

---

The list of subelement values or see subfields.

---

## Subfield Layout

Following is the subfield structure for describing data element and subelement subfields. Subfield ID and Length of Length Field are omitted from the subfield attributes when subfield ID and length are not included in the data.

Attribute	Description
Subfield ID:	Subfield identifier (omitted if not part of the data)
Length of Length Field:	2 if variable in length (omitted if not part of the data)
Data Representation:	Annotation and data length (fixed or variable in length)
Data Field:	Contents of position(s)
Justification:	Left, Right, or N/A (justification is not used in describing subelement subfields)

#### Values

---

Valid values and name of each value listed.

---

## Position Layout

Following is the position structure for describing subelement and subfield positions.

Data Representation:	Annotation and data length (fixed or variable in length)
Data Field:	Description of Data
Values:	List of values

## List of Data Elements (Numeric Order)

Following is a the list of data elements in numeric order.

**Data Element Definitions**  
**List of Data Elements (Numeric Order)**

---

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
1	Bit Map, Secondary	b-8
2	Primary Account Number (PAN)	n...19; LLVAR
3	Processing Code	n-6
4	Amount, Transaction	n-12
5	Amount, Settlement	n-12
6	Amount, Cardholder Billing	n-12
7	Transmission Date and Time	n-10
8	Amount, Cardholder Billing Fee <sup>1</sup>	n-8
9	Conversion Rate, Settlement	n-8
10	Conversion Rate, Cardholder Billing	n-8
11	Systems Trace Audit Number	n-6
12	Time, Local Transaction	n-6
13	Date, Local Transaction	n-4
14	Date, Expiration	n-4
15	Date, Settlement	n-4
16	Date, Conversion	n-4
17	Date, Capture <sup>1</sup>	n-4
18	Merchant Type	n-4
19	Acquiring Institution Country Code <sup>1</sup>	n-3
20	Primary Account Number (PAN) Country Code	n-3
21	Forwarding Institution Country Code <sup>1</sup>	n-3
22	Point-of-Service (POS) Entry Mode	n-3
23	Card Sequence Number	n-3
24	Network International ID <sup>1</sup>	n-3
25	Point-of-Service (POS) Condition Code <sup>1</sup>	n-2
26	Point-of-Service (POS) Personal ID Number (PIN) Capture Code	n-2
27	Authorization ID Response Length <sup>1</sup>	n-1

- 
1. MasterCard currently does not use this data element and it should not be included in an authorization message. A program or service may use it at a later date.

## Data Element Definitions

### List of Data Elements (Numeric Order)

Number	Name	Data Representation
28	Amount, Transaction Fee	an-9
29	Amount, Settlement Fee <sup>1</sup>	an-9
30	Amount, Transaction Processing Fee <sup>1</sup>	an-9
31	Amount, Settlement Processing Fee <sup>1</sup>	an-9
32	Acquiring Institution ID Code	n...6; LLVAR
33	Forwarding Institution ID Code	n...6; LLVAR
34	Primary Account Number (PAN), Extended <sup>1</sup>	ans...28; LLVAR
35	Track 2 Data	ans...37; LLVAR
36	Track 3 Data <sup>1</sup>	ans...104; LLVAR
37	Retrieval Reference Number	an-12
38	Authorization ID Response	ans-6
39	Response Code	an-2
40	Service Restriction Code <sup>1</sup>	an-3
41	Card Acceptor Terminal ID	ans-8
42	Card Acceptor ID Code	ans-15
43	Card Acceptor Name/Location	ans-40
44	Additional Response Data	ans...25; LLVAR
45	Track 1 Data	ans...76; LLVAR
46	Additional Data—ISO Use <sup>1</sup>	ans...999; LLVAR
47	Additional Data—National Use <sup>2</sup>	ans...999; LLVAR
48	Additional Data—Private Use This data element is an ISO-designated “private use” data element redefined by MasterCard in accordance with provisions of the ISO 8583–1987 specification.	ans...999; LLVAR
49	Currency Code, Transaction	n-3
50	Currency Code, Settlement	n-3
51	Currency Code, Cardholder Billing	n-3
52	Personal ID Number (PIN) Data	b-8

2. This data element is reserved for national use. The Authorization Platform does not perform any processing on this data element. However, if it is included in an authorization message, the network will pass it from the originator to the receiver, provided that both the originator and the receiver are customers of the same national standards organizations.

**Data Element Definitions**  
**List of Data Elements (Numeric Order)**

---

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
53	Security-Related Control Information	n-16
54	Additional Amounts	an...120; LLVAR
55	Integrated Circuit Card (ICC) System-Related Data	b...255; LLVAR
56	Reserved for ISO Use <sup>1</sup>	ans...999; LLVAR
57-59	Reserved for National Use <sup>2</sup>	ans...999; LLVAR
60	Advice Reason Code <sup>3</sup>	ans...060; LLVAR
61	Point-of-Service (POS) Data <sup>3</sup>	an...026; LLVAR
62	Intermediate Network Facility (INF) Data <sup>3</sup>	ans...100; LLVAR
63	Network Data <sup>3</sup>	an...050; LLVAR
64	Message Authentication Code (MAC) <sup>1</sup>	b-8
65	Bit Map, Extended <sup>1</sup>	b-8
66	Settlement Code <sup>1</sup>	n-1
67	Extended Payment Code <sup>1</sup>	n-2
68	Receiving Institution Country Code <sup>1</sup>	n-3
69	Settlement Institution Country Code <sup>1</sup>	n-3
70	Network Management Information Code	n-3
71	Message Number <sup>1</sup>	n-4
72	Message Number Last <sup>1</sup>	n-4
73	Date, Action	n-6;
74	Credits, Number <sup>1</sup>	n-10
75	Credits, Reversal Number <sup>1</sup>	n-10
76	Debits, Number <sup>1</sup>	n-10
77	Debits, Reversal Number <sup>1</sup>	n-10
78	Transfers, Number <sup>1</sup>	n-10
79	Transfers, Reversal Number <sup>1</sup>	n-10
80	Inquiries, Number <sup>1</sup>	n-10
81	Authorizations, Number <sup>1</sup>	n-10
82	Credits, Processing Fee Amount <sup>1</sup>	n-12

## Data Element Definitions

### List of Data Elements (Numeric Order)

Number	Name	Data Representation
83	Credits, Transaction Fee Amount <sup>1</sup>	n-12
84	Debits, Processing Fee Amount <sup>1</sup>	n-12
85	Debits, Transaction Fee Amount <sup>1</sup>	n-12
86	Credits, Amount <sup>1</sup>	n-16
87	Credits, Reversal Amount <sup>1</sup>	n-16
88	Debits, Amount <sup>1</sup>	n-16
89	Debits, Reversal Amount <sup>1</sup>	n-16
90	Original Data Elements	n-42
91	Issuer File Update Code	an-1
92	File Security Code <sup>1</sup>	an-2
93	Response Indicator <sup>1</sup>	an-5
94	Service Indicator	an-7
95	Replacement Amounts	n-42
96	Message Security Code <sup>3</sup>	b-8
97	Amount, Net Settlement <sup>1</sup>	an-17
98	Payee <sup>1</sup>	ans-25
99	Settlement Institution ID Code <sup>1</sup>	n...11; LLVAR
100	Receiving Institution ID Code	n...11; LLVAR
101	File Name	ans...17; LLVAR
102	Account ID-1	ans...28; LLVAR
103	Account ID-2	ans...28; LLVAR
104	Transaction Description <sup>1</sup>	ans...100; LLLVAR
105–111	Reserved for ISO Use <sup>1</sup>	ans...999; LLLVAR
112	Additional Data—National Use	ans...100; LLLVAR
113–119	Reserved for National Use <sup>2</sup>	ans...999; LLLVAR
120	Record Data <sup>3</sup>	ans...999; LLLVAR
121	Authorizing Agent ID Code <sup>3</sup>	n...6; LLVAR

3. Although this data element is designated as binary, it also may contain up to eight bytes of EBCDIC encoded data.

**Data Element Definitions**  
**List of Data Elements (Alphabetic Order)**

---

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
122	Additional Record Data <sup>3</sup>	ans...999; LLLVAR
123	Receipt Free Text	ans...512; LLLVAR
124	Member-defined Data	ans...199; LLLVAR
125	New PIN Data	b-8
126	Private Data	ans...100; LLLVAR
127	Private Data <sup>3</sup>	ans...100; LLLVAR
128	Message Authentication Code (MAC) <sup>1</sup>	b-8

## **List of Data Elements (Alphabetic Order)**

Following is the list of data elements in alphabetic order.

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
102	Account ID-1	ans...28; LLVAR
103	Account ID-2	ans...28; LLVAR
19	Acquiring Institution Country Code <sup>4</sup>	n-3
32	Acquiring Institution ID Code	n...6; LLVAR
54	Additional Amounts	an...120; LLLVAR
46	Additional Data—ISO Use <sup>4</sup>	ans...999; LLLVAR
47	Additional Data—National Use <sup>5</sup>	ans...999; LLLVAR
112	Additional Data—National Use	ans...100; LLLVAR
48	Additional Data—Private Use <sup>6</sup>	ans...999; LLLVAR
122	Additional Record Data <sup>6</sup>	ans...999; LLLVAR
44	Additional Response Data	ans...25; LLVAR
60	Advice Reason Code <sup>6</sup>	ans...060; LLLVAR
6	Amount, Cardholder Billing	n-12

- 4. MasterCard currently does not use this data element and it should not be included in an authorization message. A program or service may use it at a later date.
- 5. This data element is reserved for national use. The Authorization Platform does not perform any processing on this data element. However, if it is included in an authorization message, the network passes it from the originator to the receiver, provided that both the originator and the receiver are customers of the same national standards organizations.
- 6. This data element is an ISO-designated “private use” data element redefined by MasterCard in accordance with provisions of the ISO 8583-1987 specification.

## Data Element Definitions

### List of Data Elements (Alphabetic Order)

---

Number	Name	Data Representation
8	Amount, Cardholder Billing Fee <sup>4</sup>	n-8
97	Amount, Net Settlement <sup>4</sup>	an-17
5	Amount, Settlement	n-12
29	Amount, Settlement Fee <sup>4</sup>	an-9
31	Amount, Settlement Processing Fee <sup>4</sup>	an-9
4	Amount, Transaction	n-12
28	Amount, Transaction Fee	an-9
30	Amount, Transaction Processing Fee <sup>4</sup>	an-9
38	Authorization ID Response	ans-6
27	Authorization ID Response Length <sup>4</sup>	n-1
81	Authorizations, Number <sup>4</sup>	n-10
121	Authorizing Agent ID Code <sup>6</sup>	n...6; LLLVAR
65	Bit Map, Extended <sup>4</sup>	b-8
1	Bit Map, Secondary	b-8
42	Card Acceptor ID Code	ans-15
43	Card Acceptor Name/Location	ans-40
41	Card Acceptor Terminal ID	ans-8
23	Card Sequence Number	n-3
10	Conversion Rate, Cardholder Billing	n-8
9	Conversion Rate, Settlement	n-8
86	Credits, Amount <sup>4</sup>	n-16
74	Credits, Number <sup>4</sup>	n-10
82	Credits, Processing Fee Amount <sup>4</sup>	n-12
87	Credits, Reversal Amount <sup>4</sup>	n-16
75	Credits, Reversal Number <sup>4</sup>	n-10
83	Credits, Transaction Fee Amount <sup>4</sup>	n-12
51	Currency Code, Cardholder Billing	n-3
50	Currency Code, Settlement	n-3
49	Currency Code, Transaction	n-3

**Data Element Definitions**  
**List of Data Elements (Alphabetic Order)**

---

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
73	Date, Action	n-6;
17	Date, Capture <sup>4</sup>	n-4
16	Date, Conversion	n-4
14	Date, Expiration	n-4
13	Date, Local Transaction	n-4
15	Date, Settlement	n-4
88	Debits, Amount <sup>4</sup>	n-16
76	Debits, Number <sup>4</sup>	n-10
84	Debits, Processing Fee Amount <sup>4</sup>	n-12
89	Debits, Reversal Amount <sup>4</sup>	n-16
77	Debits, Reversal Number <sup>4</sup>	n-10
85	Debits, Transaction Fee Amount <sup>4</sup>	n-12
67	Extended Payment Code <sup>4</sup>	n-2
101	File Name	ans...17; LLVAR
92	File Security Code <sup>4</sup>	an-2
21	Forwarding Institution Country Code <sup>4</sup>	n-3
33	Forwarding Institution ID Code	n...6; LLVAR
80	Inquiries, Number <sup>4</sup>	n-10
55	Integrated Circuit Card (ICC) System-Related Data	b...255; LLLVAR
62	Intermediate Network Facility (INF) Data <sup>6</sup>	ans...100; LLLVAR
91	Issuer File Update Code	an-1
124	Member-defined Data	ans...199; LLLVAR
18	Merchant Type	n-4
64	Message Authentication Code (MAC) <sup>4</sup>	b-8
128	Message Authentication Code (MAC) <sup>4</sup>	b-8
71	Message Number <sup>4</sup>	n-4
72	Message Number Last <sup>4</sup>	n-4

## Data Element Definitions

### List of Data Elements (Alphabetic Order)

Number	Name	Data Representation
96	Message Security Code <sup>7</sup> .	b-8
63	Network Data <sup>6</sup>	an...050; LLLVAR
24	Network International ID <sup>4</sup>	n-3
70	Network Management Information Code	n-3
125	New PIN Data	b-8
90	Original Data Elements	n-42
98	Payee <sup>4</sup>	ans-25
52	Personal ID Number (PIN) Data	b-8
25	Point-of-Service (POS) Condition Code <sup>4</sup>	n-2
61	Point-of-Service (POS) Data <sup>6</sup>	an...026; LLLVAR
22	Point-of-Service (POS) Entry Mode	n-3
26	Point-of-Service (POS) Personal ID Number (PIN) Capture Code	n-2
2	Primary Account Number (PAN)	n...19; LLLVAR
20	Primary Account Number (PAN) Country Code	n-3
34	Primary Account Number (PAN), Extended <sup>4</sup>	ans...28; LLLVAR
126	Private Data	ans...100; LLLVAR
127	Private Data <sup>6</sup>	ans...100; LLLVAR
3	Processing Code	n-6
123	Receipt Free Text	ans...512; LLLVAR
68	Receiving Institution Country Code <sup>4</sup>	n-3
100	Receiving Institution ID Code	n...11; LLLVAR
120	Record Data <sup>6</sup>	ans...999; LLLVAR
95	Replacement Amounts	n-42
56	Reserved for ISO Use	ans...999; LLLVAR
105–111	Reserved for ISO Use <sup>4</sup>	ans...999; LLLVAR
57–59	Reserved for National Use <sup>5</sup>	ans...999; LLLVAR
113–119	Reserved for National Use <sup>5</sup>	ans...999; LLLVAR

7. Although this data element is designated as binary, it also may contain up to eight bytes of EBCDIC encoded data

Number	Name	Data Representation
39	Response Code	an-2
93	Response Indicator <sup>4</sup>	an-5
37	Retrieval Reference Number	an-12
53	Security-Related Control Information	n-16
94	Service Indicator	an-7
40	Service Restriction Code <sup>4</sup>	an-3
66	Settlement Code <sup>4</sup>	n-1
69	Settlement Institution Country Code <sup>4</sup>	n-3
99	Settlement Institution ID Code <sup>4</sup>	n...11; LLVAR
11	Systems Trace Audit Number	n-6
12	Time, Local Transaction	n-6
45	Track 1 Data	ans...76; LLVAR
35	Track 2 Data	ans...37; LLVAR
36	Track 3 Data <sup>4</sup>	ans...104; LLLVAR
104	Transaction Description <sup>4</sup>	ans...100; LLLVAR
78	Transfers, Number <sup>4</sup>	n-10
79	Transfers, Reversal Number <sup>4</sup>	n-10
7	Transmission Date and Time	n-10

## Message Type Identifier

The Message Type Identifier (MTI) is a four-digit numeric data element describing the type of message being interpreted. The MTI is required and must be present as the first data element of each Authorization Platform message.

---

### Attributes

---

Length of Length Field:	N/A
Data Representation:	n-4
Data Field:	Contents of positions 1-4
Subfields:	N/A
Justification:	N/A

## Data Element Definitions

### Message Type Identifier

---

Usage	M	•	M
Authorization Request/0100	M	•	M
Authorization Request Response/0110	M	•	M
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	M	•	M
Authorization Advice Response/0130—Issuer-generated	M	M	•
Authorization Advice Response/0130—System-generated	•	M	M
Authorization Acknowledgement/0180	M	M	•
Authorization Negative Acknowledgement/0190	•	M	M
Issuer File Update Request/0302	M	M	•
Issuer File Update Request Response/0312	•	M	M
Reversal Request/0400	M	•	M
Reversal Request Response/0410	M	•	M
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	M	M	•
Administrative Request/0600	M	•	M
Administrative Request Response/0610	M	•	M
Administrative Advice/0620	•	M	M
Administrative Advice Response/0630	M	M	•
Network Management Request/0800—Sign-On/Sign-Off	M	M	•
Network Management Request/0800—RiskFinder SAF Request	M	M	•
Network Management Request/0800—Host Session Activation/Deactivation	M	M	•
Network Management Request/0800—Network Connection Status, System-generated	•	M	M
Network Management Request/0800—Network Connection Status, Member-generated	M	M	•
Network Management Request/0800—PEK Exchange	•	M	M

**Data Element Definitions****Message Type Identifier**

Network Management Request/0800—PEK Exchange—On Demand	M	M	•
Network Management Request Response/0810—Sign-On/Sign-Off	•	M	M
Network Management Request Response/0810—RiskFinder SAF Request	•	M	M
Network Management Request Response/0810—Host Session Activation/Deactivation	•	M	M
Network Management Request Response/0810—Network Connection Status, System-generated	•	M	M
Network Management Request Response/0810—Network Connection Status, Member-generated	M	M	•
Network Management Request Response/0810—PEK Exchange	M	M	•
Network Management Request Response/0810—PEK Exchange—On Demand	•	M	M
Network Management Advice/0820—RiskFinder SAF End of File	•	M	M
Network Management Advice/0820—PEK Exchange	•	M	M

**Values**

## Position 1—Version Number

0 = ISO 8583: 1987

1 = ISO 8583: 1992

2-7 = Reserved for ISO use

8 = Reserved for national use

9 = Reserved for future use

## Position 2—Message Class

0 = Reserved for ISO use

1 = Authorization

2 = Financial

3 = File action

4 = Reversal/chargeback

5 = Reconciliation

6 = Administrative

7 = Fee collection

## Data Element Definitions

### Message Types and Applicable Program or Service

8	=	Network management
9	=	Reserved for ISO use
Position 3—Message Function		
0	=	Request
1	=	Request response
2	=	Advice
3	=	Advice response
4	=	Notification
5-9	=	Reserved for ISO use
Position 4—Transaction Originator		
0	=	Acquirer
1	=	Acquirer repeat
2	=	Card issuer
3	=	Card issuer repeat
4	=	Other
5	=	Other repeat
6-9	=	Reserved for ISO use

## Message Types and Applicable Program or Service

The following table specifies the permissible MTI values that may be used within each individual Authorization Platform message. The table key at the end of the table describes the symbols used under program and service columns.

MTI	Description	MC	NP	VI	TE	MS	CI
0100	Authorization Request	✓	✓	✓	✓	✓	✓
0110	Authorization Request Response	✓	✓	✓	✓	✓	✓
0120	Authorization Advice—Acquirer-generated	✓	✓	•	•	✓	✓
0120	Authorization Advice—Issuer-generated	✓	✓	✓	✓	✓	✓
0120	Authorization Advice—System-generated	✓	✓	✓	✓	✓	✓
0130	Authorization Advice Response—Issuer-generated	✓	✓	✓	✓	✓	✓
0130	Authorization Advice Response—System-generated	✓	✓	✓	✓	✓	✓

**Data Element Definitions**  
**About Primary and Secondary Bit Maps**

---

<b>MTI</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
0180	Authorization Acknowledgement	o	o	o	o	o	o
0190	Authorization Negative Acknowledgement	✓	✓	✓	✓	✓	✓
0302	Issuer File Update Request	✓	✓	•	•	✓	✓
0312	Issuer File Update Request Response	✓	✓	•	•	✓	✓
0400	Reversal Request/0400	✓	✓	✓	•	✓	✓
0410	Reversal Request Response/0410	✓	✓	✓	•	✓	✓
0420	Reversal Advice	✓	✓	✓	•	✓	✓
0430	Reversal Advice Response	✓	✓	✓	•	✓	✓
0600	Administrative Request/0600	✓	✓	•	•	•	•
0610	Administrative Request Response/0610	✓	✓	•	•	•	•
0620	Administrative Advice	✓	✓	✓	•	✓	✓
0630	Administrative Advice Response	✓	✓	✓	•	✓	✓
0800	Network Management Request	✓	✓	✓	✓	✓	✓
0810	Network Management Request Response	✓	✓	✓	✓	✓	✓
0820	Network Management Advice	✓	✓	✓	✓	✓	✓

Table Key:

✓ = The MTI must be provided for the program or service indicated.

O = Optional support (for example, when individual MasterCard customers may elect to support or not support certain message types at their own discretion).

• = The MTI is unavailable for the program or service.

---

## About Primary and Secondary Bit Maps

All Authorization Platform messages consists of one or two “bit maps,” each consisting of 64 bits. Bits are numbered from the left, starting with one. The first bit map contains bits one through 64; the second bit map contains bits 65 through 128.

A bit map is a series of 64 bits used to identify the presence or absence (denoted by 1 or 0) of each data element. The bit map is interpreted from left to right. The left-most bit represents bit number 1 in the Primary Bit Map and bit number 65 in the Secondary Bit Map. The rightmost bit represents bit number 64 in the Primary Bit Map and bit number 128 in the Secondary Bit Map.

## Data Element Definitions

### Primary Bit Map

---

Additional bit maps can be accommodated in the ISO 8583-1987 specification by using additional “Bit Maps, Extended” (setting the first bit in any bit map to 1 indicating the presence of a following “extended” bit map). However, MasterCard currently uses a maximum of two-bit maps (primary and secondary) in Authorization Platform messages, with a maximum number of message data elements ranging from DE 1 through DE 128. Consequently, DE 65 (the first bit in the Secondary Bit Map) must always be 0.

## Primary Bit Map

The Primary Bit Map must always be present in a message. The most frequently used data elements are indexed from DE 1 (Bit Map, Secondary) through DE 64 (Message Authentication Code [MAC]). Infrequently used data elements are indexed from the DE 66 (Settlement Code) through DE 128 (Message Authentication Code [MAC]).

---

### Attributes

---

Length of Length Field:	N/A
Data Representation:	b-8
Data Field:	Fixed length 8 bytes (for each bit map)
Subfields:	N/A
Justification:	N/A

---

If both bit maps are present, the total length of the bit map data element is 16 bytes.

---

### Usage

---

Following is the usage of Bit Map, Primary (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M
Authorization Request Response/0110	M	•	M
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	M	M	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	M	•	M
Authorization Advice Response/0130—System-generated	•	M	M
Authorization Acknowledgement/0180	M	M	•

**Data Element Definitions****Primary Bit Map**

Authorization Negative Acknowledgement/0190	•	M	M
Issuer File Update Request/0302	M	M	•
Issuer File Update Request Response/0312	•	M	M
Reversal Request/0400	M	•	M
Reversal Request Response/0410	M	•	M
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	M	M	•
Administrative Request/0600	M	•	M
Administrative Request Response/0610	M	•	M
Administrative Advice/0620	•	M	M
Administrative Advice Response/0630	M	M	•
Network Management Request/0800—Sign-On/Sign-Off	M	M	•
Network Management Request/0800—RiskFinder SAF Request	M	M	•
Network Management Request/0800—Network Connection Status, System-generated	•	M	M
Network Management Request/0800—Network Connection Status, Member-generated	M	M	•
Network Management Request/0800—Host Session Activation/Deactivation	•	M	M
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request/0800—PEK Exchange-On Demand	M	M	•
Network Management Request Response/0810—Sign-On/Sign-Off	•	M	M
Network Management Request Response/0810—RiskFinder SAF Request	•	M	M
Network Management Request Response/0810—Host Session Activation/Deactivation	•	ME	ME
Network Management Request Response/0810—Network Connection Status, System-generated	•	M	M
Network Management Request Response/0810—Network Connection Status, Member-generated	M	M	•
Network Management Request Response/0810—PEK Exchange	M	M	•

## Data Element Definitions

### DE 1—Bit Map, Secondary

Network Management Request Response/0810—PEK Exchange—On Demand	•	M	M
---	---	---	---

Network Management Advice/0820—RiskFinder SAF End of File	•	M	M
---	---	---	---

Network Management Advice/0820—PEK Exchange	•	M	M
---	---	---	---

#### Values

Bits corresponding to mandatory data elements for a specific MTI must have a value of 1 to indicate the presence of the data element in the message. Otherwise, the Authorization Platform rejects the message and returns it to the message initiator using an Administrative Advice/0620, with the “reject reason” indicated in DE 60 (Advice Reason Code).

#### Application Notes

This data element is defined and used identically within all MasterCard programs and services.

## DE 1—Bit Map, Secondary

DE 1 (Bit Map, Secondary) is a series of 64 bits that identifies the presence (1) or absence (0) of each data element in the second segment of a message. This would include DE 65 (Bit Map, Extended) through DE 128 (Message Authentication Code [MAC]).

#### Attributes

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	b-8
----------------------	-----

Data Field:	Indicates the presence or absence of data elements 65–128
-------------	---

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

#### Usage

Following is the usage of DE 1 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•

**Data Element Definitions****DE 1—Bit Map, Secondary**

Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	C	C	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	C	•	C
Authorization Advice Response/0130—System-generated	•	C	C
Authorization Acknowledgement/0180	C	C	•
Authorization Negative Acknowledgement/0190	•	C	C
Issuer File Update Request/0302	M	M	•
Issuer File Update Request Response/0312	•	M	M
Reversal Request/0400	M	•	M
Reversal Request Response/0410	M	•	M
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	M	M	•
Administrative Request/0600	M	•	M
Administrative Request Response/0610	M	•	M
Administrative Advice/0620	•	M	M
Administrative Advice Response/0630	M	M	•
Network Management Request/0800—Sign-On/Sign-Off	M	M	•
Network Management Request/0800—RiskFinder SAF Request	M	M	•
Network Management Request/0800—Host Session Activation/Deactivation	M	M	•
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request/0800—PEK Exchange—On Demand	M	M	•
Network Management Request/0800—Network Connection Status, Member-generated	M	M	•
Network Management Request/0800—Network Connection Status, System-generated	•	M	M
Network Management Request Response/0810—Sign-On/Sign-Off	•	M	M
Network Management Request Response/0810—RiskFinder SAF Request	•	M	M
Network Management Request Response/0810—Host Session Activation/Deactivation	•	M	M

## Data Element Definitions

### DE 2—Primary Account Number (PAN)

Network Management Request Response/0810—PEK Exchange	M	M	•
Network Management Request Response/0810—PEK Exchange—On Demand	•	M	M
Network Management Request Response/0810—Network Connection Status, Member-generated	M	M	•
Network Management Request Response/0810—Network Connection Status, System-generated	•	M	M
Network Management Advice/0820—RiskFinder SAF End of File	•	M	M
Network Management Advice/0820—PEK Exchange	•	M	M

#### Values

Bits corresponding to mandatory data elements for a specific MTI must have a value of 1 to indicate the presence of the data element in the message. Otherwise, the Authorization Platform rejects the message and returns it to the message initiator using an Administrative Advice/0620, with the “reject reason” indicated in DE 60 (Advice Reason Code).

#### Application Notes

This data element is defined and used identically within all MasterCard programs and services.

## DE 2—Primary Account Number (PAN)

DE 2 (Primary Account Number [PAN]) is a series of digits used to identify a customer account or relationship.

#### Attributes

Length of Length Field: 2

Data Representation: n...19; LLVAR

Data Field: Contents of positions 1–19

Subfields: N/A

Justification: N/A

#### Usage

Following is the usage of DE 2 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M

**Data Element Definitions**  
**DE 2—Primary Account Number (PAN)**

---

Authorization Request Response/0110	ME	•	ME
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	ME	ME
Issuer File Update Request/0302	C	C	•
Issuer File Update Request Response/0312	•	CE	CE
Reversal Request/0400	M	•	M
Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•
Administrative Request/0600	M	•	M
Administrative Request Response/0610	ME	•	ME
Network Management Request/0800—Sign-On/Sign-Off	M	M	•
Network Management Request/0800—Network Connection Status, Member-generated	M	M	•
Network Management Request/0800—Network Connection Status, System-generated	•	M	M
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request/0800—PEK Exchange—On Demand	M	M	•
Network Management Request/0800—Host Session Activation/Deactivation	M	M	•
Network Management Request Response/0810—Network Connection Status, System-generated	•	ME	ME
Network Management Request Response/0810—Network Connection Status, Member-generated	ME	ME	•
Network Management Request Response/0810—Host Session Activation/Deactivation	•	ME	ME
Network Management Advice/0820—PEK Exchange	•	M	M
Network Management Request Response/0810—PEK Exchange	ME	M	•

## Data Element Definitions

### DE 2—Primary Account Number (PAN)

---

Network Management Request Response/0810—PEK  
Exchange—On Demand

• ME ME

#### Values

All PANs and card prefixes used in Authorization Platform messages must conform to the standard PAN encoding requirements as documented in the ISO 7812 and 7813 specifications.

MasterCard customer ID numbers, when used in this data element, must be valid values that MasterCard assigns.

DE 2 must be at least 11 digits and contain the variable-length prefix assigned to the specific Issuer ID Number (IIN) for Administrative Request/0600 messages.

Network Management Request/0800 messages may contain the MasterCard Group Sign-on ID only, the card prefix only, or both the MasterCard Group Sign-on ID followed by the card prefix in DE 2.

#### Application Notes

This data element is defined and used identically within all MasterCard programs and services.

## About Primary Account Number

DE 2 (Primary Account Number [PAN]) is a series of digits used to identify a customer account or relationship.

### **Primary Account Number**

This data element is used for all numeric PANs up to 19 digits long when PAN is in Authorization/01xx messages, Reversal Advice/04xx messages, and Administrative Advice/06xx messages (when required). DE 2 may contain a subset of this data within Network Management/08xx messages.

This data element data consists of three primary components:

- Issuing Institution Information (IIN)
- Individual Account ID Number
- PAN check digit

When DE 2 contains a 59 BIN, DE 20 (Primary Account Number Country Code) **also must be included in the message to uniquely identify the PAN**. Note that 59 numbers are not guaranteed to be unique without an accompanying Country Code.

Specific requirements for PAN composition are described in the ISO 7812 and 7813 specifications. **All PANs used in Authorization Platform messages must conform to the ISO PAN encoding requirements, as specified in those specifications.**

#### **NOTE**

**The Individual Account ID Number encoded or embossed on a card may be a cardholder ID number or a “master account number” related to one or more of the cardholder’s accounts.**

**A card issuer may return the actual number of the cardholder account(s) affected by a transaction in an appropriate response message by using DE 102 (Account ID-1), DE 103 (Account ID-2), or both. However, the PAN used in the original Request message must then remain in DE 2 for all subsequent messages related to the original request (such as Responses, Advices, Reversals, Chargebacks, Retrieval Requests, and Retrieval Fulfillments).**

### **Issuing Institution Information**

PAN may contain Issuing Institution Information (IIN) when required in Authorization/01xx, Issuer File Update/03xx, and Network Management/08xx messages. IIN may consist of either a MasterCard customer ID number, a variable-length issuer card prefix sequence, or a MasterCard assigned Group Sign-on ID as required by a specific message.

DE 2 may contain only an IIN or card prefix sequence assigned to an issuer. It may also contain a valid MasterCard customer ID number or Group Sign-on ID for certain messages. Where card prefix information is required, the Authorization Platform accommodates variable-length prefix sequences from one to 11 digits.

## Data Element Definitions

### DE 3—Processing Code

---

Where a Group Sign-on ID is required, the Authorization Platform accommodates the five-digit Member Group ID, which MasterCard uses to identify a grouping of issuer account ranges that use the same transaction criteria for routing to the same destination route. More than one Group Sign-on ID value may be defined for an account range if an issuer chooses to route authorization traffic to different destinations according to transaction criteria.

## DE 3—Processing Code

DE 3 (Processing Code) describes the effect of a transaction on the customer account and the type of accounts affected.

---

### Attributes

---

Length of Length Field:	N/A
Data Representation:	n-6
Data Field:	Contents of subfields 1-3
Subfields:	3
Justification:	See “Subfields”

---

### Usage

---

Following is the usage of DE 3 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M
Authorization Request Response/0110	ME	•	ME
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	ME	ME
Reversal Request/0400	M	•	M
Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•

---

### Values

---

---

See “Subfields”

---

**Application Notes**


---

The following cross edits occur for:

---

**Authorization Request/0100**

<b>IF...</b>	<b>THEN...</b>
DE 48 (Transaction Category Code) = C	Cardholder Transaction Type Code must be 01, 17, or 30.
DE 48 (Transaction Category Code) = P	Cardholder Transaction Type Code must be 28.
DE 48 (Transaction Category Code) = Z	Cardholder Transaction Type Code must be 00, 01, 30, 40, 91, or 92.

---

**Reversal Request/0400 messages**

DE 48 (Transaction Category Code) = Z	Cardholder Transaction Type Code must be 00, 01, 30, 40, 91, or 92.
---------------------------------------	---

---

**Authorization Advice/0120—Acquirer-generated**

<b>IF...</b>	<b>THEN...</b>
DE 3, subfield 1 contains one of the following values : 01 = Withdrawal 28 = Payment Transaction 30 = Balance Inquiry 40 = Account Transfer 91 = PIN Unblock 92 = PIN Change or 00 = Purchase and DE 48 (Transaction Category Code) = Z	The Authorization Platform will return to the acquirer an Authorization Advice Response/0130 messages where: DE 39 = 30 DE 44 = 003

---

**Subfield 1—Cardholder Transaction Type Code**

DE 3, subfield 1 (Cardholder Transaction Type Code) describes the specific transaction type.

---

**Attributes**

Data Representation:	n-2
Data Field:	Contents of positions 1–2

---

**Data Element Definitions****DE 3—Processing Code**

Justification:		N/A					
<b>Values</b>							
<b>Cardholder Account Debits</b>		MC	NP	VI	TE	MS	CI
00	= Purchase	✓	✓	✓	✓	✓	✓
01	= Withdrawal	✓	✓	✓	✓	✓	✓
02	= Debit Adjustment		✓				
09	= Purchase with Cash Back	✓	✓			✓	
10	= Visa Only. Account Funding			✓			
17	= Cash Disbursement	✓	✓	✓	✓		
18	= Scrip Issue		✓				
<b>Cardholder Account Credits</b>		MC	NP	VI	TE	MS	CI
20	= Purchase Return/Refund	✓	✓			✓	
21	= Deposit		✓				
22	= Credit Adjustment		✓				
23	= Check Deposit Guarantee		✓				
24	= Check Deposit		✓				
28	= Payment Transaction	✓	✓	✓		✓	✓
<b>Cardholder Account Inquiries</b>		MC	NP	VI	TE	MS	CI
30	= Balance Inquiry	✓	✓	✓		✓	✓
<b>Cardholder Account Transfers</b>		MC	NP	VI	TE	MS	CI
40	= Account Transfer	✓	✓				
<b>Reserved Values</b>		MC	NP	VI	TE	MS	CI
90	= Reserved for Future Use		✓				
<b>PIN Management Transactions</b>		MC	NP	VI	TE	MS	CI
91	= PIN Unblock	✓	✓			✓	✓
92	= PIN Change	✓	✓			✓	✓

**Application Notes**

Value 20 is only applicable to Private Label and Swedish Domestic Authorization Switching Service (SASS) for MasterCard and Maestro branded transactions.

Value 28 is applicable only to eligible acquirers.

Value 30 is only applicable to eligible issuers.

Values 91 and 92 are only applicable to eligible acquirers and issuers.

**Subfield 2—Cardholder "From Account" Type Code**

DE 3, subfield 2 (Cardholder “From Account” Type Code) describes the cardholder account type affected for cardholder account debits and inquiries and the “from account” type for cardholder account transfer transactions.

**Attributes**

Data Representation:	n-2
----------------------	-----

Data Field:	Contents of positions 3–4
-------------	---------------------------

Justification:	N/A
----------------	-----

**Values**

Subfield 2 must now be one of the following values:

<b>Cardholder “From Account” Type Code</b>	MC	NP	VI	TE	MS	CI
00 = Default Account (not specified or not applicable)	✓	✓	✓	✓	✓	✓
10 = Savings Account	✓	✓	✓		✓	✓
20 = Checking Account	✓	✓	✓		✓	✓
30 = Credit Card Account	✓	✓	✓		✓	✓
38 = Credit Line Account		✓				
39 = Corporate		✓				
40 = Universal Account (Customer ID number)			✓			
50 = Money Market Investment Account		✓				
60 = Stored Value Account		✓				
90 = Revolving Loan Account			✓			

**Application Notes**

For UK Domestic Maestro, DE 3, subfield 2 must contain the value 00 - Default Account (not specified or not applicable).

### **Subfield 3—Cardholder "To Account" Type Code**

DE 3, subfield 3 (Cardholder “To Account” Type Code) describes the cardholder account type affected for cardholder account credits and the “to account” type for cardholder account transfer transactions.

---

#### **Attributes**

---

Data Representation: n-2

---

Data Field: Contents of positions 5–6

---

Justification: N/A

---

#### **Values**

---

Subfield 3 must be one of the following values:

---

<b>Cardholder “To Account” Type Code</b>		MC	NP	VI	TE	MS	CI
00	= Default Account (not specified or not applicable)	✓	✓	✓	✓	✓	✓
10	= Savings Account		✓			✓	✓
20	= Checking Account		✓			✓	✓
30	= Credit Card Account	✓	✓	✓			
38	= Credit Line Account		✓				
40	= Universal Account		✓				
50	= Money Market Investment Account		✓				
58	= IRA Investment Account		✓				
90	= Revolving Loan Account		✓				
91	= Installment Loan Account		✓				
92	= Real Estate Loan Account		✓				

---

### **DE 4—Amount, Transaction**

DE 4 (Amount, Transaction) is the amount of funds the cardholder requested in the local currency of the acquirer or source location of the transaction.

---

#### **Attributes**

---

Length of Length Field: N/A

---

Data Representation: n-12

---

Data Field:	Contents of positions 1–12
Subfields:	N/A
Justification:	Right with leading zeros

**Usage**

Following is the usage of DE 4 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M
Authorization Request Response/0110	CE	X	M
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	ME	ME
Reversal Request/0400	M	•	M
Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•

**Values**

Valid numeric data must be present in this data element.

The value must be zero for:

- Authorization Request/0100—AVS-only (discontinued for MasterCard brands as of 28 June 2011)
- Authorization Request/0100—Account Status Inquiry Service
- Authorization Request/0100—Recurring Payment Test transaction
- Authorization Request/0100 and Reversal Request/0400—Balance Inquiry, except where ATM transaction fees are allowed
- Authorization Request/0100 and Reversal Request/0400—PIN Management (PIN Unblock and PIN Change), except where ATM transaction fees are allowed
- Authorization Request/0100—Card Activation Request at POS

DE 28 (Amount, Transaction Fee) must be included in DE 4 when DE 28 is present in the message.

**Application Notes**

## Data Element Definitions

### DE 4—Amount, Transaction

---

DE 4 cannot exceed the region or country MasterCard *MoneySend* payment transaction limit.

WHEN...	THEN...
The issuer responds with DE 39 (Response Code), value 10 (Partial approval) or value 87 (Purchase amount only, no cash back allowed), the issuer is not required to echo DE 4	The Authorization Platform will forward to the acquirer, the Authorization Request Response/0110 message containing the partial approval amount in DE 4.

#### For Account Status Inquiry Service Transactions:

WHEN...	THEN the Authorization Platform...
The Authorization Request/0100 message contains DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service) and DE 4 (Amount, Transaction) contains a value equal to zero and DE 3 (Processing Code) contains a value other than 00 (Purchase)	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30</li><li>• DE 44 (Additional Response Data) = 003</li></ul>
The Authorization Request/0100 message contains DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service) and DE 4 contains a value other than zero.	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30</li><li>• DE 44 (Additional Response Data) = 004</li></ul>

#### For Automated Fuel Dispenser (AFD) Transactions:

Effective 12 June 2012 the contents of DE 4 may equal zero when the authorization Advice/0120 message is sent by a Europe region acquirer for an AFD transaction in Europe and contains DE 18 (Merchant Type) = 5542 (Fuel Dispenser, Automated) and DE 60 (Advice Reason Code) = 191 (Acquirer Processing System [APS] Completed Authorization Transaction).

Issuers should be prepared to receive zero amount AFD completion advices from any acquirer as there is no Authorization Platform edit restricting such advices from Europe region acquirers.

#### For Recurring Payment Test Transactions:

WHEN...	THEN...
The Authorization Request/0100 message contains DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence), value 4 (Standing order/recurring transactions), and DE 61, subfield 7 (POS Transaction Status), value 4 (Preauthorized Request)	DE 4 must contain a value of zero.

## DE 5—Amount, Settlement

DE 5 (Amount, Settlement) is the amount of funds to be transferred between the acquirer and the issuer equal to DE 4 (Amount, Transaction) in the settlement currency. MasterCard programs and services use U.S. dollars as the currency of settlement.

### Attributes

Length of Length Field:	N/A
Data Representation:	n-12
Data Field:	Contents of positions 1–12
Subfields:	N/A
Justification:	Right with leading zeros

### Usage

Following is the usage of DE 5 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Request Response/0110	CE	X	C
Authorization Advice/0120—Acquirer-generated	•	X	C
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice Response/0130—System-generated	•	X	C
Reversal Request/0400	•	X	C
Reversal Request Response/0410	CE	X	C
Reversal Advice/0420	•	C	C
Reversal Advice Response/0430	CE	CE	•

### Values

This data element must contain valid numeric data.

## Data Element Definitions

### DE 6—Amount, Cardholder Billing

---

#### Application Notes

---

All settlement amounts are specified in U.S. dollars. The settlement amount in authorization messages should be interpreted as “Amount, Reporting” because “settlement” of funds (for example, accounting “posting” or “memo-posting”) does not currently occur online for authorization messages.

The Authorization Platform will provide this data element if the customer chooses to receive settlement amount-related data elements.

It is optional for the acquirer and issuer to receive amount-related data elements in the settlement currency (U.S. dollars) with the exception of issuers that send Authorization Advice/0120—Issuer-generated messages to RiskFinder. Issuers that send Authorization Advice/0120—Issuer-generated messages to RiskFinder are **required** to receive settlement amount-related data elements because RiskFinder processes in U.S. dollars.

When the issuer responds with DE 39 (Response Code), value 10 (Partial approval) or value 87 (Purchase amount only, no cash back allowed), the issuer is not required to echo DE 5 if it was present in the Authorization Request/0100 message to the issuer. The Authorization Platform will provide the partial approval amount in DE 5 of the Authorization Request Response/0110 to the acquirer if the acquirer chooses to receive settlement amount-related data elements.

The issuer may receive a Reversal Request/0400 message containing a different value in DE 5 than was present in DE 5 of the original Authorization Request/0100 message. This difference occurs when the currency conversion rate used by the Authorization Platform changed between the time the Authorization Platform processed the original Authorization Request/0100 and the time the Authorization Platform processes the Reversal Request/0400 message.

If DE 4 converts to an amount that is more than 12 digits long in the settlement currency in DE 5, the Authorization Platform rejects the transaction with a format error in DE 4. When a customer receives this error code, it should verify that the transaction amount is correct.

This data will be present, as defined, except when the Authorization Platform has declined an Authorization Request/0100 message and was unable to complete currency conversion processing.

---

## DE 6—Amount, Cardholder Billing

DE 6 (Amount, Cardholder Billing) indicates the transaction amount in the issuer’s currency. It is the amount billed to the cardholder in the cardholder account currency, excluding cardholder billing fees.

---

#### Attributes

---

Length of Length Field: N/A

---

Data Representation: n-12

---

Data Field: Contents of positions 1–12

---

Subfields: N/A

---

Justification: Right with leading zeros

---

### **Usage**

Following is the usage of DE 6 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	M
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	•	X	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	ME	•
Authorization Advice Response/0130—System-generated	•	X	C
Reversal Request/0400	•	X	M
Reversal Request Response/0410	C	•	C
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•

### **Values**

This data element must contain valid numeric data.

### **Application Notes**

The Authorization Platform inserts this data element into all authorization and reversal messages. The Authorization Platform also will insert the following data elements to indicate the:

- Conversion factor used: DE 10 (Conversion Rate, Cardholder Billing)
- Conversion date: DE 16 (Date, Conversion)
- Issuer's currency: DE 51 (Currency Code, Cardholder Billing)
- If DE 39 is 87 (Purchase Amount Only, No Cash Back Allowed), DE 6 must be less than the requested amount
- If DE 39 is 10 (Partial Approval) and transaction is Automated Fuel Dispenser, DE 6 can be less, equal, or greater than requested amount.
- If DE 39 is 10 (Partial Approval) and transaction is not Automated Fuel Dispenser, DE 6 can be less or equal to the requested amount.

Where a minor unit of currency applies, amounts are expressed in the minor unit of currency without a decimal separator (example, value 100 represents USD 1.00).

This data element is defined as a mandatory echo in Authorization Request Response/0110 messages except when the issuer responds with DE 39 (Response

## Data Element Definitions

### DE 7—Transmission Date and Time

---

Code, value 10 (Partial approval) or value 87 (Purchase amount only, no cash back allowed).

The Authorization Platform forwards the partial approval amount in DE 6 of the Authorization Request Response/0110 to the acquirer.

The issuer may receive a Reversal Request/0400 message containing a different value in DE 6 than was present in DE 6 of the original Authorization Request/0100 message. This difference occurs when the currency conversion rate used by the Authorization Platform changed between the time the Authorization Platform processed the original Authorization Request/0100 and the time the Authorization Platform processes the Reversal Request/0400 message.

If DE 4 converts to an amount that is more than 12 digits long in the settlement currency in DE 5, the Authorization Platform rejects the transaction with a format error in DE 4. When a customer receives this error code, it should verify that the transaction amount is correct.

This data will be present, as defined, except when the Authorization Platform has declined an Authorization Request/0100 message and was unable to complete currency conversion processing.

---

## DE 7—Transmission Date and Time

DE 7 (Transmission Date and Time) is the date and time that a message is entered into the MasterCard Worldwide Network. Date and time must be expressed in Coordinated Universal Time (UTC).

---

### Attributes

---

Length of Length Field:	N/A
Data Representation:	n-10
Data Field:	Contents of subfields 1–2
Subfields:	2
Justification:	See “Subfields”

---

### Usage

---

Following is the usage of DE 7 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M
Authorization Request Response/0110	ME	•	ME
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•

**Data Element Definitions**  
**DE 7—Transmission Date and Time**

---

Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	ME	ME
Authorization Acknowledgement/0180	ME	ME	•
Authorization Negative Acknowledgement/0190	•	ME	ME
Issuer File Update Request/0302	M	M	•
Issuer File Update Request Response/0312	•	ME	ME
Reversal Request/0400	M	•	M
Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•
Administrative Request/0600	M	•	M
Administrative Request Response/0610	ME	•	ME
Administrative Advice/0620	•	M	M
Administrative Advice Response/0630	ME	ME	•
Network Management Request/0800—Sign-On/Sign-Off	M	M	•
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request/0800—PEK Exchange—On Demand	M	M	•
Network Management Request/0800—Host Session Activation/Deactivation	M	M	•
Network Management Request Response/0810	•	ME	ME
Network Management Request Response/0810—PEK Exchange	ME	M	•
Network Management Request Response/0810—PEK Exchange—On Demand	•	ME	ME
Network Management Request Response/0810—Host Session Activation/Deactivation	•	ME	ME
Network Management Advice/0820	•	M	M
Network Management Advice/0820—PEK Exchange	•	M	M
<b>Values</b>			
See “Subfields”			

## Data Element Definitions

### DE 7—Transmission Date and Time

---

#### Application Notes

---

This data element is defined and used identically within all MasterCard programs and services.

DE 7 must remain unchanged for all messages associated with a given system transaction, which includes all responses and acknowledgements related to an original request message (such as authorization, file update, administrative, network management). For example, the same DE 7 is used in an Authorization Request/0100 and any related Authorization Request Response/0110, Authorization Advice/0120—Acquirer-generated, Authorization Advice/0120—System-generated, or Reversal Advice/0420—System-generated message.

The Reversal Request/0400 message is the exception to this rule. Reversal Request/0400 messages are treated as an originating request and must have a unique DE 7 value assigned. The DE 7 value from the original 0100 request is included in DE 90 (Original Data Elements) for transaction matching purposes.

Each message initiator must assign a DE 7 to each originating request message. Effective 12 October 2012, the transmission time provided in DE 7 must be within three minutes of the current time recorded by the MasterCard Worldwide Network.

The combination of a message originator's DE 11 (Systems Trace Audit Number [STAN]) and DE 7 **must uniquely identify** any system transaction the message originator initiates on any given UTC day. These data elements together may be used as "key" data elements to identify and locate transaction records at some later time for the purpose of error resolution, settlement reconciliation, retrieval requests, and so forth.

---

### Subfield 1—Date

DE 7, subfield 1 (Date) describes the valid date.

---

#### Attributes

---

Data Representation: n-4

---

Data Field: Contents of positions 1–4

---

Justification: N/A

---

#### Values

---

This subfield must contain a valid date in MMDD format.

---

### Subfield 2—Time

DE 7, subfield 2 (Time) describes the valid time.

---

#### Attributes

---

Data Representation: n-6

---

Data Field: Contents of positions 5–10

---

---

Justification:	N/A
----------------	-----

**Values**

---

Time must contain a valid time in hhmmss format.
--

## **DE 8—Amount, Cardholder Billing Fee**

DE 8 (Amount, Cardholder Billing Fee) is the fee the issuer is to bill to the cardholder in the same currency as DE 6 (Amount, Cardholder Billing).

---

**Attributes**

---

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	n-8
----------------------	-----

Data Field:	N/A
-------------	-----

Subfields:	N/A
------------	-----

Justification:	Right with leading zeros
----------------	--------------------------

**Usage**

---

The Authorization Platform currently does not use this data element.
--

## **DE 9—Conversion Rate, Settlement**

DE 9 (Conversion Rate, Settlement) is the factor used in the conversion from transaction to settlement amount. DE 4 (Amount, Transaction) is multiplied by DE 9 to determine DE 5 (Amount, Settlement).

---

**Attributes**

---

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	n-8
----------------------	-----

Data Field:	Contents of subfields 1–2
-------------	---------------------------

Subfields:	2
------------	---

Justification:	Right, excluding the decimal indicator that must be the leftmost digit.
----------------	---

**Usage**

---

Following is the usage of DE 9 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Authorization Request/0100	•	X	C
----------------------------	---	---	---

Org   Sys   Dst

**Data Element Definitions**  
**DE 9—Conversion Rate, Settlement**

---

Authorization Request Response/0110	CE	X	C
Authorization Advice/0120—Acquirer-generated	•	X	C
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice Response/0130—System-generated	•	X	C
Reversal Request/0400	•	X	C
Reversal Request Response/0410	CE	X	C
Reversal Advice/0420	•	C	C
Reversal Advice Response/0430	CE	CE	•

**Values**

---

The leftmost digit must be in the range 0–7 and denotes the number of positions that the decimal point shall be moved from the right. Example: For a value of “69972522,” conversion rate is 9.972522.

---

**Application Notes**

---

The Authorization Platform will insert this data element into a message if the customer chooses to receive settlement amount-related data elements. If the settlement currency is the same as the acquirer's transaction currency, the conversion rate will be 1000000.

When used in Authorization/01xx messages, this data element should be interpreted as “Conversion Rate, Reporting” because settlement (for example, account “posting” or “memo posting”) of funds does not occur “online” with Authorization/01xx messages and Reversal Advice/04xx messages.

Note that when this data element is present in a message, DE 5 (Amount, Settlement) and DE 50 (Currency Code, Settlement) also are present.

The issuer may receive a Reversal Request/0400 message containing a different value in DE 9 than was present in DE 9 of the original Authorization Request/0100 message. This difference occurs when the currency conversion rate used by the Authorization Platform changed between the time the Authorization Platform processed the original Authorization Request/0100 and the time the Authorization Platform processes the Reversal Request/0400 message.

This data will be present, as defined, except when the Authorization Platform has declined an Authorization Request/0100 message and was unable to complete currency conversion processing.

---

## Subfield 1—Decimal Indicator

DE 9, subfield 1 (Decimal Indicator) indicates the number of positions the decimal point should be moved from the right.

---

**Attributes**

---

Data Representation: n-1

---

Data Field: Contents of position 1

---

Justification: N/A

---

**Values**

---

Must be in the range of 0–7.

---

## **Subfield 2—Conversion Rate**

DE 9, subfield 2 (Conversion Rate) indicates the conversion rate.

---

**Attributes**

---

Data Representation: n-7

---

Data Field: Contents of positions 2–8

---

Justification: N/A

---

**Values**

---

Must be a valid conversion rate.

---

## **DE 10—Conversion Rate, Cardholder Billing**

DE 10 (Conversion Rate, Cardholder Billing) is the factor used in the conversion from transaction to cardholder billing amount. DE 4 (Amount, Transaction) is multiplied by DE 10 to determine DE 6 (Amount, Cardholder Billing).

---

**Attributes**

---

Length of Length Field: N/A

---

Data Representation: n-8

---

Data Field: Contents of subfields 1–2

---

Subfields: 2

---

Justification: Right, excluding the decimal indicator that must be the leftmost digit.

---

**Usage**

---

Following is the usage of DE 10 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Org   Sys   Dst

## Data Element Definitions

### DE 10—Conversion Rate, Cardholder Billing

---

Authorization Request/0100	•	X	M
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	•	X	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	X	C
Reversal Request/0400	•	X	M
Reversal Request Response/0410	C	X	C
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	CE	CE	•

#### Values

---

Fixed length 8 positions; the leftmost decimal indicator denotes the number of positions that the decimal point shall be moved from the right. Example: For data element value “69972522,” conversion rate is 9.972522. The leftmost digit must be in the range 0–7.

#### Application Notes

---

The Authorization Platform inserts this data element into all authorization and reversal messages. If the issuer's cardholder billing currency is the same as the acquirer's transaction currency, the conversion rate will be 1000000.

Note that DE 6 (Amount, Cardholder Billing) and DE 51 (Currency Code, Cardholder Billing) also are present.

The issuer may receive a Reversal Request/0400 message containing a different value in DE 10 than was present in DE 10 of the original Authorization Request/0100 message. This occurs when the currency conversion rate used by the Authorization Platform changed between the time the Authorization Platform processed the original Authorization Request/0100 and the time the Authorization Platform processes the Reversal Request/0400 message.

This data will be present, as defined, except when the Authorization Platform has declined an Authorization Request/0100 message and was unable to complete currency conversion processing.

## Subfield 1—Decimal Indicator

DE 10, subfield 1 (Decimal Indicator) indicates the number of positions the decimal point should be moved from the right.

---

**Attributes**

---

Data Representation: n-1

---

Data Field: Contents of position 1

---

Justification: N/A

---

**Values**

---

Must be in the range of 0–7.

---

## **Subfield 2—Cardholder Billing Conversion Rate**

DE 10, subfield 2 (Cardholder Billing Conversion Rate) indicates the cardholder billing conversion rate.

---

**Attributes**

---

Data Representation: n-7

---

Data Field: Contents of positions 2–8

---

Justification: N/A

---

**Values**

---

Must be a valid conversion rate.

---

## **DE 11—System Trace Audit Number (STAN)**

DE 11 (Systems Trace Audit Number [STAN]) is a number a message initiator assigns to uniquely identify a transaction.

---

**Attributes**

---

Length of Length Field: N/A

---

Data Representation: n-6

---

Data Field: Contents of positions 1–6

---

Subfields: N/A

---

Justification: N/A

---

**Usage**

---

Following is the usage of DE 11 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Org    Sys    Dst

Authorization Request/0100

M    •    M

## Data Element Definitions

### DE 11—System Trace Audit Number (STAN)

Authorization Request Response/0110	ME	•	ME
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	ME	ME
Authorization Acknowledgement/0180	ME	ME	•
Authorization Negative Acknowledgement/0190	•	ME	ME
Issuer File Update Request/0302	M	M	•
Issuer File Update Request Response/0312	•	ME	ME
Reversal Request/0400	M	•	M
Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•
Administrative Request/0600	M	•	M
Administrative Request Response/0610	ME	•	ME
Administrative Advice/0620	•	M	M
Administrative Advice Response/0630	ME	ME	•
Network Management Request/0800—Sign-On/Sign-Off	M	M	•
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request/0800—PEK Exchange—On Demand	M	M	•
Network Management Request/0800—Host Session Activation/Deactivation	M	M	•
Network Management Request Response/0810—PEK Exchange	ME	M	•
Network Management Request Response/0810—PEK Exchange—On Demand	•	ME	ME
Network Management Request Response/0810—Host Session Activation/Deactivation	•	ME	ME
Network Management Advice/0820—PEK Exchange	•	M	M

---

### **Values**

---

This data element must **not** be all zeros or blanks.

---

### **Application Notes**

---

This data element is defined and used identically within all MasterCard programs and services.

DE 11 must remain unchanged for all messages associated with a given system transaction, which includes all responses and acknowledgements related to an original request message (such as authorization, file update, administrative, and network management). For example, the same DE 11 is used in an Authorization Request/0100 and any related Authorization Request Response/0110, Authorization Advice/0120—Acquirer-generated, Authorization Advice/0120—System-generated, or Reversal Advice/0420—System-generated message.

The Reversal Request/0400 message is the exception to this rule. Reversal Request/0400 messages are treated as an originating request and must have a unique DE 11 value assigned. The DE 11 value from the original 0100 request is included in DE 90 (Original Data Elements) for transaction matching purposes.

Each message initiator must assign DE 11 to each originating request message.

The combination of a message originator's DE 11 and DE 7 (Transmission Date and Time) **must uniquely identify** any system transaction the message originator initiates on any given UTC day. These data elements together may be used as "key" data elements to identify and locate transaction records at some later time for the purpose of error resolution, settlement reconciliation, retrieval requests.

Acquirers that process more than 999,999 transactions within a UTC day may repeat the same number.

---

## **DE 12—Time, Local Transaction**

DE 12 (Time, Local Transaction) is the local time at which the transaction takes place at the point of card acceptor location.

---

### **Attributes**

---

Length of Length Field: N/A

---

Data Representation: n-6

---

Data Field: Contents of positions 1–6

---

Subfields: N/A

---

Justification: N/A

---

### **Usage**

---

Following is the usage of DE 12 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
--	-----	-----	-----

Authorization Request/0100 C • C

**Data Element Definitions**  
**DE 13—Date, Local Transaction**

---

Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C

---

**Values**

---

Time must contain a valid time in hhmmss format.

Time must be specified in local time zone units, **not** in UTC units. The original value of this data element must not be changed. For example, if there is a delay between the time that a transaction was initiated or completed at a point of interaction and the time that the transaction was subsequently entered into the Authorization Platform, then DE 12 **must remain set to the actual local time** that the transaction was initiated at the card acceptor location.

---

**Application Notes**

---

This data element is defined and used identically within all MasterCard programs and services.

DE 12 is mandatory for all chip transactions (If missing, the Authorization Platform will not reject the message; however, a data integrity error will be reported.)

DE 12 is mandatory for all ATM transactions.

DE 12 is mandatory for all other card read transactions. (If it is missing, the Authorization Platform will not reject the message.)

DE 12 is mandatory for MasterCard Hosted Mobile Phone Top-up transactions.

**For UK Domestic Maestro:**

Must be present for transactions where DE 22, POS Entry Mode, contains 01x, 02x, 05x, 07x, 79x, 80x, 90x, or 91x and must contain the local time of the transaction.

---

## DE 13—Date, Local Transaction

DE 13 (Date, Local Transaction) is the local month and day on which the transaction takes place at the point of card acceptor location.

---

**Attributes**

---

Length of Length Field: N/A

---

Data Representation: n-4

---

Data Field: Contents of positions 1–4

---

Subfields: N/A

---

Justification: N/A

---

**Usage**

---

Following is the usage of DE 13 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C
Reversal Advice/0420	•	C	C

#### Values

Date must contain a valid date in MMDD format.

This date must be specified in local time zone units, **not** in UTC units. The original value of this data element must not be changed. For example, if there is a delay between the date that a transaction was initiated or completed at a point of interaction and the date that the transaction was subsequently entered into the Authorization Platform, DE 13 **must remain set to the actual local date** that the transaction was initiated at the card acceptor location.

#### Application Notes

This data element is defined and used identically within all MasterCard programs and services.

DE 13 is mandatory for all chip transactions (If missing, the Authorization Platform will not reject the message; however, a data integrity error will be reported.)

DE 13 is mandatory for all ATM transactions.

DE 13 is mandatory for all other card read transactions. (If missing, the Authorization Platform will not reject the message.)

DE 13 is mandatory for MasterCard Hosted Mobile Phone Top-up transactions.

#### For UK Domestic Maestro:

Must be present for transactions where DE 22, POS Entry Mode, contains 01x, 02x, 05x, 07x, 79x, 80x, 90x, or 91x and must contain the local time of the transaction.

## DE 14—Date, Expiration

DE 14 (Date, Expiration) specifies the year and month after which an issuer designates a cardholder's card to be "expired."

#### Attributes

Length of Length Field:	N/A
Data Representation:	n-4
Data Field:	Contents of positions 1–4

## Data Element Definitions

### DE 15—Date, Settlement

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

#### Usage

Following is the usage of DE 14 (whether it is mandatory, conditional, optional, system-provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C

#### Values

This data element must consist of a year and a month in YYMM format.

#### Application Notes

This data element is defined and used identically within all MasterCard programs and services.

IF...	THEN...
Track 1 or Track 2 (magnetic stripe) data is not present in the Authorization/01xx message	DE 14 is conditional.
Track 1 or Track 2 data (magnetic stripe) data is present in the Authorization/01xx message for MasterCard and Visa transactions	DE 14 is optional.
Track 1 or Track 2 (magnetic stripe) data is not present in the Authorization/01xx message for transactions other than MasterCard and Visa	DE 14 is mandatory.
The expiration date is unavailable	DE 14 must not be present (applies to MasterCard and Visa only).
An EMV transaction	DE 14 must be populated with mandatory expiration date contained on the chip in TAG 5F24.

### DE 15—Date, Settlement

DE 15 (Date, Settlement) is the date (month and day) that funds will be transferred between an acquirer and an issuer or an appropriate intermediate network facility (INF).

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-4
Data Field:	Contents of positions 1–4
Subfields:	N/A
Justification:	N/A

**Usage**

Following is the usage of DE 15 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	M
Authorization Request Response/0110	ME	•	ME
Authorization Advice/0120—Acquirer-generated	•	X	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	X	M
Reversal Request/0400	•	X	M
Reversal Request Response/0410	ME	X	M
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•

**Values**

This data element must consist of a month and day in MMDD format.

## Data Element Definitions

### DE 16—Date, Conversion

---

#### Application Notes

---

This data element is defined and used identically within all MasterCard programs and services.

For Authorization/01xx and Reversal Advice/04xx messages (in which there is no concurrent “online” settlement of funds), this data element is a date of “network reporting.” For example, the Authorization Platform provides program- or service-specific financial network business date to inform issuers and acquirers of the reporting date to which a transaction applies. It should be interpreted as “Date, Reporting.”

**In all cases** the Authorization Platform determines and inserts DE 15 in all originating Authorization/01xx and Reversal Advice/04xx messages.

The Authorization Platform provides this date. Therefore, this data element must not be present in any originating request or advice messages. Any customer processor system or INF **must not** change this date in any subsequent response message.

---

## DE 16—Date, Conversion

DE 16 (Date, Conversion) indicates the effective date of DE 9 (Conversion Rate, Settlement) and also DE 10 (Conversion Rate, Cardholder Billing) whenever these data elements are present within a message.

---

#### Attributes

---

Length of Length Field: N/A

---

Data Representation: n-4

---

Data Field: Contents of positions 1–4

---

Subfields: N/A

---

Justification: N/A

---

---

#### Usage

---

Following is the usage of DE 16 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	M
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	•	X	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•

Authorization Advice Response/0130—System-generated	•	X	C
Reversal Request/0400	•	X	M
Reversal Request Response/0410	C	X	C
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•

**Values**

This data element must consist of a month and day in MMDD format.

**Application Notes**

This data element is defined and used identically within all MasterCard programs and services.

This data will be present, as defined, except when the Authorization Platform has declined an Authorization Request/0100 message and was unable to complete currency conversion processing.

## DE 17—Date, Capture

DE 17 (Date, Capture) is the month and day the acquirer processed the transaction data.

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-4
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

**Usage**

The Authorization Platform currently does not use this data element.

## DE 18—Merchant Type

DE 18 (Merchant Type) is the classification (card acceptor business code/merchant category code [MCC]) of the merchant's type of business or service.

**Attributes**

Length of Length Field:	N/A
-------------------------	-----

## Data Element Definitions

### DE 18—Merchant Type

---

Data Representation:	n-4
Data Field:	Contents of positions 1–4
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of DE 18 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Reversal Request/0400	M	•	M

#### Values

This data element must contain a valid MCC. Refer to the *Quick Reference Booklet* for valid codes.

#### Application Notes

IF...	THEN...
The transaction is a MasterCard Electronic card Authorization Request/0100 message that occurs at magnetic stripe-reading or chip-reading terminals when the MCC represents a non-face-to-face environment, such as MCC 5542—Fuel Dispenser, Automated when PIN is present or chip is present with CAT 1.	The Authorization Platform sends the acquirer an Authorization Request Response/0100 where DE 39 (Response Code) = 58 (Transaction not permitted to acquirer/terminal).
The transaction is an Authorization Request/0100 or Reversal Request/0400 message and DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) contains value 01 (Withdrawal) and DE 18 is not 6010 (Member Financial Institution—Manual Cash Disbursements) or 6011 (Member Financial Institution—Automated Cash Disbursements)	The Authorization Platform sends an Authorization Request Response/0110 or Reversal Request Response/0410 message where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 018</li></ul>

Acquirer sends an Authorization Request/0100, Authorization Advice/0120, or Reversal Request/0400 message containing DE 18 (Merchant Type), value 6539 (Funding Transaction, Excluding MasterCard <i>MoneySend</i> )	The Authorization Platform sends the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 message where DE 39 (Response Code), is value 58 (Transaction not permitted to acquirer/terminal). This edit only applies to request and advice messages originated by Dual Message acquirers. This edit does not apply to messages originated by Single Message acquirers and therefore Dual Message issuers should expect to receive this data.
The acquirer sends an Authorization Request/0100 or Reversal Request/0400 containing DE 48, subelement 77 contains value C07 (MasterCard <i>MoneySend</i> ) and DE 18 is not 6536 (MasterCard <i>MoneySend</i> Intracountry) or 6537 (MasterCard <i>MoneySend</i> Intercountry)	The Authorization Platform sends the acquirer an Authorization Request Response/0110 or Reversal Request Response/0410 where: DE 39 = 30 DE 44 = 018

## DE 19—Acquiring Institution Country Code

DE 19 (Acquiring Institution Country Code) is the code of the country where the acquiring institution is located. Refer to the ISO 3166 specification for more information.

---

### Attributes

---

Length of Length Field:	N/A
Data Representation:	n-3
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

---

### Usage

---

The Authorization Platform currently does not use this data element.

---

## DE 20—Primary Account Number (PAN) Country Code

DE 20 (Primary Account Number [PAN] Country Code) is a code identifying the country where the card issuer is located.

## Data Element Definitions

### DE 20—Primary Account Number (PAN) Country Code

#### Attributes

Length of Length Field:	N/A
Data Representation:	n-3
Data Field:	Contents of positions 1-3
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of DE 20 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice Response/0130—System-generated	•	CE	CE
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE
Reversal Advice/0420	•	C	C
Reversal Advice Response/0430	CE	CE	•
Network Management Request/0800—Sign-On/Sign-Off	C	C	•

#### Values

Country Codes must be selected from the **numeric** ISO standard Country Codes. Refer to the *Quick Reference Booklet* for valid codes.

---

#### **Application Notes**

---

This data element is defined and used identically within all MasterCard programs and services.

DE 20 is required in any Authorization Platform message when the associated DE 2 (Primary Account Number [PAN]) is present and begins with a 59 BIN. PANs beginning with a 59 are **not** guaranteed to be internationally unique without the use of this associated Country Code. When the BIN begins with 59, the country code entered in DE 20 is identified as that in IPM table 40 issuer account range.

**For UK Domestic Maestro:** DE 20 is not applicable for UKDM transactions.

---

## **DE 21—Forwarding Institution Country Code**

DE 21 (Forwarding Institution Country Code) is the code of the country where the forwarding institution is located.

---

#### **Attributes**

---

Length of Length Field:	N/A
Data Representation:	n-3
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

---

#### **Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 22—Point-of-Service (POS) Entry Mode**

DE 22 (Point-of-Service [POS] Entry Mode) consists of numeric codes to indicate the method by which the PAN was entered into the interchange system and to indicate the POS terminal PIN entry capabilities.

---

#### **Attributes**

---

Length of Length Field:	N/A
Data Representation:	n-3
Data Field:	Contents of subfields 1–2
Subfields:	2
Justification:	See “Subfields”

---

#### **Usage**

---

## Data Element Definitions

### DE 22—Point-of-Service (POS) Entry Mode

---

Following is the usage of DE 22 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Reversal Request/0400	M	•	M
Reversal Advice/0420	•	M	M

#### Values

See “Subfields”

#### Application Notes

Following DE 22, subfield details are the [Authorization Platform Edits](#) that describe transaction-specific program and service edits for this data element.

#### PIN Management Transactions

Chip PIN Management: Only subfield 1, value 05 (PAN auto entry via chip) and subfield 2, value 1 (Terminal has PIN entry capability) are valid.

Magnetic Stripe PIN Management: subfield 1, values 02 and 90 are valid for magnetic stripe PIN change

#### All ATM Transactions

DE 22, subfield 2, must be value 1 (Terminal has PIN entry capability).

#### MasterCard Electronic Card

MasterCard Electronic consumer e-commerce *MoneySend* Payment Transactions do not require UCAF data (DE 48, subelement 43).

#### Short Message Service (SMS) Balance Inquiry service

Issuers participating in the Short Message Service (SMS) Balance Inquiry service will receive DE 22, subfield 1 (POS Terminal PAN Entry Mode), value 81 (PAN entry via electronic commerce, including chip).

## Subfield 1—POS Terminal PAN Entry Mode

DE 22, subfield 1 (POS Terminal PAN Entry Mode) indicates how the PAN was entered at the terminal.

---

#### Attributes

---

Data Representation: n-2

**Data Element Definitions**  
**DE 22—Point-of-Service (POS) Entry Mode**

---

Data Field:	Contents of positions 1–2
Justification:	N/A
<b>Values</b>	
00 =	PAN entry mode unknown
01 =	PAN manual entry
02 =	PAN auto-entry via magnetic stripe—track data is not required. OR The acquirer is not qualified to use value 90 so MasterCard replaced value 90 or 91 with value 02.
03 =	PAN auto-entry via bar code reader
04 =	PAN auto-entry via optical character reader (OCR)
05 =	PAN auto-entry via chip
06 =	PAN auto-entry via chip <i>PayPass</i> Mapping Service applied
<b>NOTE</b>	
<b>Acquirers do not send or receive value 06. Only MasterCard sends value 06 to the issuer when <i>PayPass</i> Mapping Service was performed.</b>	
07 =	PAN auto-entry via contactless M/Chip
08 =	PAN auto-entry via contactless M/Chip <i>PayPass</i> Mapping Service applied
<b>NOTE</b>	
<b>Acquirers do not send or receive value 08. Only MasterCard sends value 08 to the issuer when <i>PayPass</i> Mapping Service was performed.</b>	
79 =	A hybrid terminal with an online connection to the acquirer failed in sending a chip fallback transaction (in which DE 22, subfield 1 = 80) to the issuer. or A hybrid terminal with no online connection to the acquirer failed to read the chip card. The merchant is prompted to read the magnetic stripe from the card, the magstripe is successfully read and indicates a service code 2XX (or 6XX if card is domestic). To complete the transaction in both cases, a voice transaction takes place during which the merchant communicates the PAN and the expiry date originating from the magstripe track 2 data to the acquirer. The acquirer then sends an online transaction to the issuer in which the value of DE 22, subfield 1 = 79 and in which DE 61 subfield 11 indicate that the terminal is chip capable. Refer to the <i>M/Chip Requirements</i> for additional information.

## Data Element Definitions

### DE 22—Point-of-Service (POS) Entry Mode

---

80	=	Chip card at chip-capable terminal was unable to process transaction using data on the chip; therefore, the terminal defaulted to the magnetic stripe-read PAN. The full track data has been read from the data encoded on the card and transmitted within the Authorization Request/0100 in DE 45 (Track 1 Data) or DE 35 (Track 2 Data) without alteration or truncation. To use this value, the acquirer must be qualified to use value 90.
81	=	PAN entry via electronic commerce, including chip.
82	=	PAN Auto Entry via Server (issuer, acquirer, or third party vendor system)
90	=	PAN auto-entry via magnetic stripe—the full track data has been read from the data encoded 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.
91	=	PAN auto-entry via contactless magnetic stripe—the full track data has 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.
92	=	Contactless input, <i>PayPass</i> Mapping Service applied when acquirer DE 22, subfield 1 = 91.
<b>NOTE</b>		
<b>Acquirers do not send or receive value 92. Only MasterCard sends value 92 to the issuer when the PayPass Mapping Service was performed.</b>		
95	=	Visa only. Chip card with unreliable Card Verification Value (CVV) data.

### Subfield 2—POS Terminal PIN Entry Mode

DE 22, subfield 2 (POS Terminal PIN Entry Mode) indicates how the PIN was entered at the terminal.

---

#### Attributes

---

Data Representation: n-1

---

Data Field: Contents of position 3

---

Justification: N/A

---

#### Values

---

0 = Unspecified or unknown

---

1 = Terminal has PIN entry capability

---

2 = Terminal does not have PIN entry capability

---

8 = Terminal has PIN entry capability but PIN pad is not currently operative

---

## Authorization Platform Edits

The authorization system performs edits on specific programs and services.

Edits are performed on the following programs and services.

- MasterCard Electronic Commerce Transactions
- Chip Transactions
- Magnetic Stripe or Chip-Read Transactions for MasterCard Electronic Card

### MasterCard Electronic Card Transactions

The Authorization Platform performs a cross-edit between DE 22, subfield 1 and DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), position 3 (UCAF Collection Indicator) and DE 61 (Point-of-Service [POS] Data).

#### Authorization Request/0100 Message

<b>WHEN....</b>	<b>THEN...</b>
DE 22, subfield 1 contains the value 81 (PAN entry via electronic commerce, including chip)	DE 48, subelement 42 must be present.

### Chip Transactions

If MasterCard determines through its Internal Chip Monitoring process that improperly formatted chip transactions are being submitted from acquirers not certified to send chip transactions, MasterCard will notify each acquirer before activating an edit.

#### Authorization Request/0100 message

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 22, subfield 1 contains value 05 or 07 and DE 55 may or may not be present and Acquirer Chip Testing Level associated with the acquirer indicates the acquirer is not permitted to send chip transactions	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: <ul style="list-style-type: none"><li>• DE 39 = 30 (Format error)</li><li>• DE 44 = 022</li></ul>
DE 22, subfield 1, contains value 80 and Acquirer Chip Testing Level associated with the acquirer indicates the acquirer is not permitted to send chip transactions	Replaces DE 22, subfield 1, value 80 with value 90 before forwarding the Authorization Requestt/0100 message to the issuer and Notifies the acquirer of this downgrade by populating DE 48, subelement 74 (Additional Processing Information) in

## Data Element Definitions

### DE 22—Point-of-Service (POS) Entry Mode

---

WHEN...	THEN the Authorization Platform...
	<p>the Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"><li>• Subfield 1 = 90 (Chip Fallback Transaction Downgrade Process)</li><li>• Subfield 2 = C (Completed Successfully)</li></ul>

### Authorization Advice/0120—Acquirer-generated Edit

WHEN...	THEN the Authorization Platform...
<p>DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) contains value 80 and</p> <p>Acquirer Chip Testing Level associated with the acquirer indicates the acquirer is not permitted to send chip transactions</p>	<p>Replaces DE 22, subfield 1, value 80 with value 90 before forwarding the Authorization Advice/0120 message to the issuer.</p>

### Reversal Request/0400 message

WHEN...	THEN the Authorization Platform...
<p>DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) contains value 80 and</p> <p>Acquirer Chip Testing Level associated with the acquirer indicates the acquirer is not permitted to send chip transactions</p>	<p>Replaces DE 22, subfield 1, value 80 with value 90 before forwarding the Reversal Request/0400 message to the issuer and</p> <p>Notifies the acquirer of this downgrade by populating DE 48, subelement 74 (Additional Processing Information) in the Reversal Request Response/0410 message where:</p> <ul style="list-style-type: none"><li>• Subfield 1 = 90 (Chip Fallback Transaction Downgrade Process)</li><li>• Subfield 2 = C (Completed Successfully)</li></ul>

### Reversal Advice/0420 message

WHEN...	THEN the Authorization Platform...
<p>DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) contains value 80 and</p> <p>Acquirer Chip Testing Level associated with the acquirer indicates the acquirer is not permitted to send chip transactions</p>	<p>Replaces DE 22, subfield 1, value 80 with value 90 before forwarding the Reversal Advice/0420 message to the issuer</p>

## **Magnetic Stripe or Chip-Read Transactions for MasterCard Electronic Card**

The Authorization Platform performs the following edits on DE 22 for MasterCard Electronic Card transactions.

### **Authorization Request/0100 Message**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The Authorization Request/0100 message for a MasterCard Electronic card contains DE 22, subfield 1, value 02, 05, 07, 80, 90, or 91	<p>Determines whether the MCC in DE 18 (Merchant Type) is one of the following values that represent a non-face-to-face environment:</p> <ul style="list-style-type: none"> <li>• 5960 = Direct Marketing—Insurance Services</li> <li>• 5962 = Direct Marketing—Travel-Related Arrangement Services</li> <li>• 5964 = Direct Marketing—Catalog Merchants</li> <li>• 5965 = Direct Marketing—Combination Catalog and Retail Merchants</li> <li>• 5966 = Direct Marketing—Outbound Telemarketing Merchants</li> <li>• 5967 = Direct Marketing—Inbound Telemarketing Merchants</li> <li>• 5968 = Direct Marketing—Continuity/Subscription Merchants</li> <li>• 5969 = Direct Marketing—Other Direct Marketers—not elsewhere classified</li> </ul>
The value in DE 18 is equal to a non-face-to-face environment	Sends an Authorization Request Response/0110 message to the acquirer with DE 39 (Response Code), value 58 (Transaction not permitted to acquirer/terminal).
The Authorization Request/0100 message for a MasterCard Electronic card contains DE 22, subfield 1, value 02, 05, 07, 80, 90, or 91, and DE 18 (Merchant Type) MCC value is 5542 (Fuel Dispensers, Automated) and DE 52 (Personal ID number [PIN] Data) or DE 55 (Integrated Circuit Card [ICC] System-related Data) is not present and DE 61, subfield 10 is not value 1.	Sends an Authorization Request Response/0110 message to the acquirer with DE 39 (Response Code), value 58 (Transaction not permitted to acquirer/terminal).

## **DE 23—Card Sequence Number**

DE 23 (Card Sequence Number) distinguishes among separate cards having the same PAN or DE 34 (Primary Account Number [PAN] Extended). Issuers may encode chip cards with Card Sequence Numbers. Acquirers with chip-reading capability may pass this information encoded on the chip in DE 23 of Authorization Request/0100 messages.

---

### **Attributes**

---

Length of Length Field:	N/A
Data Representation:	n-3
Data Field:	Contents of positions 1–3
Subfields:	N/A
Justification:	N/A

---

### **Usage**

---

Following is the usage of DE 23 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice Response/0130—System-generated	•	CE	CE
Reversal Request/0400	C	•	C

---

### **Values**

---

---

#### **Acquirers:**

---

DE 23 must be three positions in the numeric range 000–099. For contact chip or contactless chip transactions where DE 22 subfield 1 is 05 or 07 respectively, DE 23 must contain the value of the Application PAN Sequence Number (EMV tag 5F34) as personalized on the chip. Considering that the Application PAN Sequence Number (EMV tag 5F34) is defined as a one-byte numeric value in the EMV specification, the terminal or the acquirer software must convert this one-byte numeric value to a three-byte value with leading zeros in DE 23. For example, if the value of EMV tag 5F34 on the chip card is 2, then the value of DE 23 is 002. For chip or contactless chip transactions, if EMV tag 5F34 is not personalized (not present) on the chip, DE 23 cannot be present in the authorization message.

When DE 23 (Card Sequence Number) is present in an Authorization Request/0100 message and the value is not in the range of 000–099, then the Authorization Platform forwards the Authorization Request Response/0110 where DE 39 = 30 (Format Error) and DE 44 (Additional Response Data) = 023.

**Issuers:**

The Authorization Platform does not cross-edit the presence or absence of DE 23 and the value in DE 22 (Point-of-Service [POS] Entry Mode) in Authorization Request/0100 messages. However, if DE 22 has a value 05 (PAN auto-entry via chip) or 07 (PAN auto-entry via contactless M/Chip) and if DE 23 is present in the Authorization Request/0100, DE 23 contains the card sequence number from the chip. If DE 22 has a value other than 05 or 07 and DE 23 is present, then DE 23 may contain erroneous information unrelated to the chip transaction.

Because of the potential for DE 23 to be present in Authorization/01xx messages, chip issuers must be prepared to receive store-and-forward (SAF) records containing DE 23.

Issuers must not return DE 23 in an Authorization Request Response/0110. If an issuer does so, MasterCard will delete DE 23 before passing the Authorization Request Response/0110 to the acquirer.

**Application Notes**

This data element is defined and used identically within all MasterCard programs and services.

**For UK Domestic Maestro:**

DE 23 must be present for:

- PAN key entry/manual transactions when the card sequence number is included in the criteria for uniquely identifying a card.
- Transactions containing ICC data when the card product indicates the card sequence number in the criteria for uniquely identifying a card.

## **DE 24—Network International ID**

DE 24 (Network International ID) identifies a single international network of card issuers.

---

**Attributes**

---

Length of Length Field: N/A

---

## Data Element Definitions

### DE 25—Point-of-Service (POS) Condition Code

---

Data Representation:	n-3
Data Field:	N/A
Subfields:	N/A
Justification:	N/A
<b>Usage</b>	

The Authorization Platform currently does not use this data element.

## DE 25—Point-of-Service (POS) Condition Code

DE 25 (Point-of-Service [POS] Condition Code) is an ID of the condition under which the transaction takes place at the point of interaction.

---

### Attributes

---

Length of Length Field:	N/A
Data Representation:	n-2
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

---

### Usage

---

The Authorization Platform currently does not use this data element.

All programs and services the Authorization Platform supports use DE 61 (Point-of-Service [POS] Data) as MasterCard defined and implemented for use by all customers, to specify the applicable conditions at the point of interaction.

### NOTE

**All MasterCard customers are required to use DE 61 for DE 25 information; as specified by MasterCard in this document, DE 25 must not be used.**

---

## DE 26—Point-of-Service (POS) Personal ID Number (PIN) Capture Code

DE 26 (Point-of-Service [POS] Personal ID Number [PIN] Capture Code) indicates the technique, maximum number, or both of PIN characters that can be accepted by the POS terminal used to construct the PIN data.

---

### Attributes

---

Length of Length Field:	N/A
-------------------------	-----

**Data Element Definitions**  
**DE 27—Authorization ID Response Length**

---

Data Representation:	n-2
Data Field:	Contents of positions 1–2
Subfields:	N/A
Justification:	Right

**Usage**

Following is the usage of DE 26 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C

**Values**

13–99	=	Reserved
04–12	=	Indicates the maximum number of PIN characters that the terminal can accept
00–03	=	Invalid

**Application Notes**

This data element is defined and used identically within all MasterCard programs and services.

DE 26 must be used to indicate the maximum number of PIN characters that the acquiring terminal device (for example; ATM and POS terminal) is capable of accepting.

The Authorization Platform requires that this data element be included in an Authorization Request/0100 message only when DE 52 (Personal ID Number [PIN] Data) is present and the maximum PIN character acceptance capability of the terminal is known to be other than 12 digits.

**NOTE**

**This data element is not used to specify the number of PIN characters actually accepted by a POS terminal device.**

**For UK Domestic Maestro:** DE 26 is not applicable for UKDM transactions.

## DE 27—Authorization ID Response Length

DE 27 (Authorization ID Response Length) is the maximum length of the authorization response that the acquirer can accommodate. The issuer or its agent is expected to limit response to this length.

## Data Element Definitions

### DE 28—Amount, Transaction Fee

---

#### Attributes

Length of Length Field:	N/A
Data Representation:	n-1
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

#### Usage

The Authorization Platform currently does not use this data element.

ISO and MasterCard defined DE 38 (Authorization ID Response) to be a six-character data element. All issuers and acquirers are expected to be able to accommodate and use the six-character data element for all authorization ID response codes.

---

## DE 28—Amount, Transaction Fee

DE 28 (Amount, Transaction Fee) is the fee charged (for example, by the acquirer) for transaction activity in the currency of DE 4 (Amount, Transaction).

#### Attributes

Length of Length Field:	N/A
Data Representation:	an-9
Data Field:	N/A
Subfields:	2
Justification:	See “Subfields”

#### Usage

Following is the usage of DE 28 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	X	CE
Authorization Advice/0120—System-generated	•	X	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	X	CE
Reversal Advice/0420	•	X	C

Reversal Advice Response/0430	CE	CE	•
-------------------------------	----	----	---

#### **Values**

This data element may be present in a message whenever an online transaction fee is permitted by the operating rules of a bank card product.

The credit or debit indicator (the first position of the data element) applies to the message recipient. Within acquirer-generated message types, a D (debit) fee amount indicates that the fee is to be applied as a debit to the message recipient, the issuer, (and therefore as a credit to the message originator, the acquirer).

#### **Application Notes**

The Authorization Platform does not support real-time settlement of transaction fees or processing fees concurrently with each individual transaction. All such fees for each financial network are calculated and settled daily, upon completion of each financial network business day, for all customers.

#### **NOTE**

**For acquirers that are approved to levy transaction fees, DE 28 must contain the transaction fee amount, and this amount also must be added to the requested amount contained in DE 4 (Amount, Transaction).**

If DE 28 is not provided in an Authorization Request Response/0110 or Reversal Request Response/0410 or is provided but it contains a value different from the original request, the Authorization Platform will populate the DE 28 value from the original Authorization Request/0100 or Reversal Request/0400 message in the response message before sending to the acquirer.

If the Authorization Request/0100 message or Reversal Request/0400 message contains DE 28, and subfield 1 is not C or D or if subfield 2 is zeros or is greater than DE 4, then the Authorization Platform forwards to the acquirer an Authorization Request Response/0110 message or Reversal Request Response/0410 where DE 39 = 30 (Format Error) and DE 44 = 028.

## **Subfield 1—Debit/Credit Indicator**

DE 28, subfield 1 (Debit/Credit Indicator) indicates the program type.

---

#### **Attributes**

---

Data Representation: a-1

---

Data Field: Contents of position 1

---

Justification: N/A

---

#### **Values**

---

C = Credit

---

D = Debit

---

## Data Element Definitions

### DE 29—Amount, Settlement Fee

---

#### Subfield 2—Amount

DE 28, subfield 2 (Amount) indicates the fee amount in the currency of DE 4 (Amount, Transaction).

---

##### Attributes

---

Data Representation: n-8

---

Data Field: Contents of positions 2-9

---

Justification: Right with leading zeros

---

##### Values

---

The fee amount must not contain all zeros or be greater than DE 4 (Amount, Transaction).

---

### DE 29—Amount, Settlement Fee

DE 29 (Amount, Settlement Fee) is the fee to be transferred between the acquirer and the issuer equal to DE 28 (Amount, Transaction Fee) in the currency of DE 5 (Amount, Settlement).

---

##### Attributes

---

Length of Length Field: N/A

---

Data Representation: an-9

---

Data Field: N/A

---

Subfields: 2

---

Justification: See “Subfields”

---

##### Usage

---

The Authorization Platform currently does not use this data element.

The Authorization Platform does not support real-time settlement of transaction fees or processing fees concurrently with each individual transaction. All such fees for each financial network are calculated and settled daily, upon completion of each financial network’s business day, for all customers.

---

#### Subfield 1—Debit/Credit Indicator

DE 29, subfield 1 (Debit/Credit Indicator) indicates the program type.

---

##### Attributes

---

Data Representation: a-1

---

Data Field:	Contents of position 1
Justification:	N/A
<b>Values</b>	
C =	Credit
D =	Debit

## Subfield 2—Amount

DE 29, subfield 2 (Amount) indicates the fee amount in the currency of DE 5 (Amount, Settlement).

---

### Attributes

---

Data Representation:	n-8
Data Field:	Contents of positions 2–9
Justification:	Right with leading zeros
<b>Values</b>	
Fee amount in the currency of DE 5 (Amount, Settlement).	

## DE 30—Amount, Transaction Processing Fee

DE 30 (Amount, Transaction Processing Fee) is the fee charged (for example, by the acquirer, issuer, or INF) for the handling and routing of messages in the currency of DE 4 (Amount, Transaction).

---

### Attributes

---

Length of Length Field:	N/A
Data Representation:	an-9
Data Field:	N/A
Subfields:	2
Justification:	See “Subfields”

---

### Usage

---

The Authorization Platform currently does not use this data element.

The Authorization Platform does not support real-time settlement of transaction fees or processing fees concurrently with each individual transaction. All such fees for each financial network are calculated and settled daily, upon completion of each financial network’s business day, for all customers.

## Data Element Definitions

### DE 31—Amount, Settlement Processing Fee

---

#### Subfield 1—Debit/Credit Indicator

DE 30, subfield 1 (Debit/Credit Indicator) indicates the program type.

---

##### Attributes

---

Data Representation: a-1

---

Data Field: Contents of position 1

---

Justification: N/A

---

##### Values

---

C = Credit

---

D = Debit

---

#### Subfield 2—Amount

DE 30, subfield 2 (Amount) indicates the fee amount in the currency of DE 4 (Amount, Transaction).

---

##### Attributes

---

Data Representation: n-8

---

Data Field: Contents of positions 2–9

---

Justification: Right with leading zeros

---

##### Values

---

Fee amount in the currency of DE 4 (Amount, Transaction).

---

## DE 31—Amount, Settlement Processing Fee

DE 31 (Amount, Settlement Processing Fee) is the fee charged (for example, by the acquirer, issuer, or INF) for the handling and routing of messages in the currency of DE 5 (Amount, Settlement).

---

##### Attributes

---

Length of Length Field: N/A

---

Data Representation: an-9

---

Data Field: N/A

---

Subfields: 2

---

Justification: See “Subfields”

---

---

**Usage**

---

The Authorization Platform currently does not use this data element.

The Authorization Platform does not support real-time settlement of transaction fees or processing fees concurrently with each individual transaction. All such fees for each financial network are calculated and settled daily, upon completion of each financial network's business day, for all customers.

---

## **Subfield 1—Debit/Credit Indicator**

DE 31, subfield 1 (Debit/Credit Indicator) indicates the program type.

---

**Attributes**

---

Data Representation: a-1

---

Data Field: Contents of position 1

---

Justification: N/A

---

**Values**

---

C = Credit

---

D = Debit

---

## **Subfield 2—Amount**

DE 31, subfield 2 (Amount) indicates the fee amount in the currency of DE 5 (Amount, Settlement).

---

**Attributes**

---

Data Representation: n-8

---

Data Field: Contents of positions 2–9

---

Justification: Right with leading zeros

---

**Values**

---

Fee amount in the currency of DE 5 (Amount, Settlement).

---

## **DE 32—Acquiring Institution ID Code**

DE 32 (Acquiring Institution ID Code) identifies the acquiring institution (for example, merchant bank) or its agent.

## Data Element Definitions

### DE 32—Acquiring Institution ID Code

---

#### Attributes

Length of Length Field:	2
Data Representation:	n...6; LLVAR
Data Field:	Contents of positions 1–6
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of DE 32 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M
Authorization Request Response/0110	ME	•	ME
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	ME	ME
Reversal Request/0400	M	•	M
Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•
Administrative Request/0600	M	•	M
Administrative Request Response/0610	ME	•	ME

#### Values

A MasterCard customer ID number that MasterCard assigned to the entity acting as the acquiring institution for a transaction.

#### Application Notes

This data element is defined and used identically within all MasterCard programs and services.

DE 32 **must** contain a six-digit customer ID number assigned by MasterCard that identifies the institution acting as the “acquiring bank” or “merchant bank” for a transaction.

When an institution acts as the customer processor system (CPS) or intermediate network facility (INF) for an acquirer, the institution **must**:

- Provide the acquirer's MasterCard-assigned six-digit customer ID in DE 32 and
- Provide its MasterCard-assigned six-digit customer ID in DE 33 (Forwarding Institution ID Code)

The MasterCard customer ID number must be set up in the Authorization Platform for participants to process Administrative Request/06xx messages.

IF...	THEN...
In a MasterCard transaction, the acquirer submits a transaction with a value of 90 in DE 22 (Point-of-Service [POS] Entry Mode)	DE 45 (Track 1 Data) or DE 35 (Track 2 Data) must be present, and DE 32 must contain the proper MasterCard customer ID number.
The Authorization Request/0100, Authorization Advice/0120, or Reversal Request/0400 message contains DE 32 and DE 32 is not 6 digits in length	The Authorization Platform forwards the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 where DE 39 = 30 (Format Error) and DE 44 = 032.

## DE 33—Forwarding Institution ID Code

DE 33 (Forwarding Institution ID Code) identifies the institution forwarding a Request or Advice message in an interchange system if it is not the same institution as specified in DE 32 (Acquiring Institution ID Code). DE 33 is used within a message to contain the MasterCard six-digit customer ID number of the CPS or INF responsible for directly routing that message to the Authorization Platform.

---

### Attributes

---

Length of Length Field: 2

---

Data Representation: n...6; LLVAR

---

Data Field: Contents of positions 1–6

---

Subfields: N/A

---

Justification: N/A

---

### Usage

---

## Data Element Definitions

### DE 33—Forwarding Institution ID Code

Following is the usage of DE 33 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice Response/0130—System-generated	•	CE	CE
Issuer File Update Request/0302	M	M	•
Issuer File Update Request Response/0312	•	ME	ME
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE
Reversal Advice/0420	•	C	C
Reversal Advice Response/0430	CE	CE	•
Administrative Request/0600	C	•	C
Administrative Request Response/0610	CE	•	CE
Administrative Advice/0620	•	M	M
Administrative Advice Response/0630	ME	ME	•
Network Management Request/0800—Sign-On/Sign-Off	M	M	•
Network Management Request/0800—PEK Exchange	M	M	•
Network Management Request/0800—PEK Exchange—On Demand	•	M	M
Network Management Request/0800—Host Session Activation/Deactivation	M	M	•
Network Management Request Response/0810	•	ME	ME
Network Management Request Response/0810—PEK Exchange	ME	M	•
Network Management Request Response/0810—PEK Exchange—On Demand	•	ME	ME

---

Network Management Request Response/0810—Host Session Activation/Deactivation	•	ME	ME
Network Management Advice/0820	•	M	M
Network Management Advice/0820—PEK Exchange	•	M	M

**Values**


---

This data element, when used, must contain a valid MasterCard customer ID number.

**Application Notes**

DE 33 must be present in messages together with DE 32 whenever the MasterCard customer ID number of a CPS or INF is different than the MasterCard customer ID number of the actual acquiring institution.

Automated Referral Service (ARS) store-and-forward transactions are included with other Stand-In processing transactions and are identified with a 003850 in DE 33 of the Authorization Advice/0120 message.

RiskFinder transactions are identified with 003200 in DE 33 of the Administrative Advice/0620.

The MasterCard customer ID number must be set up in the Authorization Platform for participants to process Administrative Request/06xx messages.

If an Authorization Request/0100, Authorization Advice/0120, or Reversal Request/0400 message contains DE 33 and DE 33 is not 6 digits in length, then the Authorization Platform will forward to the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 where DE 39 = 30 (Format Error) and DE 44 = 033.

## DE 34—Primary Account Number (PAN), Extended

DE 34 (Primary Account Number [PAN], Extended) identifies a customer account or relationship, and is used only when PAN begins with a 59 BIN.

**Attributes**


---

Length of Length Field:	2
Data Representation:	ans...28; LLVAR
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

**Usage**


---

The Authorization Platform currently does not use this data element.

## Data Element Definitions

### DE 35—Track 2 Data

---

## DE 35—Track 2 Data

DE 35 (Track 2 Data) is the information encoded on track 2 of the card magnetic stripe as defined in the ISO 7813 specification, including data element separators but excluding beginning and ending sentinels and longitudinal redundancy check (LRC) characters as defined therein.

---

### Attributes

---

Length of Length Field:	2
Data Representation:	ans...37; LLVAR
Data Field:	Contents of positions 1–37
Subfields:	N/A
Justification:	N/A

---

### Usage

---

Following is the usage of DE 35 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	X	C
Authorization Advice/0120—Acquirer-generated	O	•	O
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C

---

### Values

---

Whenever DE 35 is captured automatically at the point of interaction, DE 35 must contain whatever is encoded on the magnetic stripe (track 2) of the card, regardless of whether the card has been properly encoded with information in accordance with ISO specifications. The ISO 7810, 7811, 7812, and 7813 specifications document the international standards for encoding information on magnetic stripe cards.

For chip transactions, DE 35 carries data read from the chip as EMV tag 57 (Track 2 Equivalent Data). All ICCs issued by MasterCard customers must support EMV tag 57 (Track 2 Equivalent Data). Since January 2008, the value of the CVC in EMV tag 57 (Track 2 Equivalent Data) on the chip and the CVC value on the physical magnetic stripe must be different.

DE 35 must contain the hexadecimal digits “0” through “9” and “D” or “=” (the equal sign).

---

### Application Notes

---

The account number in DE 2 (Primary Account Number [PAN]) or DE 34 (Primary Account Number [PAN], Extended) must match the account number in DE 35.

This data element is defined and used identically within all MasterCard programs and services.

DE 35 is mandatory for all chip transactions (if missing, the Authorization Platform will not reject the message; however, a data integrity error will be reported).

DE 35 is mandatory for all ATM transactions. For Maestro transactions, such as e-commerce, the Authorization Platform creates track 2 data if it is not provided by the acquirer.

DE35 is optional for 0120 AFD completion advice. See Chapter 5 AFD Completion for more detail.

The field separator character (binary “1101”) is represented as the EBCDIC character “D”. However, because many ATM and POS devices perform nonstandard character translation while reading binary coded decimal (BCD) encoded magnetic stripe data, the EBCDIC character “=” may also be used to represent the field separator character in magnetic stripe data.

Following is Track 2 information content and format for MasterCard transactions:

Field ID and Name	F (Fixed), V (Variable)	Maximum Length
1 Start Sentinel	F	n-1
2 Primary Account Number	V	n...19
3 Separator (binary)	F	ans-1
4 Expiration Date	F	ans-4
5 Extended Service Code	F	ans-3
6 Discretionary Data (must include CVC 1)	V	Balance of available digits not to exceed total track length of 40 characters.
7 End Sentinel	F	n-1
8 Longitudinal Redundancy Check <sup>8</sup>	F	n-1

Please refer to the following manuals for additional Track 2 data information depending on the Acceptance Brand for the PAN:

- *Security Rules and Procedures*
- *Cirrus Worldwide Operating Rules*
- *Maestro Global Rules*

---

8. These fields are encoded on the card but must be omitted within Track-2 data.

## Data Element Definitions

### DE 36—Track 3 Data

---

## DE 36—Track 3 Data

DE 36 (Track 3 Data) is the information encoded on track 3 of the card magnetic stripe as defined in the ISO 4909–1986 specification, including data element separators but excluding beginning and ending sentinels and LRC characters as defined therein.

---

### Attributes

---

Length of Length Field: 2

---

Data Representation: ans...104; LLLVAR

---

Data Field: N/A

---

Subfields: N/A

---

Justification: N/A

---

### Usage

---

The Authorization Platform currently does not use this data element.

---

## DE 37—Retrieval Reference Number

DE 37 (Retrieval Reference Number) is a document reference number supplied by the system retaining the original source document of the transaction and assists in locating that source document or a copy thereof. DE 37 is made available for use by automated merchant POS systems that may be interconnected into the interchange system. Merchant POS systems may assign a unique receipt or sales document ID to be used to satisfy regulatory or legal requirements when the merchant performs source document capture and truncation. DE 37 may be used to relay source document reference numbers to the issuer at the time each transaction is processed.

---

### Attributes

---

Length of Length Field: 2

---

Data Representation: an-12

---

Data Field: Contents of positions 1–12

---

Subfields: 2 (for Chip transactions)

---

Justification: See “Subfields”

---

### Usage

---

Following is the usage of DE 37 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
--	-----	-----	-----

Authorization Request/0100	C	•	C
----------------------------	---	---	---

**Data Element Definitions**  
**DE 37—Retrieval Reference Number**

---

Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice Response/0130—System-generated	•	CE	CE
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE
Reversal Advice/0420	•	C	C
Reversal Advice Response/0430	CE	CE	•

**Values**

---

Number assigned by the acquirer.

When present, DE 37 must contain a value other than all zeros or all spaces.

DE 37 can have trailing spaces if the transaction is not a Visa or EMV chip transaction.

---

**Application Notes**

---

The Authorization Platform will pass DE 37, unaltered, to the receiving entity. The receiving entity must return this data element within any corresponding response.

DE 37 is mandatory for all chip transactions (DE 22 = 05x or 07x), chip fallback transactions (DE 22 = 80x), as well as contactless magnetic stripe transactions (DE 22 = 91x). If DE 37 is not present, the Authorization Platform will not reject the message. DE 37 is mandatory for all ATM transactions.

DE 37 is mandatory for all other card read transactions. (If missing, the Authorization Platform will not reject the message.)

DE 37 is mandatory for all UK Domestic Maestro transactions (DE 22 = 01x, 02x, 05x, 07x, 79x, 80x, 90x, or 91x.)

**Visa Transactions:** Acquirers that use the MasterCard Worldwide Network must populate CIS DE 37 with a 12-position, all numeric value containing a valid Julian date, in Visa Authorization Request/0100 and Reversal Request/0400 messages.

The format for CIS DE 37 on Visa transactions is (ydddhhnnnnnn):

- yddd (positions 1–4) is the year and day of year, equivalent of the value from DE 7 (Transmission Date and Time), y=0–9, ddd=001–366
- hh (positions 5 and 6) is the hours value from the time in DE 7 (Transmission Date and Time)
- nnnnnn (positions 7–12) is the value from DE 11 (Systems Trace Audit Number)

Visa will only edit positions 1–4. To avoid problems with system edits that may detect and reject duplicate and reused CIS DE 37 values, Visa recommends that endpoints construct CIS DE 37, positions 5–12 from the data in CIS DE 7 and CIS DE 11.

**Data Element Definitions**  
**DE 37—Retrieval Reference Number**

---

Acquirers may construct DE 37 in the same manner for MasterCard, as is indicated above for Visa messages.

---

## **Subfield 1—Transaction Date and Initiator Discretionary Data**

DE 37, subfield 1 (Transaction Date and Initiator Discretionary Data) is used to pass chip data. The value information is specific to chip transactions. Non-chip transactions can use any scheme as long as data is as defined in Data Representation.

---

### **Attributes**

---

Data Representation: an-7

---

Data Field: Contents of positions 1-7

---

Justification: Left

---

### **Values**

---

The date (MMDD) the transaction is captured at the point-of-service terminal. If no discretionary data is included, the remaining three positions of this subfield should be zero-filled.

This subfield is left-justified with trailing zeros.

---

## **Subfield 2—Terminal Transaction Number**

DE 37, subfield 2 (Terminal Transaction Number) is a unique number that identifies the transaction with a specific POS terminal within a specific 24 hour time period. The value information is specific to chip transactions. Non-chip transactions can use any scheme as long as data is as defined in Data Representation.

---

### **Attributes**

---

Data Representation: n-5

---

Data Field: Contents of positions 8-12

---

Justification: Right

---

### **Values**

---

The Terminal Transaction Number—A sequential number, per terminal. Only numeric data may be present in this subfield. This subfield must contain a unique number that identifies the transaction with a specific POS terminal within a specific 24 hour time period.

MasterCard recommends that this subfield contain the value of the Transaction Sequence Counter (EMV tag 9F41), if available.

This subfield is right-justified with leading zeros.

---

## DE 38—Authorization ID Response

DE 38 (Authorization ID Response) is a transaction response ID code that the authorizing institution assigns. DE 38 is used to transmit a card issuer's "authorization code" for Authorization transactions.

---

### Attributes

---

Length of Length Field:	N/A
Data Representation:	ans-6
Data Field:	Contents of positions 1–6
Subfields:	N/A
Justification:	Left

---

### Usage

---

Following is the usage of DE 38 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C
Reversal Advice/0420	•	C	C

---

### Values

---

When present, DE 38 must be left-justified and cannot contain all spaces, embedded spaces, all low values, or all high values.

---

### Application Notes

---

In general, the authorization code used in DE 38 may be any combination of alphanumeric characters. However, the following table identifies the standard conventions the major brands use:

Card Type	Length	Authorization ID Response Code Format
MasterCard	6	alphanumeric, with no spaces or special characters.
Visa	6	alphanumeric, with no special characters.
American Express	5	alphanumeric, trailing space(s).
Diners Club	6	numeric, trailing space(s).

## Data Element Definitions

### DE 39—Response Code

---

DE 38 is mandatory in the Authorization Request Response/0110 message when DE 39 (Response Code) contains the value 00 (approved), 08 (Honor with ID), 10 (Partial Approval), 85 (Not Declined), or 87 (Purchase amount only, no cash back allowed). If the transaction is approved by Stand-In processing, a six-digit authorization approval code beginning with "8" appears in this field. If X-Code or Limit-1 processing at the MIP generates the authorization response, this field is blank.

DE 38, position 6 may contain any of the following Account Level Management account category codes when the account range is participating in an Account Level Management service. Valid account category codes by program are:

- B = Enhanced Value (Enhanced Value and High Spend)
- M = Enhanced Value (Enhanced Value and High Spend) and Product Graduation
- P = Product Graduation (or the Co-brand Proprietary card program)
- S = High Value (High Value, Enhanced Value for Small Business, and Premium High Spend)
- T = High Value (High Value and Enhanced Value for Small Business) and Product Graduation
- W = World Elite Spend Shortfall
- Y = Product Graduation and World Elite Spend Shortfall
- Z = The default value provided by MasterCard indicating that while the account range does participate in Account Level Management processing, the specific cardholder account found in DE 2 (Primary Account Number [PAN]) of the transaction does not participate in Account Level Management processing.

**Issuers:** If DE 48, subelement 38 is present in the Authorization Request/0100 message and the issuer approves the request, then the Authorization Request Response/0110 message, DE 38, position 6 should contain the same value as received in DE 48, subelement 38.

Failure to include the category code in DE 38, position 6 on the approved authorization will cause the authorization request to be routed to and processed by the Stand-In System.

**Acquirers:** Acquirers should use DE 38, position 6 if the Authorization Request Response/0110 message was approved (DE 39 = 00, 08, 10, 85, or 87). Acquirers should use this value in their clearing process as indicated by IPM Clearing Member Parameter Extract (MPE). If the issuer provides DE 38 in an Authorization Request Response/0110 message and DE 39 is not an approval (00, 08, 10, 85, or 87), the Authorization Platform removes the DE 38 value from the response to the acquirer. This condition is excepted for UK Domestic Maestro transactions.

---

## DE 39—Response Code

DE 39 (Response Code) defines the disposition of a previous message or an action taken as a result of receipt of a previous message. Response codes also are used to indicate approval or decline of a transaction. In the event an authorization is declined, the response code indicates the reason for rejection and may indicate an action to be taken at the card acceptor (for example, "capture card").

**Attributes**

Length of Length Field:	N/A
Data Representation:	an-2
Data Field:	Contents of positions 1–2
Subfields:	N/A
Justification:	N/A

**Usage**

Following is the usage of DE 39 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	M	•	M
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	M	M	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	M	•	M
Authorization Advice Response/0130—System-generated	•	M	M
Authorization Acknowledgement/0180	M	M	•
Authorization Response Negative Acknowledgement/0190	•	M	M
Issuer File Update Request Response/0312	•	M	M
Reversal Request/0400	M	•	M
Reversal Request Response/0410	M	•	M
Reversal Advice/0420	•	C	C
Reversal Advice Response/0430	M	M	•
Administrative Request Response/0610	M	•	M
Administrative Advice Response/0630	M	M	•
Network Management Request Response/0810	•	M	M
Network Management Request Response/0810—Network Connection Status, Member-generated	M	M	•
Network Management Request Response/0810—Network Connection Status, System-generated	•	M	M

## Data Element Definitions

### DE 39—Response Code

Network Management Request Response/0810—Host Session Activation/Deactivation	•	M	M
Network Management Request Response/0810—PEK Exchange	M	M	•
Network Management Request Response/0810—PEK Exchange—On Demand	•	M	M

#### Values

Valid values are listed by message type.

#### Application Notes

DE 39 must be present in all Request Response, Advice Response, and Acknowledgement messages. In addition, it is also present in Authorization Advice/0120 “Stand-In” messages to indicate the response code used in the Authorization Request Response/0110 to the original Authorization Request/0100. The Authorization Platform responds to the following response codes as indicated for MasterCard brands only:

IF the issuer provides a response code value of...	THEN the Authorization Platform...
91, 92, or 96 in the Authorization Request Response/0110 (applies to MasterCard only.)	Automatically invokes Stand-In processing. Stand-In processes the transaction according to issuer-specified parameters that generate the issuer-specified response (for example, approve, decline, refer, or capture card.)
00, 08, 10, 85, or 87 in the Authorization Request Response/0110	Requires that DE 38 (Authorization Identification Response) is present.
Invalid values in DE 39 for a MasterCard ATM transaction...	Instead, the issuer should use the following response code...
01, 03, 08, 12, 15, 63, 76, 77, or 87	57
78	14
84 or 94	Any valid response code

## Authorization Request Response/0110 Response Codes

The following DE 39 response codes are valid in this message.

Values		Action	MC	NP	VI	TE	MS	CI
00	=	Approved or completed successfully	Approve	✓	✓	✓	✓	✓
01	=	Refer to card issuer	Call Issuer	✓	✓	✓	✓	✓
03	=	Invalid merchant	Decline	✓	✓	✓	✓	✓

**Data Element Definitions**
**DE 39—Response Code**

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
04	=	Capture card	Capture	✓	✓	✓	✓	✓
05	=	Do not honor	Decline	✓	✓	✓	✓	✓
08	=	Honor with ID	Approve	✓	✓	✓	✓	✓
10	=	Partial Approval	Approve	✓	✓	✓		✓
12	=	Invalid transaction	Decline	✓	✓	✓	✓	✓
13	=	Invalid amount	Decline	✓	✓	✓	✓	✓
14	=	Invalid card number	Decline	✓	✓	✓	✓	✓
15	=	Invalid issuer	Decline	✓	✓	✓	✓	✓
30	=	Format error	Decline	✓	✓	✓	✓	✓
41	=	Lost card	Capture	✓	✓	✓	✓	✓
43	=	Stolen card	Capture	✓	✓	✓	✓	✓
51	=	Insufficient funds/over credit limit	Decline	✓	✓	✓	✓	✓
54	=	Expired card	Decline	✓	✓	✓	✓	✓
55	=	Invalid PIN	Decline	✓	✓	✓	✓	✓
57	=	Transaction not permitted to issuer/cardholder	Decline	✓	✓	✓		✓
58	=	Transaction not permitted to acquirer/terminal	Decline	✓	✓	✓		✓
61	=	Exceeds withdrawal amount limit	Decline	✓	✓	✓	✓	✓
62	=	Restricted card	Decline	✓	✓	✓	✓	✓
63	=	Security violation	Decline	✓	✓	✓	✓	✓
65	=	Exceeds withdrawal count limit	Decline	✓	✓	✓	✓	✓
70	=	Contact Card Issuer	Call Issuer	✓	✓		✓	✓
71	=	PIN Not Changed	Decline	✓	✓		✓	✓
75	=	Allowable number of PIN tries exceeded	Decline	✓	✓	✓	✓	✓
76	=	Invalid/nonexistent “To Account” specified	Decline		✓	✓		

**Data Element Definitions****DE 39—Response Code**

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
77	=	Invalid/nonexistent “From Account” specified	Decline		✓	✓		
78	=	Invalid/nonexistent account specified (general)	Decline	✓	✓	✓	✓	✓
84	=	Invalid Authorization Life Cycle	Decline		✓			
85	=	Not declined Valid for all zero amount transactions.	Valid	✓	✓		✓	✓
86	=	PIN Validation not possible	Decline	✓	✓	✓	✓	✓
87	=	Purchase Amount Only, No Cash Back Allowed	Approved	✓			✓	
88	=	Cryptographic failure	Decline	✓	✓	✓	✓	✓
89	=	Unacceptable PIN—Transaction Declined—Retry	Decline	✓	✓		✓	✓
91	=	Authorization Platform or issuer system inoperative	Decline	✓	✓	✓	✓	✓
92	=	Unable to route transaction	Decline	✓	✓	✓	✓	✓
94	=	Duplicate transmission detected	Decline	✓	✓	✓	✓	
96	=	System error	Decline	✓	✓	✓	✓	✓

**Authorization Advice/0120 Response Codes**

The following DE 39 response codes are valid in this message.

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
00	=	Approved or completed successfully	Approve	✓	✓	✓	✓	✓
01	=	Refer to card issuer	Call Issuer	✓	✓	✓	✓	✓
03	=	Invalid merchant	Decline	✓	✓	✓	✓	
04	=	Capture card	Capture	✓	✓	✓	✓	✓
05	=	Do not honor	Decline	✓	✓	✓	✓	
08	=	Honor with ID	Approve	✓	✓	✓	✓	

**Data Element Definitions**
**DE 39—Response Code**

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
10	= Partial Approval	Approve	✓	✓	✓		✓	
12	= Invalid transaction	Decline	✓	✓	✓	✓	✓	
13	= Invalid amount	Decline	✓	✓	✓	✓	✓	✓
14	= Invalid card number	Decline	✓	✓	✓	✓	✓	✓
15	= Invalid issuer	Decline	✓	✓	✓	✓	✓	
30	= Format error	Decline	✓	✓	✓	✓	✓	✓
41	= Lost card	Capture	✓	✓	✓	✓	✓	✓
43	= Stolen card	Capture	✓	✓	✓	✓	✓	✓
51	= Insufficient funds/over credit limit	Decline	✓	✓	✓	✓	✓	✓
54	= Expired card	Decline	✓	✓	✓	✓	✓	✓
55	= Invalid PIN	Decline	✓	✓	✓	✓	✓	✓
57	= Transaction not permitted to issuer/cardholder	Decline	✓	✓	✓		✓	✓
58	= Transaction not permitted to acquirer/terminal	Decline	✓	✓	✓		✓	✓
61	= Exceeds withdrawal amount limit	Decline	✓	✓	✓	✓	✓	✓
62	= Restricted card	Decline	✓	✓	✓	✓	✓	✓
63	= Security violation	Decline	✓	✓	✓	✓	✓	
65	= Exceeds withdrawal count limit	Decline	✓	✓	✓	✓	✓	✓
70	= Contact Card Issuer	Call Issuer	✓	✓			✓	✓
71	= PIN Not Changed	Decline	✓	✓			✓	✓
75	= Allowable number of PIN tries exceeded	Decline	✓	✓	✓	✓	✓	✓
76	= Invalid/nonexistent “To Account” specified	Decline			✓	✓		
77	= Invalid/nonexistent “From Account” specified	Decline			✓	✓		
78	= Invalid/nonexistent account specified (general)	Decline	✓	✓	✓	✓	✓	

## Data Element Definitions

### DE 39—Response Code

Values	Action	MC	NP	VI	TE	MS	CI
84 = Invalid Authorization Life Cycle	Decline		✓				
85 = Not declined	Valid	✓	✓		✓	✓	✓
86 = PIN Validation not possible	Decline	✓	✓	✓	✓	✓	✓
87 = Purchase Amount Only, No Cash Back Allowed	Approved	✓				✓	
88 = Cryptographic failure	Decline	✓	✓	✓	✓	✓	✓
89 = Unacceptable PIN—Transaction Declined—Retry	Decline	✓	✓			✓	✓
91 = Authorization Platform or issuer system inoperative	Decline	✓	✓	✓	✓	✓	✓
92 = Unable to route transaction	Decline	✓	✓	✓	✓	✓	✓
94 = Duplicate transmission detected	Decline	✓	✓	✓	✓	✓	
96 = System error	Decline	✓	✓	✓	✓	✓	✓

## Authorization Advice Response/0130 Response Codes

The following DE 39 response codes are valid in this message.

Values	Action	MC	NP	VI	TE	MS	CI
00 = Approved or completed successfully	—	✓	✓	✓		✓	✓
12 = Invalid transaction	—	✓	✓	✓	✓	✓	✓
14 = Invalid card number	—	✓				✓	✓
30 = Format error	—	✓	✓	✓		✓	✓
57 = Transaction not permitted to issuer/cardholder. Valid only for Pay with Rewards Service	—	✓					
94 = Duplicate Transmission detected	—	✓	✓	✓		✓	✓
96 = System error	—	✓	✓	✓		✓	✓

## Authorization Advice Response/0180 Response Codes

The following DE 39 response codes are valid in this message.

Values	Action	MC	NP	VI	TE	MS	CI
00 = Completed successfully	—	✓	✓	✓	✓	✓	✓

## Authorization Negative Acknowledgement/0190 Response Codes

The following DE 39 response codes are valid in this message.

Values	Action	MC	NP	VI	TE	MS	CI
30 = Format error	—	✓	✓	✓	✓	✓	✓
68 = Response received late	—	✓	✓	✓	✓	✓	✓
96 = System error	—	✓	✓	✓	✓	✓	✓

## Issuer File Update Request Response/0312 Response Codes

The following DE 39 response codes are valid in this message.

Values	Action	MC	NP	VI	TE	MS	CI
00 = Issuer File Update action completed successfully	—	✓	✓	✓	✓	✓	✓
25 = Unable to locate record on file (no action taken)	—	✓	✓	✓	✓	✓	✓
27 = Issuer File Update field edit error	—	✓	✓	✓	✓	✓	✓
30 = Format error	—	✓	✓	✓	✓	✓	✓
40 = Requested function not supported	—	✓	✓	✓	✓	✓	✓
63 = Security violation	—	✓	✓	✓	✓	✓	✓
80 = Duplicate add, action not performed	—	✓	✓	✓	✓	✓	✓
96 = System error	—	✓	✓	✓	✓	✓	✓

## Reversal Request/0400 Message Response Codes

The following DE 39 response codes are valid in this message.

## Data Element Definitions

### DE 39—Response Code

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
00	=	Approved or completed successfully	Approve	✓	✓	✓	✓	✓
01	=	Refer to card issuer	Call Issuer	✓	✓	✓	✓	✓
03	=	Invalid merchant	Decline	✓	✓	✓	✓	✓
04	=	Capture card	Capture	✓	✓	✓	✓	✓
05	=	Do not honor	Decline	✓	✓	✓	✓	✓
06	=	Error	Decline	✓			✓	✓
08	=	Honor with ID	Approve	✓	✓	✓	✓	
10	=	Partial Approval	Approve	✓	✓	✓		✓
12	=	Invalid transaction	Decline	✓	✓	✓	✓	✓
13	=	Invalid amount	Decline	✓	✓	✓	✓	✓
14	=	Invalid card number	Decline	✓	✓	✓	✓	✓
15	=	Invalid issuer	Decline	✓	✓	✓	✓	✓
17	=	Customer cancellation	Decline	✓			✓	✓
30	=	Format error	Decline	✓	✓	✓	✓	✓
32	=	Partial reversal	Decline	✓			✓	✓
34	=	Suspect Fraud	Decline	✓	✓		✓	
41	=	Lost card	Capture	✓	✓	✓	✓	✓
43	=	Stolen card	Capture	✓	✓	✓	✓	✓
51	=	Insufficient funds/over credit limit	Decline	✓	✓	✓	✓	✓
54	=	Expired card	Decline	✓	✓	✓	✓	✓
55	=	Invalid PIN	Decline	✓	✓	✓	✓	✓
57	=	Transaction not permitted to issuer/cardholder	Decline	✓	✓	✓		✓
58	=	Transaction not permitted to acquirer/terminal	Decline	✓	✓	✓	✓	✓
61	=	Exceeds withdrawal amount limit	Decline	✓	✓	✓	✓	✓

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
62	=	Restricted card	Decline	✓	✓	✓	✓	✓
63	=	Security violation	Decline	✓	✓	✓	✓	✓
65	=	Exceeds withdrawal count limit	Decline	✓	✓	✓	✓	✓
68	=	Response received late	Decline	✓			✓	✓
70	=	Contact Card Issuer	Call Issuer	✓	✓		✓	✓
71	=	PIN Not Changed	Decline	✓	✓		✓	✓
75	=	Allowable number of PIN tries exceeded	Decline	✓	✓	✓	✓	✓
76	=	Invalid/nonexistent “To Account” specified	Decline		✓	✓		
77	=	Invalid/nonexistent “From Account” specified	Decline		✓	✓		
78	=	Invalid/nonexistent account specified (general)	Decline	✓	✓	✓	✓	✓
84	=	Invalid Authorization Life Cycle	Decline		✓			
85	=	Not declined	Valid	✓	✓		✓	✓
86	=	PIN Validation not possible	Decline	✓	✓	✓	✓	✓
87	=	Purchase Amount Only, No Cash Back Allowed	Approved	✓			✓	
88	=	Cryptographic failure	Decline	✓	✓	✓	✓	✓
89	=	Unacceptable PIN—Transaction Declined—Retry	Decline	✓	✓		✓	✓
91	=	Authorization Platform or issuer system inoperative	Decline	✓	✓	✓	✓	✓
92	=	Unable to route transaction	Decline	✓	✓	✓	✓	✓
94	=	Duplicate transmission detected	Decline	✓	✓	✓	✓	✓
96	=	System error	Decline	✓	✓	✓	✓	✓

## Reversal Request Response/0410 Response Codes

The following DE 39 response codes are valid in this message.

## Data Element Definitions

### DE 39—Response Code

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
00	= Approved or completed successfully	Approve	✓	✓	✓	✓	✓	✓
01	= Refer to card issuer	Call Issuer	✓	✓	✓	✓	✓	
12	= Invalid transaction	Decline	✓	✓	✓	✓	✓	
13	= Invalid amount	Decline	✓	✓	✓	✓	✓	✓
14	= Invalid card number	Decline	✓	✓	✓	✓	✓	✓
30	= Format error	Decline	✓	✓	✓	✓	✓	✓
41	= Lost card	Capture	✓	✓	✓	✓	✓	✓
43	= Stolen card	Capture	✓	✓	✓	✓	✓	✓
57	= Transaction not permitted to issuer/cardholder	Decline	✓	✓	✓		✓	✓
58	= Transaction not permitted to acquirer/terminal	Decline	✓	✓	✓		✓	✓
62	= Restricted card	Decline	✓	✓	✓	✓	✓	✓
63	= Security violation	Decline	✓	✓	✓	✓	✓	
91	= Authorization Platform or issuer system inoperative	Decline	✓	✓	✓	✓	✓	✓
92	= Unable to route transaction	Decline	✓	✓	✓	✓	✓	✓
94	= Duplicate transmission detected	Decline	✓	✓	✓	✓	✓	✓
96	= System error	Decline	✓	✓	✓	✓	✓	✓

### Reversal Advice/0420 Response Codes

The following DE 39 response codes are valid in this message.

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
00	= Approved or completed successfully	Approve	✓	✓	✓	✓	✓	✓
01	= Refer to card issuer	Call Issuer	✓	✓	✓	✓	✓	
03	= Invalid merchant	Decline	✓	✓	✓	✓	✓	
04	= Capture card	Capture	✓	✓	✓	✓	✓	✓
05	= Do not honor	Decline	✓	✓	✓	✓	✓	

**Data Element Definitions**
**DE 39—Response Code**

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
06	=	Error	Decline	✓			✓	✓
08	=	Honor with ID	Approve	✓	✓	✓	✓	
10	=	Partial Approval	Approve	✓	✓	✓		✓
12	=	Invalid transaction	Decline	✓	✓	✓	✓	✓
13	=	Invalid amount	Decline	✓	✓	✓	✓	✓
14	=	Invalid card number	Decline	✓	✓	✓	✓	✓
15	=	Invalid issuer	Decline	✓	✓	✓	✓	✓
17	=	Customer cancellation	Decline	✓			✓	✓
30	=	Format error	Decline	✓	✓	✓	✓	✓
32	=	Partial reversal	Decline	✓			✓	✓
34	=	Suspect Fraud	Decline	✓	✓			✓
41	=	Lost card	Capture	✓	✓	✓	✓	✓
43	=	Stolen card	Capture	✓	✓	✓	✓	✓
51	=	Insufficient funds/over credit limit	Decline	✓	✓	✓	✓	✓
54	=	Expired card	Decline	✓	✓	✓	✓	✓
55	=	Invalid PIN	Decline	✓	✓	✓	✓	✓
57	=	Transaction not permitted to issuer/cardholder	Decline	✓	✓	✓	✓	✓
58	=	Transaction not permitted to acquirer/terminal	Decline	✓	✓	✓	✓	✓
61	=	Exceeds withdrawal amount limit	Decline	✓	✓	✓	✓	✓
62	=	Restricted card	Decline	✓	✓	✓	✓	✓
63	=	Security violation	Decline	✓	✓	✓	✓	✓
65	=	Exceeds withdrawal count limit	Decline	✓	✓	✓	✓	✓
68	=	Response received late	Decline	✓			✓	✓
70	=	Contact Card Issuer	Call Issuer	✓	✓		✓	✓

**Data Element Definitions****DE 39—Response Code**

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
71	=	PIN Not Changed	Decline	✓	✓		✓	✓
75	=	Allowable number of PIN tries exceeded	Decline	✓	✓	✓	✓	✓
76	=	Invalid/nonexistent “To Account” specified	Decline		✓	✓		
77	=	Invalid/nonexistent “From Account” specified	Decline		✓	✓		
78	=	Invalid/nonexistent account specified (general)	Decline	✓	✓	✓	✓	✓
82	=	Timeout at issuer	—	✓	✓	✓	✓	✓
84	=	Invalid Authorization Life Cycle	Decline		✓			
85	=	Not declined Valid for zero amount transactions.	Valid	✓	✓		✓	✓
86	=	PIN Validation not possible	Decline	✓	✓	✓	✓	✓
87	=	Purchase Amount Only, No Cash Back Allowed	Approved	✓			✓	
88	=	Cryptographic failure	Decline	✓	✓	✓	✓	✓
89	=	Unacceptable PIN—Transaction Declined—Retry	Decline	✓	✓		✓	✓
91	=	Authorization Platform or issuer system inoperative	Decline	✓	✓	✓	✓	✓
92	=	Unable to route transaction	Decline	✓	✓	✓	✓	✓
94	=	Duplicate transmission detected	Decline	✓	✓	✓	✓	✓
96	=	System error	Decline	✓	✓	✓	✓	✓

**Reversal Advice Response/0430 Message and Administrative Advice Response/0630 Response Codes**

The following DE 39 response codes are valid in these messages.

**Data Element Definitions****DE 39—Response Code**

<b>Values</b>	<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
00 = Approved or completed successfully	—	✓	✓	✓	✓	✓	✓
30 = Format error	—	✓	✓	✓	✓	✓	✓
94 = Duplicate Transmission detected	—	✓	✓	✓	✓	✓	✓
96 = System error	—	✓	✓	✓	✓	✓	✓

**Administrative Request Response/0610 Response Codes**

The following DE 39 response codes are valid in this message.

<b>Values</b>	<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
00 = Received and processed successfully	None	✓	✓				
30 = Format error	Determine error and resubmit request	✓	✓				
57 = Transaction not permitted to issuer/cardholder	Decline	✓	✓				
58 = Transaction not permitted to acquirer/terminal	Decline	✓	✓				
91 = Authorization Platform or issuer system inoperative	Resubmit request	✓	✓				
92 = Unable to route transaction	Determine error and resubmit request	✓	✓				
96 = System error	Resubmit request	✓	✓				

**Network Management Request Response/0810 Response Codes**

The following DE 39 response codes are valid in this message.

<b>Values</b>	<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
00 = Approved or completed successfully	—	✓	✓	✓	✓	✓	✓
30 = Format error	—	✓	✓	✓	✓	✓	✓

## Data Element Definitions

### DE 40—Service Restriction Code

Values	Action	MC	NP	VI	TE	MS	CI
63 = Security violation	—	✓	✓	✓	✓	✓	✓
79 = Key Exchange Validation failed	—	✓	✓	✓	✓	✓	✓
91 = Authorization Platform or issuer system inoperative	—	✓	✓	✓	✓	✓	✓
94 = Duplicate SAF request	—	✓	✓	✓	✓	✓	✓
96 = System error	—	✓	✓	✓	✓	✓	✓

### DE 40—Service Restriction Code

DE 40 (Service Restriction Code) identifies geographic or service availability.

#### Attributes

Length of Length Field: N/A

Data Representation: an-3

Data Field: N/A

Subfields: N/A

Justification: N/A

#### Usage

The Authorization Platform currently does not use this data element.

### DE 41—Card Acceptor Terminal ID

DE 41 (Card Acceptor Terminal ID) uniquely identifies a terminal at the card acceptor location of acquiring institutions or merchant POS systems. The terminal ID should be printed on all transaction receipts in ATM and POS transactions where the terminal is capable of generating customer receipts.

#### Attributes

Length of Length Field: N/A

Data Representation: ans-8

Data Field: Contents of positions 1–8

Subfields: N/A

Justification: Left

### **Usage**

Following is the usage of DE 41 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice Response/0130—System-generated	•	CE	CE
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE
Reversal Advice/0420	CE	CE	•
Administrative Request/0600	O	•	O
Administrative Request Response/0610	CE	•	CE

### **Values**

Each terminal ID may be up to eight characters long and the terminal owner assigns it. It must be unique within the terminal owning organization (for example, unique within merchant or unique within acquiring institution).

### **Application Notes**

This data element is defined and used identically within all MasterCard programs and services.

This data element must be present in Authorization Request/0100 messages if DE 42 (Card Acceptor ID Code) does not uniquely identify the terminal.

DE 41 is mandatory for all chip transactions (if missing, the Authorization Platform will not reject the message; however, a data integrity error will be reported.)

DE 41 is mandatory for all ATM transactions.

DE 41 is mandatory for all other card read transactions. If missing, the Authorization Platform will not reject the message.

**For UK Domestic Maestro:** Must be present for transactions where DE 22, POS Entry Mode, contains 01x, 02x, 05x, 07x, 79x, 80x, 90x, or 91x.

**Data Element Definitions**  
**DE 42—Card Acceptor ID Code**

---

## DE 42—Card Acceptor ID Code

DE 42 (Card Acceptor ID Code) identifies the card acceptor that defines the point of the transaction in both local and interchange environments. DE 42 is used as a “merchant ID” to uniquely identify the merchant in a POS transaction.

---

### Attributes

---

Length of Length Field:	N/A
Data Representation:	ans-15
Data Field:	Contents of positions 1–15
Subfields:	N/A
Justification:	Left

---

### Usage

---

Following is the usage of DE 42 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C
Administrative Request/0600	O	•	O
Administrative Request Response/0610	CE	•	CE

---

### Values

---

Number assigned by the acquirer.

---

### Application Notes

---

DE 42 is required in card-activated POS phone transactions initiated at public phones to identify the service provider (for example, AT&T, GTE). Refer to DE 43 (Card Acceptor Name/Location for Bankcard-Activated Public Phones).

DE 42 is not required for ATM transactions or other transactions where the acquiring institution directly provides the service (for example, where the “card acceptor” is the acquiring institution).

DE 42 is required for POS transaction types containing DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), values 00 (Purchase), 09 (Purchase with Cash Back) and 28 (Payment Transaction).

Merchant Verification Service for Private Label transactions is performed using either DE 42 or DE 48, subelement 32. Acquirers are required to contact their merchant or their private label issuer to learn more about the Private Label Merchant Verification Service and whether DE 42 or DE 48, subelement 32 is used in this service.

An American Express merchant ID consists of the 10-digit numeric value (referred to as “SE number” by American Express) or two-character alphanumeric IATA airline code (which may be followed by the IATA travel agent ID, T + 5-8 digits, separated by a space). Since DE 42 is defined as ans-15, an American Express merchant ID should consist of the 10-digit SE number in character format, preceded by either five leading zeros or spaces, or followed by either five trailing zeros or spaces. This 10-digit number also should pass the Luhn-10 check digit routine.

The following Authorization Platform edit will apply:

WHEN...	THEN the Authorization Platform...
DE 42 (Card Acceptor ID Code) is not present and DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type code) contains the value 00 (Purchase), 09 (Purchase with Cash Back), or 28 (Payment Transaction) in an Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or a Reversal Request/0400 message	<p>Sends the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or a Reversal Request Response/0410 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format Error)</li> <li>• DE 44 (Additional Response Data) = 042 (which identifies DE 42 as the source of the error)</li> </ul>

## DE 43—Card Acceptor Name/Location for All Transactions

DE 43 (Card Acceptor Name/Location) contains the name and location of the card acceptor that defines the point of interaction in both local and interchange environments (excluding ATM and Card-Activated Public Phones).

### Attributes

Length of Length Field:	N/A
Data Representation:	ans-40 (supports extended character sets)
Data Field:	Contents of subfields 1–5
Subfields:	5
Justification:	See “Subfields”

### Usage

Following is the usage of DE 43 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•

## Data Element Definitions

### DE 43—Card Acceptor Name/Location for All Transactions

---

Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C
Reversal Advice/0420	•	C	C
Administrative Request/0600	O	•	O
Administrative Request Response/0610	CE	•	CE

#### Values

---

The data element subfields are dependent on the type of message type sent. The data element subfields in DE 43 for all transactions are for all transactions except those initiated at ATMs or at Bankcard-Activated POS phones.

#### Application Notes

---

This data element is required for all Authorization Request/0100 messages for MasterCard and Visa programs and services.

For Authorization Request/0100, use of DE 43 is conditional (C) based on the program or service being processed. If the program is MasterCard or Visa, use of DE 43 is mandatory (M). Its usage is optional if the transaction involves Private Label, Travel and Entertainment, or other programs.

This data element satisfies “Regulation-E” requirements. It also is required when the DE 22 (Point-of-Service [POS] Entry Mode) is 05 (PAN auto-entry via integrated circuit card).

As ISO specifies, this data element is an alphanumeric text string of 40 characters. MasterCard requires standardized formatting of this data element as specified in the following table to meet uniform standards for printing this information on customer account statements and billing statements.

This data element is required for all MasterCard programs and services. The Authorization Platform does not perform edits on this data element.

DE 43 is required for MasterCard Hosted Mobile Phone Top-up transactions.

**For UK Domestic Maestro:** Must be present for transactions where DE 22, POS Entry Mode, contains 01x, 02x, 05x, 07x, 79x, 80x, 90x, or 91x. Must always be present for Reversal Advice/0420 messages.

---

## Subfield 1—Merchant Name ("Doing Business As" name)

DE 43 (Card Acceptor Name/Location for All Transactions), subfield 1 (Merchant Name) is the merchant doing business as name.

---

#### Attributes

---

Data Representation: ans-22

---

Data Field: Contents of positions 1–22

---

Justification: Left

---

#### Values

---

---

Valid merchant name or “doing business as” name.

---

The merchant or “doing business as” name associated with a rePower transaction must have the value: MC rePower following the carrier name.

---

## **Subfield 2—Space**

DE 43 (Card Acceptor Name/Location for All Transactions), subfield 2 (Space) indicates a space character.

---

### **Attributes**

---

Data Representation: ans-1

---

Data Field: Contents of position 23

---

Justification: N/A

---

### **Value**

---

Delimiter (space).

---

## **Subfield 3—Merchant's City**

DE 43 (Card Acceptor Name/Location for All Transactions), subfield 3 (Merchant's City) indicates the city of the merchant.

---

### **Attributes**

---

Data Representation: ans-13

---

Data Field: Contents of positions 24–36

---

Justification: Left

---

### **Values**

---

Valid city name.

---

## **Subfield 4—Space**

DE 43 (Card Acceptor Name/Location for All Transactions), subfield 4 (Space) indicates a space character.

---

### **Attributes**

---

Data Representation: ans-1

---

Data Field: Contents of position 37

---

Justification: N/A

---

## Data Element Definitions

### DE 43—Card Acceptor Name/Location for ATM Transactions

---

#### Value

Delimiter (space).

### Subfield 5—Merchant's State (or Country Code, if not U.S.)

DE 43 (Card Acceptor Name/Location for All Transactions), subfield 5 (Merchant's State) indicates the state or country code (if not U.S.) of the merchant.

#### Attributes

Data Representation: a-3

Data Field: Contents of positions 38-40

Justification: Left

#### Values

State and Country Code must contain valid data. The three-character alphabetic Country Code must be used (not the three-character numeric Country Code). Refer to the *Quick Reference Booklet* for valid codes.

## DE 43—Card Acceptor Name/Location for ATM Transactions

DE 43 (Card Acceptor Name/Location for ATM Transactions) contains the name and location of the card acceptor that defines the point of interaction in both local and interchange environments. The data element subfields are dependent on the message type sent. The data element subfields in DE 43 for ATM transactions are for transactions initiated at ATM terminals.

#### Attributes

Length of Length Field: N/A

Data Representation: ans-40

Data Field: Contents of subfields 1-5

Subfields: 5

Justification: See "Subfields"

#### Usage

Following is the usage of DE 43 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Authorization Request/0100

Org Sys Dst

C • C

## Data Element Definitions

### DE 43—Card Acceptor Name/Location for ATM Transactions

Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C
Reversal Advice/0420	•	C	C

#### Values

See “Subfields.”

#### Application Notes

This data element is required for all MasterCard programs and services. The Authorization Platform does not perform edits on this data element.

For Authorization Request/0100, use of DE 43 is conditional (C) based on the program or service being processed. If the program is MasterCard or Visa, use of DE 43 is mandatory (M). Its usage is optional if the transaction involves Private Label, Travel and Entertainment, or other programs.

## Subfield 1—ATM Owning Institution or Terminal/Merchant Address or Both

DE 43 (Card Acceptor Name/Location for ATM Transactions), subfield 1 (ATM Owning Institution or Terminal/Merchant Address or Both) indicates the ATM owning institution name and terminal or merchant street address.

#### Attributes

Data Representation: ans-22

Data Field: Contents of positions 1–22

Justification: Left

#### Values

ATM owning institution name and terminal or merchant street address required.

## Subfield 2—Space

DE 43 (Card Acceptor Name/Location for ATM Transactions), subfield 2 (Space) indicates a space character.

#### Attributes

Data Representation: ans-1

Data Field: Contents of position 23

## Data Element Definitions

### DE 43—Card Acceptor Name/Location for ATM Transactions

---

Justification:	N/A
<b>Value</b>	
Delimiter (space).	

### Subfield 3—ATM or Merchant Location City

DE 43 (Card Acceptor Name/Location for ATM Transactions), subfield 3 (ATM or Merchant Location City) indicates the ATM or merchant's location city.

---

#### Attributes

---

Data Representation:	ans-13
Data Field:	Contents of positions 24–36
Justification:	Left
<b>Values</b>	
Valid ATM or merchant location city name.	

### Subfield 4—Space

DE 43 (Card Acceptor Name/Location for ATM Transactions), subfield 4 (Space) is used to include space character.

---

#### Attributes

---

Data Representation:	ans-1
Data Field:	Contents of position 37
Justification:	N/A
<b>Value</b>	
Delimiter (space).	

### Subfield 5—ATM or Merchant State, Province, or Country Code Location

DE 43 (Card Acceptor Name/Location for ATM Transactions), subfield 5 (ATM or Merchant State, Province, or Country Code Location) indicates the ATM or Merchant location.

---

#### Attributes

---

Data Representation:	a-3
----------------------	-----

Data Field:	Contents of positions 38–40
Justification:	Right, blank-filled
<b>Values</b>	
U.S.A and U.S. territories:	ATM or merchant location state code
Canada and Canadian territories:	ATM or merchant location province code
All other Countries:	ATM or merchant location country code
State and Country Code must contain valid data. The three-character alphabetic Country Code must be used (not the three-character numeric Country Code). Refer to the <i>Quick Reference Booklet</i> for valid codes.	

## DE 43—Card Acceptor Name/Location for Bankcard-Activated Public Phones

DE 43 (Card Acceptor Name/Location for Bankcard-Activated Public Phones) contains the name and location of the card acceptor that defines the point of interaction in both local and interchange environments. The data element subfields are dependent on the type of message type sent. The data element subfields in DE 43 for Bankcard-Activated Public Phone Transactions are for transactions initiated through a phone service provider.

### Attributes

Length of Length Field:	N/A
Data Representation:	ans-40 (supports extended character sets)
Data Field:	Contents of subfields 1–8
Subfields:	8
Justification:	See “Subfields”

### Usage

Following is the usage of DE 43 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C

## Data Element Definitions

### DE 43—Card Acceptor Name/Location for Bankcard-Activated Public Phones

---

Reversal Advice/0420

• C C

#### Values

See “Subfields”

When the transaction is initiated at a POS phone device, DE 43 must be formatted as described as described by the subfield data and the phone service provider (such as “AT&T” or “GTE”) must be identified using DE 42 (Card Acceptor ID Code).

This data element is required for all Authorization Request/0100 messages for MasterCard and Visa programs and services.

For Authorization Request/0100, use of DE 43 is conditional (C) based on the program or service being processed. If the program is MasterCard or Visa, use of DE 43 is mandatory (M). Its usage is optional if the transaction involves Private Label, Travel and Entertainment, or other programs.

#### Application Notes

This data element is required for all MasterCard programs and services. The Authorization Platform does not perform edits on this data element.

## Subfield 1—Abbreviation "TEL"

DE 43 (Card Acceptor Name/Location for Bankcard-Activated Public Phones), subfield 1 (Abbreviation TEL) indicates the transaction was initiated through a phone service provider.

---

#### Attributes

Data Representation: a-3

Data Field: Contents of positions 1–3

Justification: N/A

---

#### Values

TEL = Telephone

## Subfield 2—Phone Number Dialed

DE 43 (Card Acceptor Name/Location for Bankcard-Activated Public Phones), subfield 2 (Phone Number Dialed) indicates the phone number the transaction initiated from.

---

#### Attributes

Data Representation: ans-15

Data Field: Contents of positions 4–18

Justification: N/A

---

**Values**

---

If U.S. or Canadian number; includes area code. If non-U.S. or non-Canadian number, includes full phone number with country code, city code, and local number.

---

**Subfield 3—Abbreviation "M"**

DE 43 (Card Acceptor Name/Location for Bankcard-Activated Public Phones), subfield 3 (Abbreviation M) indicates minutes.

---

**Attributes**

---

Data Representation: a-1

---

Data Field: Contents of position 19

---

Justification: N/A

---

**Values**

---

M = Minutes

---

**Subfield 4—Call Duration**

DE 43 (Card Acceptor Name/Location for Bankcard-Activated Public Phones), subfield 4 (Call Duration) indicates the duration of the call in minutes.

---

**Attributes**

---

Data Representation: ans-3

---

Data Field: Contents of positions 20–22

---

Justification: Left-justified with trailing spaces

---

**Values**

---

Duration of call in minutes in mmm format (10 = 10 minutes).

---

**Subfield 5—Space**

DE 43 (Card Acceptor Name/Location for Bankcard-Activated Public Phones), subfield 5 (Space) indicates a space character.

---

**Attributes**

---

Data Representation: ans-1

---

Data Field: Contents of position 23

---

Justification: N/A

---

**Data Element Definitions****DE 43—Card Acceptor Name/Location for Bankcard-Activated Public Phones**

---

**Values**

---

Delimiter (space).

---

**Subfield 6—Call Origin City**

DE 43 (Card Acceptor Name/Location for Bankcard-Activated Public Phones), subfield 6 (Call Origin City) indicates the city where the call originated.

---

**Attributes**

---

Data Representation: ans-13

---

Data Field: Contents of positions 24-36

---

Justification: Left

---

**Values**

---

Valid city name.

---

**Subfield 7—Space**

DE 43 (Card Acceptor Name/Location for Bankcard-Activated Public Phones), subfield 7 (Space) indicates a space character.

---

**Attributes**

---

Data Representation: ans-1

---

Data Field: Contents of position 37

---

Justification: N/A

---

**Values**

---

Delimiter (space).

---

**Subfield 8—Call Origin State or Country Code**

DE 43 (Card Acceptor Name/Location for Bankcard-Activated Public Phones), subfield 8 (Call Origin State or Country Code) indicates the call origin state or country code.

---

**Attributes**

---

Data Representation: a-3

---

Data Field: Contents of positions 38-40

---

Justification: Left justified, blank-filled

---

#### **Values**

State or Country Code (country code if not U.S.) The three-character **alphabetic** Country Code must be used (not the three-character numeric Country Code). Refer to the *Quick Reference Booklet* for valid codes.

## **DE 44—Additional Response Data**

DE 44 (Additional Response Data) provides other supplemental data that may be required in response to an authorization or other type of transaction request. This data element may also be present in any response message when DE 39 (Response Code) contains the value 30, indicating that a “Format Error” condition was detected in the preceding message. In this case, the first three bytes of DE 44 (if present) will contain a three-digit numeric value indicating the data element number where the format error occurred.

#### **Attributes**

Length of Length Field:	2
-------------------------	---

Data Representation:	ans...25; LLVAR
----------------------	-----------------

Data Field:	Contents of positions 1–25
-------------	----------------------------

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

#### **Usage**

Following is the usage of DE 44 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice Response/0130—System-generated	•	CE	CE
Authorization Negative Acknowledgement/0190	•	C	C
Issuer File Update Request Response/0312	•	C	C
Reversal Request Response/0410	C	•	C

**Data Element Definitions**  
**DE 44—Additional Response Data**

---

Reversal Advice Response/0430	C	C	•
Administrative Request Response/0610	C	•	C
Administrative Advice Response/0630	C	C	•
Network Management Request Response/0810—PEK Exchange	C	C	•
Network Management Request Response/0810—PEK Exchange—On Demand	•	C	C
Network Management Request Response/0810—Host Session Activation/Deactivation	•	C	C
Network Management Request Response/0810—Network Connection Status, System-generated	•	C	C
Network Management Request Response/0810—RiskFinder SAF Request	•	C	C
Network Management Request Response/0810—Sign-On/Sign-Off	•	C	C

**Values**

---

Contains supplemental data.

---

**Application Notes**

---

The following table lists the usage of this data element. Usage is dependent on values in DE 39. The following table defines the additional response data that is in DE 44 when the listed values are present in DE 39. No data element edits are performed on the variable-length field.

---

## DE 44 Values by Program or Service

The following table lists the usage of DE 44 by program or service. Usage is dependent on values in DE 39 (Response Code). The following table defines the additional response data that is in DE 44 when the listed values are present in DE 39. No data element edits are performed on the variable-length field.

IF DE 39 is...	THEN DE 44 Contains...	MC	NP	VI	TE	MS	CI
00	N/A						
01	Contains the phone number for “call issuer” response codes. Applies to Authorization Request Response/0110 messages.	✓	✓	✓	✓	✓	✓

**Data Element Definitions**  
**DE 44—Additional Response Data**

---

<b>IF DE 39 is...</b>	<b>THEN DE 44 Contains...</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
08	<p>Contains the ID information for “approve with ID” response codes for example:</p> <ul style="list-style-type: none"> <li>• B = Blank Name</li> <li>• C = Cardholder’s ID number or hologram message</li> <li>• X= Cardholder’s last name</li> </ul> <p>Applies to Authorization Request Response/0110 messages.</p>	√	√	√	√	√	
12	<p>DE 44 should be accessed when the value 12 is present in DE 39 for MasterCard Corporate Fleet Card® transactions only as follows:</p> <ul style="list-style-type: none"> <li>• 01 = Issuer determines that the ID number provided in the Authorization Request/0100 message is invalid causing the transaction to be declined</li> <li>• 02 = Issuer determines that the Driver Number provided in the Authorization Request/0100 message is invalid causing the transaction to be declined</li> <li>• 03 = Issuer determines that the Vehicle Number provided in the Authorization Request/0100 message is invalid causing the transaction to be declined.</li> </ul> <p>Applies to Authorization Request Response/0110 messages.</p>		√				
25	<p>Contains 120 indicating an error in DE 120 (Record Data) and a three-digit code (such as 120xxx, where xxx indicates the field in the file update request where the error occurred). A listing of these codes can be found in the Error Codes section for DE 120. Applies to Issuer File Update Request Response/0312 messages.</p>	√	√	√	√	√	√
27	<p>Contains a 120 indicating an error in DE 120 and a three-digit code (such as 120xxx, where xxx indicates the field in the file update request where the error occurred). A listing of these codes can be found in the Error Codes section for DE 120. Applies to Issuer File Update Request Response/0312 messages.</p>	√	√	√	√	√	√
30	<p>Contains the data element in error when a format error is detected (For example, if the error is in one of the subelements of DE 48, 048 will be shown). Applies to all response messages.</p>	√	√	√	√	√	√

## Data Element Definitions

### DE 45—Track 1 Data

IF DE 39 is...	THEN DE 44 Contains...	MC	NP	VI	TE	MS	CI
57	Contains 003 indicating an error in DE 3 (Processing Code) when an issuer is unable to process a balance inquiry (30), purchase with cash back (09), purchase return (20), or payment (28) transaction type.	✓	✓	✓		✓	✓
85	Used in electronic commerce transactions, contains the date and time after which a cardholder may re-apply for a certificate. Format is YYYYMMDDHH. HH is the 24-hour military clock.		✓		✓		✓

### DE 45—Track 1 Data

DE 45 (Track 1 Data) is the information encoded on track 1 of the card's magnetic stripe as defined in the ISO 7813 specification, including data element separators but excluding beginning and ending sentinels and LRC characters as defined in this data element definition.

#### Attributes

Length of Length Field:	2
Data Representation:	ans...76; LLVAR
Data Field:	Contents of positions 1–76
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of DE 45 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	O	•	O
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C

#### Values

Whenever DE 45 is captured automatically at the point of interaction, this data element must contain whatever is encoded on the magnetic stripe (track 1) of the card, regardless of whether the card has been properly encoded with information in accordance with ISO specifications.

The ISO 7810, 7811, 7812, and 7813 specifications document the international standards for encoding information on magnetic stripe cards.

Length subelement must not be greater than 76 bytes.

The account number in DE 2 (Primary Account Number) or DE 34 (Primary Account Number [PAN], Extended) must match the account number in DE 45.

### **Application Notes**

This data element is defined and used identically within all MasterCard programs and services.

DE 45 is optional for 0120 AFD completion advice. Please refer to *AFD Completion* for more information.

Field ID and Name	F = Fixed V = Variable	Maximum Length
1 Start Sentinel	F	n-1
2 Format Code-B (encode character B)	F	an-1
3 Primary Account Number	V	n...19
4 Separator (binary)	F	ans-1
5 Cardholder name	V	ans...2-26
6 Separator (binary)	F	ans-1
7 Expiration Date	F	ans-4
8 Extended Service Code	F	ans-3
9 Discretionary Data (must include CVC 1)	V	Balance of available digits not to exceed total track length of 79 characters.
10 End Sentinel	F	n-1
11 Longitudinal Redundancy Check	F	n-1

Please refer to the following for additional Track 1 data information depending on the acceptance brand for the PAN:

- *Security Rules and Procedures*
- *Cirrus Worldwide Operating Rules*
- *Maestro Global Rules*

## Data Element Definitions

### DE 46—Expanded Additional Amounts

---

## DE 46—Expanded Additional Amounts

DE 46 (Additional Data—ISO Use) provides data supplemental to that already conveyed in the specific data elements in the message.

---

### Attributes

---

Length of Length Field:	3
Data Representation:	ans...999; LLLVAR
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

---

### Usage

---

The Authorization Platform currently does not use this data element.  
This data element is reserved for future definition and use.

---

## DE 47—Additional Data—National Use

DE 47 (Additional Data—National Use) is reserved for national organizations to define data unique to country applications.

---

### Attributes

---

Length of Length Field:	3
Data Representation:	ans...999; LLLVAR
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

---

### Usage

---

The Authorization Platform currently does not use this data element. ISO reserves this data element for future definition and use.

---

### Values

---

N/A

---

### Application Notes

---

This data element should not be present in any Authorization Platform messages. However, if encountered in Authorization Platform messages routed between customers of the same country, it is passed unaltered through the network. The Authorization Platform performs no editing or processing functions on this data element.

---

## **DE 48—Additional Data—Private Use**

DE 48 (Additional Data—Private Use) is reserved for private organizations to define data unique to specific networks or specific programs and services. DE 48 provides other supplemental data in a message when a specific ISO-designated data element is not available. It is a free-format, variable-length data element that may be used for multiple purposes.

---

### **Attributes**

---

Length of Length Field:	3
Data Representation:	ans...999; LLIVAR Although this data element is ans, some subelements deviate from ans and contain binary data. Please refer to subelement descriptions of each subelement. The length field must be in the range 001–999. Subelements are identified by valid subelement ID and length.
Data Field:	Contents of subelements
Subelements:	99
Justification:	See “Subelements”

---

### **Usage**

---

The following applies to DE 48 usage:

- Subelements may occur as many times as needed based on the program or service used.
- Subelements do not need to be in any particular order or sequence within DE 48.
- Customers must be able to send and receive all subelements available within DE 48.

Following is the overall usage of DE 48 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	X	M
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	M	X	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Reversal Request/0400	M	X	M

## Data Element Definitions

### DE 48—Additional Data—Private Use

Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	C	C
Administrative Advice/0620	•	C	C
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request Response/0810—PEK Exchange	M	M	•
Network Management Advice/0820	•	C	C
Network Management Advice/0820—PEK Exchange	•	M	M

#### Values

The length field must be in the range 001–999. Subelements are identified by valid subelement “ID” and “length”.

For Network Management Request/0800 messages, ID values in the range 00–69 are universally defined by CIS for use by all programs and services, and 70–99 are defined within individual programs and services only.

#### Application Notes

MasterCard may occasionally introduce new DE 48 subelements between releases to facilitate special processing within a country, region, or among pilot participants. MasterCard requires customers to be able to successfully process various online messages that may contain new unannounced DE 48 subelements.

This data element's content may vary by program and service. Additional or supplemental information that may be required in a transaction message is specified in Authorization Platform Edits for this data element.

For information on other uses of this data element, refer to the message layouts.

## DE 48 Transaction Category Code

In Authorization/01XX and Reversal/04XX messages, the format is “LLLt,” where “t” is the transaction category code (TCC). The message must contain an appropriate TCC as the first byte of data after the length within DE 48. The TCC classifies major categories of transactions, such as “Retail Sale,” “Cash Disbursement,” and “Mail Order.” The TCC must be selected from one of the values listed below.

TCC	Description	MC	NP	VI	TE	MS	CI
Space	A value of space in place of a valid TCC requests that the Authorization Platform perform the TCC assignment.	✓	✓	✓	✓	✓	✓
A	Auto/Vehicle Rental	✓	✓	✓	✓	✓	
C	Cash Disbursement	✓	✓	✓	✓	✓	✓
F	Restaurant	✓	✓	✓	✓	✓	

**Data Element Definitions**  
**DE 48—Additional Data—Private Use**

---

TCC	Description	MC	NP	VI	TE	MS	CI
H	Hotel/Motel	✓	✓	✓	✓	✓	
O	Hospitalization, College	✓	✓	✓	✓	✓	
P	Payment Transaction	✓	✓			✓	✓
R	Retail Sale	✓	✓	✓	✓	✓	
T	Phone, Mail, or Electronic Commerce Order	✓	✓	✓	✓	✓	✓
U	Unique	✓	✓	✓	✓	✓	✓
X	Airline and Other Transportation Services	✓	✓	✓	✓	✓	
Z	ATM Cash Disbursement	✓	✓	✓	✓	✓	✓

**NOTE**

MasterCard will optionally assign the Transaction Category Code (TCC) in DE 48 (Additional Data—Private Use) of authorization messages on behalf of an acquirer. All acquirers processing through the MasterCard Worldwide Network may choose to have the Authorization Platform assign the TCC in authorization messages on their behalf.

## DE 48 Subelement Encoding Scheme in Authorization Request/0100 Messages

The following table identifies the structure of the DE 48 subelement encoding scheme in the Authorization Request/0100 message.

LLL	"VAR"—999 maximum bytes (TCC + Subelement Data)						
3 bytes	1 byte	2 bytes	2 bytes	1–99 bytes	2 bytes	2 bytes	
		SE ID + Length + Data will not exceed 103 bytes			SE ID + Length + Data will not exceed 103 bytes		
Total Data Element Length	TCC	First Subelement (SE) Data			Second Subelement (SE) Data		
		SE ID	SE Length	SE Variable Length Data	SE ID	SE Length	
<b>mandatory</b>		SE Variable Length Data					
<b>1002 maximum bytes (LLL + TCC + Subelement Data)</b>							

## Data Element Definitions

### DE 48—Additional Data—Private Use

Number of Bytes	Attribute	Description
3	Total Data Element Length	The “LLL” portion of the data element up to 999
1	Transaction Category Code (TCC)	Must be a valid TCC or a space
2	Subelement ID	In the range 00–99
2	Subelement Length	In the range of 01–99
1...99	Subelement Variable Length Data	Contains valid values.

### DE 48 Subelement Encoding Scheme in Network Management Messages

The table below identifies the structure of the DE 48 subelement encoding scheme in Network Management messages.

LLL	“VAR”—999 maximum bytes (Subelement Data)					
3 bytes	2 bytes	2 bytes	1–96 bytes	2 bytes	2 byte	1–96 bytes
Total Data Element Length	First Subelement (SE) Data			Second Subelement (SE) Data		
	SE ID	SE Length	SE Variable Length Data	SE ID	SE Length	SE Variable Length Data
1002 maximum bytes (LLL + Subelement Data)						

Number of Bytes	Attribute	Description
3	Total Data Element Length	The “LLL” portion of LLLVAR
2	Subelement ID	In the range 00–99
2	Subelement Length	In the range of 01–96
1...96	Subelement Variable Length Data	Contains valid values.

### List of DE 48 Subelements

DE 48 subelements are listed in numeric order. Subelements that are specific to a brand service or program are clearly indicated in the subelement title or description or both.

**Data Element Definitions**  
**DE 48—Additional Data—Private Use**

---

<b>Subelement ID and Name</b>	<b>Data Representation</b>
10      Encrypted PIN Block Key	an...16
11      Key Exchange Block Data (Single-length Keys)	an-38
11      Key Exchange Block Data (Double-length Keys)	an-54
11      Key Exchange Block Data (Triple-length Keys)	an-70
12      Routing Indicator	a-1
13      MasterCard Hosted Mobile Phone Top-up Request Data	ans-47
14      Reserved for Future Use	N/A
15      Authorization Platform Advice Date and Time	n-10
16      Processor Pseudo ICA	n-7
17–19    Reserved for Future Use	N/A
20      Cardholder Verification Method	a-1
21–22    Reserved for Future Use	N/A
23      Payment Initiation Channel	an-2
25      MasterCard Cash Program Data	ans...14
26–31    Reserved for Future Use	N/A
32      MasterCard Assigned ID	an-6
33      PAN Mapping File Information	ans..43
34      Dynamic CVC 3 ATC Information	an-11
35 <i>PayPass</i> Non-Card Form Factor Request/Response	an-1
36      Visa Defined Data (Visa Only)	an-14
37      Reserved for Future Use	N/A
38      Account Category	an-1
39      Expert Monitoring Compromised Account Service Information	ans-30
40      Electronic Commerce Merchant/Cardholder Certificate Serial Number (Visa Only)	n...40
41      Electronic Commerce Certificate Qualifying Information	ans...95
42      Electronic Commerce Indicators	n-7

**Data Element Definitions****DE 48—Additional Data—Private Use**

<b>Subelement ID and Name</b>	<b>Data Representation</b>
43 Universal Cardholder Authentication Field (UCAF)	ans...32
44 Visa 3-D Secure Electronic Commerce Transaction Identifier (XID) (Visa Only)	b-20
45 Visa 3-D Secure Electronic Commerce Transaction Response Code (Visa Only)	an-1
46 Card-Level Result (Visa Only)	an-2
47 MasterCard Payment Gateway Indicator	ans...8
48 Mobile Program Indicators	n-1
49–57 Reserved for Future Use	N/A
58 ATM Additional Data	ans-33
59–60 Reserved for Future Use	N/A
61 POS Data, Extended Condition Codes	n-5
62 Reserved for Future Use	N/A
63 Trace ID	ans-15
64 Transit Program	n-4
65–70 Reserved for Future Use	N/A
71 On-behalf Services	ans...40
72 Issuer Chip Authentication	b...16
73 MasterCard Internal Use Only	n...10
74 Additional Processing Information	an...30
75 Fraud Scoring Data	an...32
76 MasterCard Electronic Acceptance Indicator	a-1
77 Payment Transaction Type Indicator	an-3
78 U.S. Deferred Billing Indicator (Visa Only)	a-1
79 Chip CVR/TVR Bit Error Result	an...50
80 PIN Service Code	a-2
81 Reserved for Future Use	N/A
82 Address Verification Service Request	n-2
83 Address Verification Service Response	a-1

**Data Element Definitions**  
**DE 48—Additional Data—Private Use**

---

<b>Subelement ID and Name</b>	<b>Data Representation</b>
84 Merchant Advice Code	an-2
84 Visa Response Codes (Visa Only)	an-2
85 U.S. Existing Debt Indicator (Visa Only)	n-1
86 Relationship Participant Indicator (Visa Only)	a-1
87 Card Validation Code Result	a-1
87 CVV2 Response (Visa Only)	a-1
88 Magnetic Stripe Compliance Status Indicator	a-1
89 Magnetic Stripe Compliance Error Indicator	a-1
90 Lodging and Auto Rental Indicator	a-1
90 Custom Payment Service Request (Visa Only)	a-1
91 Custom Payment Service Request Transaction ID (Visa Only)	an...19
91 Custom Payment Service Response Transaction ID (Visa Only)	an...19
91 Acquirer Reference Data (American Express Only)	ans...15
92 CVC 2	n-3
92 CVV2 Data (Visa Only)	n-6
93 Fleet Card ID Request Data (Visa Only)	ans...19
94 Commercial Card Inquiry Request (Visa Only)	ans-4
94 Commercial Card Inquiry Response (Visa Only)	ans-4
95 MasterCard Promotion Code	an-6
95 American Express Customer ID Number (American Express Only)	n-4
96 Visa Market-specific Data Identifier (Visa Only)	a-1
97 Prestigious Properties Indicator (Visa Only)	a-1
98 MasterCard Corporate Fleet Card® ID/Driver Number	n-6
99 MasterCard Corporate Fleet Card® Vehicle Number	n-6

## **Subelement 10—Encrypted PIN Block Key**

Subelement 10 (Encrypted PIN Block Key) contains 16 hexadecimal characters in the range 0–9 and A–F to represent the 16 bits of a PIN block key encrypted under another key. Individual network, program, or service rules define the other encryption key.

### **Attributes**

Subelement ID:	10
Length of Length Field:	2
Data Representation:	an...16
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

### **Usage**

The Authorization Platform currently does not use this subelement.

## **Subelement 11—Key Exchange Block Data (Single-Length Keys)**

Subelement 11 (Key Exchange Block Data [Single-Length Keys]) contains a data block specifically formatted to contain all the control data, encrypted key data, and key check values to complete an encryption key change operation between any two processors (for example, between a CPS or INF and the network).

### **Attributes**

Subelement ID:	11
Length of Length Field:	2
Data Representation:	an-38
Data Field:	Contents of subfields 1–5
Subfields:	5
Justification:	N/A

### **Usage**

Following is the usage of subelement 11 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request Response/0810—PEK Exchange	M	M	•

---

**Values**

---

Subelement 11 must be encoded for subfields 1–5 defined as follows:

---

**Subfield 1 (Key Class ID)**

---

Data Representation: an-2

---

Data Field: Contents of positions 1–2

---

Values: PK (PIN key)

---

**Subfield 2 (Key Index Number)**

---

Data Representation: n-2

---

Data Field: Contents of positions 3–4

---

Values: 00

---

**Subfield 3 (Key Cycle Number)**

---

Data Representation: n-2

---

Data Field: Contents of positions 5–6

---

Values: 00-99 (sequential)

---

**Subfield 4 (PIN Encryption Key [PEK])**

---

Data Representation: an-16

---

Data Field: Contents of positions 7–22

---

Values: hex, 0–9, A–F

---

**Subfield 5 (Key Check Value)**

---

Data Representation: an-16

---

Data Field: Contents of positions 23–38

---

Values: hex, 0–9, A–F

---

## **Subelement 11—Key Exchange Block Data (Double-Length Keys)**

Subelement 11 (Key Exchange Block Data [Double-Length Keys]) contains a data block specifically formatted to contain all the control data, encrypted key data, and key check values to complete an encryption key change operation between any two processors (for example, between a CPS or INF and the network).

---

**Attributes**

---

Subelement ID: 11

---

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Length of Length Field:	2
Data Representation:	an-54
Data Field:	Contents of subfields 1–5
Subfields:	5
Justification:	N/A

#### Usage

Following is the usage of subelement 11 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request Response/0810—PEK Exchange	M	M	•

#### Values

Subelement 11 must be encoded for subfields 1–5 defined as follows:

##### Subfield 1 (Key Class ID)

Data Representation:	an-2
Data Field:	Contents of positions 1–2
Values:	PK (PIN key)

##### Subfield 2 (Key Index Number)

Data Representation:	n-2
Data Field:	Contents of positions 3–4
Values:	00

##### Subfield 3 (Key Cycle Number)

Data Representation:	n-2
Data Field:	Contents of positions 4–6
Values:	00-99 (sequential)

##### Subfield 4 (PIN Encryption Key [PEK])

Data Representation:	an-32
Data Field:	Contents of positions 7–38
Values:	hex, 0–9, A–F

##### Subfield 5 (Key Check Value)

Data Representation:	an-16
----------------------	-------

Data Field:	Contents of positions 39–54
Values:	hex, 0–9, A–F

## Subelement 11—Key Exchange Block Data (Triple-Length Keys)

Subelement 11 (Key Exchange Block Data [Triple-Length Keys]) contains a data block specifically formatted to contain all the control data, encrypted key data, and key check values to complete an encryption key change operation between any two processors (for example, between a CPS or INF and the network).

---

### **Attributes**

---

Subelement ID:	11
Length of Length Field:	2
Data Representation:	an-70
Data Field:	Contents of subfields 1–5
Subfields:	5
Justification:	N/A

---

### **Usage**

---

Following is the usage of subelement 11 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request Response/0810—PEK Exchange	M	M	•

---

### **Values**

---

Subelement 11 must be encoded for subfields 1–5 as defined below:

---

#### **Subfield 1 (Key Class ID)**

---

Data Representation:	an-2
Data Field:	Contents of positions 1–2
Values:	PK (PIN key)

---

#### **Subfield 2 (Key Index Number)**

---

Data Representation:	n-2
Data Field:	Contents of positions 3–4
Values:	00

---

#### **Subfield 3 (Key Cycle Number)**

---

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Data Representation:	n-2
----------------------	-----

Data Field:	Contents of positions 5–6
-------------	---------------------------

Values:	00-99 (sequential)
---------	--------------------

#### **Subfield 4 (PIN Encryption Key [PEK])**

Data Representation:	an-48
----------------------	-------

Data Field:	Contents of positions 7–54
-------------	----------------------------

Values:	hex, 0–9, A–F
---------	---------------

#### **Subfield 5 (Key Check Value)**

Data Representation:	an-16
----------------------	-------

Data Field:	Contents of positions 55–70
-------------	-----------------------------

Values:	hex, 0–9, A–F
---------	---------------

## Subelement 12—Routing Indicator

Subelement 12 (Routing Indicator) is defined and derived by the Authorization Platform and passed to the issuer to indicate that alternate issuer host routing has been invoked. Subelement 12 is applicable only to issuers that use an alternate issuer host route instead of the Stand-In System.

---

### **Attributes**

Subelement ID:	12
----------------	----

Length of Length Field:	2
-------------------------	---

Data Representation:	a-1
----------------------	-----

Data Field:	Contents of position 1
-------------	------------------------

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

---

### **Usage**

Following is the usage of subelement 12 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:	Org	Sys	Dst
--	-----	-----	-----

Authorization Request/0100	•	X	C
----------------------------	---	---	---

---

### **Values**

A = Alternate issuer host routing
-----------------------------------

P = Primary issuer host routing
---------------------------------

## **Subelement 13—MasterCard Hosted Mobile Phone Top-up Request Data**

Subelement 13 (MasterCard Hosted Mobile Phone Top-up Request Data) contains the mobile phone number and mobile phone service provider name.

---

### **Attributes**

---

Subelement ID:	13
Length of Length Field:	2
Data Representation:	ans-47
Data Field:	Contents of subfields
Subfields:	2
Justification:	See “Subfields”

---

### **Usage**

---

Following is the usage of subelement 13 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE

---

## **Subfield 1—Mobile Phone Number**

DE 48, subelement 13, subfield 1 contains the phone number of the wireless phone for which the customer is purchasing extra service.

---

### **Attributes**

---

Data Representation:	ans-17
Data Field:	Contents of positions 1–17
Justification:	Left

---

### **Values**

---

Cannot contain all spaces or all zeros.

---

### **Application Notes**

---

Subfield 1 is logged and displayed as asterisks by the eService Transaction Research tool.

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Subfield 2—Mobile Phone Service Provider Name

DE 48, subelement 13, subfield 2 contains the name or other identifier of the mobile phone service provider.

---

##### Attributes

---

Data Representation: ans-30

---

Data Field: Contents of positions 18–47

---

Justification: Left

---

##### Values

---

Cannot contain all spaces or all zeros.

---

#### Subelement 15—Authorization System Advice Date and Time

DE 48, subelement 15 (Authorization System Advice Date and Time), (in UTC units) is a transaction “time stamp” the Authorization Platform supplies for each Authorization Advice/0120-Acquirer-generated message. It indicates the date and time that the advice is entered into the network.

---

##### Attributes

---

Subelement ID 15

---

Length of Length Field: 2

---

Data Representation: n-10

---

Data Field: Contents of subfields 1–2

---

Subfields: 2

---

Justification: See “Subfields”

---

##### Usage

---

Following is the usage of subelement 15 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Advice/0120—Acquirer-generated	•	X	M
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME

##### Values

---

See “Subfields.”

---

---

#### **Application Notes**

---

Acquirers may use the contents of subelement 15 to aid in the creation of the clearing message.

---

#### **Subfield 1—Date**

DE 48, subelement 15, subfield 1 (Date) contains the valid date of the Authorization Advice/0120—Acquirer-generated inserted by the Authorization Platform.

---

#### **Attributes**

---

Data Representation:	n-4
Data Field:	Contents of positions 1–4
Justification	N/A
Values:	This subfield contains a valid date in MMDD format.

---

#### **Subfield 2—Time**

DE 48, subelement 15, subfield 2 (Time) contains the valid time of the Authorization Advice/0120-Acquirer-generated inserted by the Authorization Platform.

---

#### **Attributes**

---

Data Representation:	n-6
Data Field:	Contents of positions 5–10
Justification	N/A
Values:	This subfield contains a valid time in hhmmss format.

---

### **Subelement 16—Processor Pseudo ICA**

DE 48, subelement 16 (Processor Pseudo ICA) identifies the institution submitting a request or advice that is not the same as the institution provided in DE 32 (Acquiring Institution ID Code) or DE 33 (Forwarding Institution ID Code).

---

#### **Attribute**

---

Subelement ID	16
Length of Length Field:	2
Data Representation:	n-7

---

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Data Field:	N/A
-------------	-----

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

#### Usage

Following is the usage of DE 48, subelement 16 (whether it is mandatory, conditional, optional, system-provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Advice/0120—Acquirer-generated	•	X	C
Authorization Advice/0120—System-generated	•	X	C

#### Application Notes

The Authorization Platform populates this subelement based on the institution submitting the transaction and the issuer's preference for receipt of this data.

---

## Subelement 20—Cardholder Verification Method

Acquirers use subelement 20 (Cardholder Verification Method) to notify MasterCard that the original transaction is signature/offline PIN-based, no CVM used, or online PIN-based for transaction routing in Authorization Advice/0120—Acquirer-generated and Reversal Request/0400 messages.

---

#### Attributes

Subelement ID:	20
----------------	----

Length of Length Field:	2
-------------------------	---

Data Representation:	a-1
----------------------	-----

Data Field:	Contents of position 1
-------------	------------------------

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

#### Usage

Following is the usage of subelement 20 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Advice/0120—Acquirer-generated	M	X	•
Reversal Request/0400	M	X	•

#### Values

---

P	=	Online PIN verification
S	=	Can signify signature, “Offline PIN verification” (for chip card transactions) or “No CVM used”

## **Subelement 23—Payment Initiation Channel**

DE 48, subelement 23 (Payment Initiation Channel) provides information about the device type used to initiate a non-card transaction.

<b>Attribute</b>	<b>Description</b>
Subelement ID:	23
Length of Length Field:	2
Data Representation:	an-2
Data Field:	Contents of subfield 1
Subfields:	1
Justification:	N/A

### **Usage**

Following is the usage of subelement 23 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	O	•	C
Authorization Advice/0120	C	•	C
Reversal Request/0400		•	C C

### **Values**

See subfield 1.

## **Subfield 1—Device Type**

DE 48, subelement 23, subfield 1 (Device Type) indicates the type of device used at the terminal.

<b>Attribute</b>	<b>Description</b>
Data Representation:	an-2
Data Field:	Contents of positions 1–2
Justification:	N/A

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Values

---

00 = Card (default)  
01 = Mobile Phone or Smartphone  
02 = Key Fob  
03 = Watch  
04 = Mobile Tag  
05 = Wristband  
06 = Mobile Phone Case or Sleeve  
07–99 = Reserved for Future Use

---

### Subelement 25—MasterCard Cash Program Data

Subelement 25 (MasterCard Cash Program Data) contains information necessary to process MasterCard Cash transactions, which includes message type identifiers.

Attribute	Description
Subelement ID:	25
Length of Length Field:	2
Data Representation:	ans...14; LLVAR
Data Field:	Contents of subfields
Subfields:	1
Justification:	See “Subfields”

---

#### Usage

---

Following is the usage of subelement 25 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C

---

#### Values

---

See subfields.

---

### Subfield 01—Message Identifier

DE 48, subelement 25, subfield 01 (Message Identifier) indicates the type of cash transaction.

<b>Attribute</b>	<b>Description</b>
Subfield ID:	01
Length of Length Field:	2
Data Representation:	ans...10
Data Field:	Contents of positions 1–2, positions 3–10 undefined
Justification:	N/A
<b>Values</b>	
LR = Unlinked load request, or linked load request with no purchase	
LP = Linked load request with a purchase	
LU = Linked status update	
CM = Confirmation message	

## **Subelement 32—MasterCard Assigned ID**

Subelement 32 (MasterCard Assigned ID) contains the merchant ID assigned by MasterCard.

<b>Attributes</b>	
Subelement ID:	32
Length of Length Field:	2
Data Representation:	an-6
Data Field:	Contents of positions 1–6
Subfields:	N/A
Justification:	N/A

Usage	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Values

---

The MasterCard Assigned ID should always be a value assigned by MasterCard, and is the same value in both the Authorization and Clearing systems. MasterCard assigns one ID to the merchant regardless if the merchant is participating in multiple programs. This field is required when transactions are submitted for real-time substantiation. Real-time substantiation is indicated by DE 48, subelement 61, subfield 3 (Real-time Substantiation Indicator) containing a value of 1 (Merchant terminal verified the purchased items against the Inventory Information Approval System [IIAS]).

In addition, the MasterCard Assigned ID can be used with the Private Label Merchant Verification Service if the issuer chooses to do so. Merchant Verification Service for Private Label transactions is performed using either DE 42 or DE 48, subelement 32. Acquirers are required to contact their merchant or their private label issuer to learn more about the Private Label Merchant Verification Service and whether DE 42 or DE 48, subelement 32 is used in this service.

Participating merchants must submit the MasterCard Assigned ID for e-commerce transactions that are processed under the Maestro® Advance Registration Program™, the MasterCard® Advance Registration Program™, the Maestro Recurring Payments Program, and the MasterCard® Utility Payment Program.

---

## Subelement 33—PAN Mapping File Information

DE 48, subelement 33 (PAN Mapping File Information) supports the mapping between the virtual account data and actual account data.

---

#### Attributes

---

Subelement ID:	33
Length of Length Field:	2
Data Representation:	an...43; LLVAR
Data Field:	Contents of subfields 1-4
Subfields:	4
Justification:	See “Subfields”

---

#### Usage

---

Following is the usage of subelement 33 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Request Response/0110	•	X	C
Authorization Advice/0120—Acquirer-generated	•	X	C
Authorization Advice/0120—Issuer-generated	C	C	•

Authorization Advice/0120—System-generated	•	X	C
Authorization Advice Response/0130—Issuer-generated	C	•	C
Reversal Request/0400	•	X	C
Reversal Request Response/0410	•	X	C
Reversal Advice/0420	•	X	C
<b>Values</b>			
See “Subfields”			
<b>Application Notes</b>			
<p>The Authorization Platform inserts this subelement when PAN Mapping Service was performed on the transaction. Subelement 33 may be used for research or audit purposes but need not be used for processing authorization messages. Subfields 1-2 are always present, subfields 3-4 are conditional.</p> <p>Acquirers may receive subelement 33 in Magnetic stripe, Contact M/Chip, or <i>PayPass</i> M/Chip transactions when the issuer is participating in the <i>PayPass</i> Mapping Service. Acquirers do not receive subelement 33 for the MasterCard inControl Purchase Control Service or MasterCard inControl Virtual Card Spend Control Service.</p> <p>Issuers that issue <i>PayPass</i> cards or devices that provide a primary account number (PAN) within a transaction different than what is embossed on the card, must ensure that the following is returned in Authorization Request Response/0110 messages when responding back to transit post-authorized aggregated transactions:</p> <ul style="list-style-type: none"> <li>• The value E in DE 48, subelement 33, subfield 1 (Account Number Indicator)</li> <li>• The embossed number in DE 48, subelement 33, subfield 2 (Account Number)</li> <li>• The card expiration date of the embossed number in DE 48, subelement 33, subfield 3 (Expiration Date)</li> </ul>			

### **Subelement 33 Encoding Scheme**

The following table illustrates the structure of DE 48, subelement (SE) 33 when all four subfields (SF) are present and when only subfields one and two are present.

The following table illustrates the structure of DE 48, subelement 33 when all four subfields are present.

<b>“VAR”—43 maximum bytes (continues)...</b>											
2 bytes	2 bytes	2 bytes	2 bytes	1 byte	2 bytes	2 bytes	12...19 bytes	2 bytes	2 bytes	4 bytes	
SE ID 33	SE Length	SF ID 01	SF Length	SF Data	SF ID 02	SF Length	SF Data	SF ID 03	SF Length	SF Data	

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

...continued) "VAR"—43 maximum bytes		
2 bytes	2 bytes	3 bytes
SF ID 04	SF Length	SF Data

The following table illustrates the structure of DE 48, subelement 33 when only subfields one and two are present.

"VAR"—28 maximum bytes									
2 bytes	2 bytes	2 bytes	2 bytes	1 byte	2 bytes	2 bytes	12...19 bytes	SF ID 03 Not present	SF ID 04 Not present
SE ID 33	SE Length	SF ID 01	SF Length	SF Data	SF ID 02	SF Length	SF Data		

#### Subfield 1—Account Number Indicator

DE 48, subelement 33, subfield 1 (Account Number Indicator) indicates the type of PAN mapping account.

---

##### Attributes

---

Subfield ID: 01

---

Length of Length Field: 2

---

Data Representation: an-1

---

Data Field: Contents of subfield 1

---

Justification: N/A

---

##### Values

---

E = Embossed Account Number Provided by Issuer

L = Pay with Rewards Loyalty Program Operator [LPO] card

M = Primary Account Number

P = *PayPass* Account Number

R = Pay with Rewards card

V = Virtual Card Number

---

#### Subfield 2—Account Number

DE 48, subelement 33, subfield 2 (Account Number) indicates the PAN mapping account numbers.

---

##### Attributes

---

Subfield ID: 02

---

Length of Length Field:	2
Data Representation:	n...19; LLVAR
Data Field:	Contents of subfield 2
Justification:	N/A

**Values**

Acquirer message = Contains actual number  
Issuer message = Contains virtual number  
For *PayPass* transit transactions, subfield 2 is the embossed number rather than the virtual number, if subfield 1 value is E.

### **Subfield 3—Expiration Date**

DE 48, subelement 33, subfield 3 (Expiration Date) indicates the expiration date of the PAN mapping accounts.

**Attributes**

Subfield ID:	03
Length of Length Field:	2
Data Representation:	n-4; format YYMM
Data Field:	Contents of subfield 3

Justification: N/A

**Values**

Acquirer message =	May contain actual expiration date only if issuer provided in MCC106 (PAN Mapping File) or in transit post-authorized aggregated authorization responses.
Issuer message =	May contain virtual expiration date only if acquirer provided in DE 14 of the authorization message. For <i>PayPass</i> transit transactions, subfield 3 is the expiration date of the embossed number rather than the virtual number, if subfield 1 value is E.

### **Subfield 4—Product Code**

DE 48, subelement 33, subfield 4 (Product Code) may indicate the product code for subfield 2 account number.

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Attributes

Subfield ID:	04
Length of Length Field:	2
Data Representation:	an-3
Data Field:	Contents of subfield 4
Justification:	N/A

#### Values

---

Subfield 4 may contain product code for subfield 2 account number.

---

## Subelement 34—Dynamic CVC 3 ATC Information

Subelement 34 (Dynamic CVC 3 ATC Information) supports the *PayPass* Dynamic CVC 3 On-behalf Services.

---

#### Attributes

Subelement ID:	34
Length of Length Field:	2
Data Representation:	an-11
Data Field:	Contents of subfields 1-3
Subfields:	3
Justification:	See “Subfields”

---

#### Usage

Following is the usage of subelement 34 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Advice/0120—System-generated	•	X	C

---

#### Values

---

See “Subfields”

---

#### **Application Notes**

The Authorization Platform inserts this subelement when the *PayPass Dynamic CVC 3 Pre-validation Service* or *Dynamic CVC 3 Validation in Stand-In Processing Service* was performed on the transaction and the validation result was V (Valid), A (ATC outside allowed range), or E (CVC 3 ATC Replay).

These results are found in DE 48, subelement 71, subfield 2 (On-behalf [OB] Result 1). Subelement 34 should be used for processing authorization messages and maintaining the ATC values on the issuer host. Subfields 1–3 are always present.

---

#### **Subfield 1—ATC Value**

DE 48, subelement 34, subfield 1 (ATC Value) contains the derived full ATC Value used in the validation.

---

#### **Attributes**

---

Data Representation:	n-5
Data Field:	Contents of subfield 1
Justification:	Right-justified, leading zeros

---

#### **Subfield 2—ATC Discrepancy Value**

DE 48, subelement 34, subfield 2 (ATC Discrepancy Value) is the differential between the transaction ATC and the maximum value allowed by the issuer when the transaction ATC is above the previous ATC, or the differential between the transaction ATC and the minimum value allowed by the issuer when the transaction ATC is below the previous ATC. ATC Discrepancy Value will be zero when the transaction ATC is within the issuer-defined limits.

---

#### **Attributes**

---

Data Representation:	n-5
Data Field:	Contents of subfield 2
Justification:	Right-justified, leading zeros

---

#### **Subfield 3—ATC Discrepancy Indicator**

DE 48, subelement 34, subfield 3 (ATC Discrepancy Indicator) indicates if the ATC Discrepancy Value is above, below or within the maximum values allowed by the issuer.

---

#### **Attributes**

---

Data Representation:	an-1
----------------------	------

---

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Data Field:	Contents of subfield 3
Justification:	N/A
<b>Values</b>	
G =	Indicates that the ATC value is greater than the maximum value allowed
L =	Indicates that the ATC value is lower than the minimum value allowed
W =	Indicates that the ATC value is within the issuer defined limits

### Subelement 34 Subfield Data Examples

Following are examples of how data may appear in subfield 1, subfield 2, and subfield 3.

#### Example 1

Last valid ATC value processed by MasterCard was 00011.

Issuer provided a maximum allowed range of 00035.

$00011 + 00035 = 00046$ , which represents the maximum ATC value, allowed in the next transaction.

The derived value of the ATC in the next transaction is 00088.

The ATC Discrepancy Value for this transaction is 42 which represents the difference between the maximum ATC value allowed 00046 and the derived ATC value from the transaction 00088.

Subelement 34 will contain the following:

- Subfield 1 = 00088
- Subfield 2 = 00042
- Subfield 3 = G

#### Example 2

Last valid ATC value processed by MasterCard was 00068.

Issuer provided a minimum allowed range of 00035.

$00068 - 00035 = 00033$ , which represents the minimum ATC value allowed in the next transaction.

The derived value of the ATC in the next transaction is 00020.

The ATC Discrepancy Value for this transaction is 13, which represents the difference between the minimum ATC value allowed 00033 and the derived ATC value from the transaction 00020.

Subelement 34 will contain the following:

- Subfield 1 = 00020
- Subfield 2 = 00013
- Subfield 3 = L

### **Example 3**

Last valid ATC value processed by MasterCard was 00037.

Issuer provided a maximum allowed range of 00005.

00037 + 00005 = 00042, which represents the maximum ATC value allowed in the next transaction.

The derived value of the ATC in the next transaction is 00040.

The ATC Discrepancy Value for this transaction is 0 because the derived value of the ATC in the next transaction 00040 is greater than the last valid ATC value 00037 and below the maximum ATC value allowed in the next transaction 00042.

Subelement 34 will contain the following:

- Subfield 1 = 00040
- Subfield 2 = 00000
- Subfield 3 = W

## **Subelement 35—PayPass Non-Card Form Factor Request/Response**

Subelement 35 (*PayPass Non-Card Form Factor Request/Response*) supports *PayPass Mapping Service*.

---

### **Attributes**

---

Subelement ID:	35
Length of Length Field:	2
Data Representation:	an-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

---

### **Usage**

---

Following is the usage of subelement 35 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Org    Sys    Dst

## Data Element Definitions

### DE 48—Additional Data—Private Use

Authorization Request/0100	•	X	C
Authorization Request Response/0110	C	C	•

#### Values

The *PayPass* issuer will receive the Authorization Request/0100 message containing DE 48, subelement 35, value R (Cardholder request for device).

The *PayPass* issuer should respond with an Authorization Request Response/0110 message containing DE 48, subelement 35, value A (Approve cardholder request for device) or D (Decline cardholder request for device).

#### Application Notes

Issuers choosing the *PayPass* Mapping Service “Processing and Issuance of devices” participation option (Passive Participation) will receive an Authorization Request/0100 message when a cardholder requests a *PayPass* device from the issuer-branded, secure Web site hosted by MasterCard. The issuer may then decide if the cardholder should receive the *PayPass* device.

The Authorization Platform will use the value in DE 48, subelement 35 of the Authorization Request Response/0110 message to issue the *PayPass* device or to decline the cardholder’s request.

If an issuer chooses not to support subelement 35, the issuer-branded Web site will evaluate the responses provided for AVS Only and CVC 2 and approve or decline the cardholder request based on those values.

## Subelement 36—Visa Defined Data (Visa Only)

DE 48, subelement 36 (Visa Defined Data [Visa Only]) supports the Visa-assigned Merchant Verification Value.

Attribute	Description
Subelement ID:	36
Length of Length Field:	2
Data Representation:	n-14
Data Field:	Contents of subfields
Subfields:	1
Justification:	See “Subfields”

#### Usage

Following is the usage of subelement 36 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Reversal Request/0400	C	•	C

**Values**

See “Subfields”.

**Subfield 1—Merchant Verification Value**

DE 48, subelement 36, subfield 1 (Merchant Verification Value) contains the merchant verification value for subelement 36.

---

**Attribute**                    **Description**

---

Subfield ID:                    01

---

Length of Length Field:    2

---

Data Representation:        an-10

---

Data Field:                    Contents of subfield 1.

---

Justification:                N/A

---

**Values**

---

0–9 and A–F

---

**Subelement 38—Account Category**

Subelement 38 (Account Category) supports Account Level Management.

---

**Attributes**

---

Subelement ID:                38

---

Length of Length Field:    2

---

Data Representation:        an-1

---

Data Field:                    Contents of positions 1

---

Subfields:                    NA

---

Justification:                NA

---

**Usage**

---

Following is the usage of subelement 38 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Reversal Advice/0420	•	C	C
<b>Values</b>			
B = Enhanced Value (Enhanced Value and High Spend)			
M = Enhanced Value (Enhanced Value and High Spend) and Product Graduation			
P = Product Graduation (or the Co-brand Proprietary card program)			
S = High Value (High Value, Enhanced Value for Small Business and Premium High Spend)			
T = High Value (High Value, Enhanced Value for Small Business and Premium High Spend) and Product Graduation			
W = World Elite Spend Shortfall			
Y = Product Graduation and World Elite Spend Shortfall			
Z = The default value provided by MasterCard indicating that while the account range does participate in Account Level Management processing, the specific cardholder account found in DE 2 (Primary Account Number [PAN]) of the transaction does not participate in Account Level Management processing.			
<b>Application Notes</b>			
The Authorization Platform derives the specific value from information submitted by the issuer.			

### Subelement 39—Expert Monitoring Compromised Account Service Information

DE 48, subelement 39 (Expert Monitoring Compromised Account Service Information) contains confirmed or suspected account data compromise event information for account ranges participating in the Expert Monitoring Compromised Account Service.

<b>Attributes</b>			
Subelement ID:	39		
Length of Length Field:	2		
Data Representation:	ans-30		
Data Field:	Contents of positions 1–30		
Subfields:	N/A		
Justification:	Left		
<b>Usage</b>			

Following is the usage of subelement 39 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Advice/0120—System-generated	•	X	C

#### **Positions 1–3 (Threat Score)**

Data Representation:	n-3
Data Field:	Contents of positions 1–3
Values:	000 = Threat score not available 001–999 = Threat score indicating the likelihood that the account will experience fraud due to the compromise(s) in which the account was exposed.
<b>Positions 4–6 (Threat Score Days Elapsed)</b>	

Data Representation:	n-3
Data Field:	Contents of positions 4–6
Values:	Number of days since the threat score was refreshed

#### **Positions 7–12 (Case Key Code #1)**

Data Representation:	ans-6
Data Field:	Contents of positions 7–12
Values:	Unique Key to Identify Case

#### **Positions 13–18 (Case Key Code #2)**

Data Representation:	ans-6
Data Field:	Contents of positions 13–18
Values:	Unique Key to Identify Case

#### **Positions 19–24 (Case Key Code #3)**

Data Representation:	ans-6
Data Field:	Contents of positions 19–24
Values:	Unique Key to Identify Case

#### **Positions 25 (Account Number)**

Data Representation:	n-1
Data Field:	Contents of positions 25

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Values:	0–9 = Number of events in which the account number has been exposed
---------	---

#### **Positions 26 (Expiration Date)**

Data Representation:	n-1
----------------------	-----

Data Field:	Contents of positions 26
-------------	--------------------------

Values:	0–9 = Number of events in which expiration date has been exposed
---------	--

#### **Positions 27 (CVC 2)**

Data Representation:	n-1
----------------------	-----

Data Field:	Contents of positions 27
-------------	--------------------------

Values:	0–9 = Number of events in which the CVC 2 has been exposed
---------	--

#### **Positions 28 (PIN)**

Data Representation:	n-1
----------------------	-----

Data Field:	Contents of positions 28
-------------	--------------------------

Values:	0–9 = Number of events in which the PIN has been exposed
---------	--

#### **Position 29 (Magnetic Stripe)**

Data Representation:	n-1
----------------------	-----

Data Field:	Contents of positions 29
-------------	--------------------------

Values:	0–9 = Number of events in which the Magnetic Stripe has been exposed
---------	--

#### **Position 30 (Personal Information)**

Data Representation:	n-1
----------------------	-----

Data Field:	Contents of positions 30
-------------	--------------------------

Values:	0–9 = Number of events in which the cardholder's personal information has been exposed
---------	--

## **Subelement 40—Electronic Commerce Merchant/Cardholder Certificate Serial Number (Visa Only)**

Subelement 40 (Electronic Commerce Merchant/Cardholder Certificate Serial Number) contains certificate information on electronic commerce transactions when applicable.

**Attributes**

Subelement ID:	40
Length of Length Field:	2
Data Representation:	n...40 (also contains binary data. See “Subfields.”)
Data Field:	Contents of subfield 1 or 2 or both
Subfields:	2
Justification:	N/A

**Usage**

Following is the usage of subelement 40 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Acquirer-generated	C	C	C
Authorization Advice/0120—System-generated	•	C	C

**Values**

Contains the contents of subfield 1 or subfield 2 or both.

### **Subfield 1—Merchant Certificate Serial Number**

DE 48, subelement 40, subfield 1 (Merchant Certificate Serial Number) is the Merchant Certificate Serial Number in binary data.

**Attributes**

Subfield ID:	01
Length of Length Field:	2
Data Representation:	b...16
Data Field:	Merchant Certificate Serial Number in binary data.
Positions:	N/A
Values:	Merchant specific: b...16

### **Subfield 2—Cardholder Certificate Serial Number**

DE 48, subelement 40, subfield 2 (Cardholder Certificate Serial Number) is the cardholder certificate serial number in binary format.

**Data Element Definitions****DE 48—Additional Data—Private Use****Attributes**

Subfield ID:	02
Length of Length Field:	2
Data Representation:	b...16
Data Field:	Cardholder Certificate Serial Number in binary data.
Positions:	N/A
Values:	Cardholder specific: b...16

**Subelement 41—Electronic Commerce Certificate Qualifying Information**

MasterCard discontinued use of subelement 41 (Electronic Commerce Certificate Qualifying Information) for submitting Electronic Commerce Certificate Qualifying Information. Subelement 41, subfields 1–10 and 12–18 are reserved for future use. Subelement 41, subfield 11 (Citizen ID) may contain Citizen ID (formerly National ID) information. Applicable only to domestic Venezuela transactions.

**Attributes**

Subelement ID:	41
Length of Length Field:	2 (value in the range of 05–95)
Data Representation:	ans...95; LLVAR
Data Field:	Contents of subfield(s)
Subfields:	18
Justification:	N/A

**Usage**

Following is the usage of subelement 41 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120	•	C	C

**Values**

See subfields.

### **Subfield 1—Reserved for Future Use**

DE 48, subelement 41, subfield 1 (Reserved for Future Use) is for future use.

---

#### **Attributes**

---

Subfield ID:	01
Length of Length Field:	2
Data Representation:	ans..26

---

### **Subfield 2—Reserved for Future Use**

DE 48, subelement 41, subfield 2 (Reserved for Future Use) is for future use.

---

#### **Attributes**

---

Subfield ID:	02
Length of Length Field:	2
Data Representation:	n-6

---

### **Subfield 3—Reserved for Future Use**

DE 48, subelement 41, subfield 3 (Reserved for Future Use) is for future use.

---

#### **Attributes**

---

Subfield ID:	03
Length of Length Field:	2
Data Representation:	n-3

---

### **Subfield 4—Reserved for Future Use**

DE 48, subelement 41, subfield 4 (Reserved for Future Use) is for future use.

---

#### **Attributes**

---

Subfield ID:	04
Length of Length Field:	2
Data Representation:	an...22

---

### **Subfield 5—Reserved for Future Use**

DE 48, subelement 41, subfield 5 (Reserved for Future Use) is for future use.

**Data Element Definitions****DE 48—Additional Data—Private Use**

---

**Attributes**

---

Subfield ID:	05
Length of Length Field:	2
Data Representation:	ans...20

---

**Subfield 6—Reserved for Future Use**

DE 48, subelement 41, subfield 6 (Reserved for Future Use) is for future use.

---

**Attributes**

---

Subfield ID:	06
Length of Length Field:	2
Data Representation:	a...13

---

**Subfield 7—Reserved for Future Use**

DE 48, subelement 41, subfield 7 (Reserved for Future Use) is for future use.

---

**Attributes**

---

Subfield ID:	07
Length of Length Field:	2
Data Representation:	a-3

---

**Subfield 8—Reserved for Future Use**

DE 48, subelement 41, subfield 8 (Reserved for Future Use) is for future use.

---

**Attributes**

---

Subfield ID:	08
Length of Length Field:	2
Data Representation:	an...10

---

**Subfield 9—Reserved for Future Use**

DE 48, subelement 41, subfield 9 (Reserved for Future Use) is for future use.

---

**Attributes**

---

Subfield ID:	09
--------------	----

---

Length of Length Field:	2
Data Representation:	a...22

### **Subfield 10—Reserved for Future Use**

DE 48, subelement 41, subfield 10 (Reserved for Future Use) is for future use.

---

#### **Attributes**

---

Subfield ID:	10
Length of Length Field:	2
Data Representation:	n-9

### **Subfield 11—Citizen ID**

DE 48, subelement 41, subfield 11 (Citizen ID) indicates the citizen ID.

---

#### **Attributes**

---

Subfield ID:	11
Length of Length Field:	2
Data Representation:	an...20
Data Field:	National ID
Values:	Cardholder specific

### **Subfield 12—Reserved for Future Use**

DE 48, subelement 41, subfield 12 (Reserved for Future Use) is for future use.

---

#### **Attributes**

---

Subfield ID:	12
Length of Length Field:	2
Data Representation:	ans...20

### **Subfield 13—Reserved for Future Use**

DE 48, subelement 41, subfield 13 (Reserved for Future Use) is for future use.

---

#### **Attributes**

---

Subfield ID:	13
--------------	----

**Data Element Definitions****DE 48—Additional Data—Private Use**

Length of Length Field:	2
Data Representation:	ans...20

**Subfield 14—Reserved for Future Use**

DE 48, subelement 41, subfield 14 (Reserved for Future Use) is for future use.

**Attributes**

Subfield ID:	14
Length of Length Field:	2
Data Representation:	ans...20

**Subfield 15—Reserved for Future Use**

DE 48, subelement 41, subfield 12 (Reserved for Future Use) is for future use.

**Attributes**

Subfield ID:	15
Length of Length Field:	2
Data Representation:	ans...10

**Subfield 16—Reserved for Future Use**

DE 48, subelement 41, subfield 16 (Reserved for Future Use) is for future use.

**Attributes**

Subfield ID:	16
Length of Length Field:	2
Data Representation:	n-2

**Subfield 17—Reserved for Future Use**

DE 48, subelement 41, subfield 17 (Reserved for Future Use) is for future use.

**Attributes**

Subfield ID:	17
Length of Length Field:	2
Data Representation:	a-1

### **Subfield 18—Reserved for Future Use**

DE 48, subelement 41, subfield 18 (Reserved for Future Use) is for future use.

---

#### **Attributes**

---

Subfield ID:	18
Length of Length Field:	2
Data Representation:	a...20

---

### **Subelement 42—Electronic Commerce Indicators**

Subelement 42 (Electronic Commerce Indicators) contains the electronic commerce indicators representing the security level and cardholder authentication associated with the transaction.

---

#### **Attributes**

---

Subelement ID:	42
Length of Length Field:	2 (valid value: 07)
Data Representation:	n-7
Data Field:	Contents of subfield 1
Subfields:	1
Justification:	N/A

---

#### **Usage**

---

Subelement 42 must be present in all Authorization Request/0100 messages for electronic commerce transactions. Following is the usage of subelement 42 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C

---

#### **Values**

---

Contains the electronic commerce security level indicator and UCAF collection indicator data in subfield 1 that consists of a valid combination of positions 1, 2, and 3.

**Data Element Definitions****DE 48—Additional Data—Private Use****Subfield 1—Electronic Commerce Security Level Indicator and UCAF Collection Indicator**

DE 48, subelement 42, subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator) indicates the electronic commerce security level and UCAF collection in positions 1, 2, and 3.

**Attributes**

Subfield ID:	01
Length of Length Field:	2 (valid value: 03)
Data Representation:	n-3
Data Field:	Indicates the electronic commerce security level and UCAF collection in positions 1, 2, and 3

**Values**

Valid combination of the security level indicators in positions 1 and 2 and the UCAF collection indicator in position 3.

**Position 1 (Security Protocol)**

Data Representation:	n-1
Data Field:	The electronic commerce security level indicator
Values:	0 = Reserved for existing MasterCard Europe/Visa definitions
	1 = Reserved for future use
	2 = Channel
	3-8 = Reserved for future use
	9 = None (no security protocol)

**Position 2 (Cardholder Authentication)**

Data Representation:	n-1
Data Field:	The cardholder authentication indicator
Values:	0 = Reserved for future use
	1 = Cardholder certificate not used
	2-9 = Reserved for future use

**Valid combinations of position 1 and position 2:**

21 = Channel encryption; cardholder certificate not used (this is the preferred value for MasterCard SecureCode)

91 = No security protocol; cardholder certificate not used

**Position 3 (UCAF Collection Indicator)**

Data Representation:	n-1
Data Field:	The UCAF collection indicator
Values:	
	0 = UCAF data collection is not supported by the merchant
	1 = UCAF data collection is supported by the merchant, but UCAF data was not populated (DE 48, subelement 43 is not present)
	2 = UCAF data collection is supported by the merchant, and UCAF data must be present (DE 48, subelement 43)
	3 = UCAF data collection is supported by the merchant, and UCAF (MasterCard assigned Static Accountholder Authentication Value) data must be present.
	<b>Note: DE 48, subelements 32 and 43 are required for Static AAV transactions.</b>
	Identifies participation in one of the following programs:
	<ul style="list-style-type: none"> <li>• Maestro Advance Registration Program</li> <li>• Maestro Recurring Payments Program</li> <li>• MasterCard Advance Registration Program</li> <li>• MasterCard Utility Payment Program</li> </ul>

## **Subelement 43—Universal Cardholder Authentication Field (UCAF)**

Subelement 43 (Universal Cardholder Authentication Field [UCAF]) contains the encoded MasterCard® SecureCode™ issuer or cardholder generated authentication data (collected by the merchant) resulting from all MasterCard SecureCode fully authenticated transactions, data for Visa transactions associated with the Visa 3-D Secure Electronic Commerce Verification Service (if collected), or the static AAV assigned by MasterCard for Maestro, MasterCard Advance Registration Program, Maestro Recurring Payments Program, or MasterCard Utility Payment Program.

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Attributes

Subelement ID:	43
Length of Length Field:	2
Data Representation:	ans...32; LLVAR
Data Field:	Contains UCAF® data
Subfields:	N/A
Justification:	N/A

#### Usage

Subelement 43 must be present whenever UCAF data is collected for electronic commerce transactions. Following is the usage of subelement 43 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE

#### Values

Refer to the specific program or service applications for:

- [3-D Secure for MasterCard SecureCode](#)
- [Static AAV for Maestro or MasterCard Advance Registration Program](#)
- [Visa 3-D Secure Electronic Commerce Verification Service \(Visa Only\)](#)
- [Recurring Payment Test Transactions](#)

## Subelement 43—3-D Secure for MasterCard SecureCode

Subelement 43 contains UCAF data and is described here for MasterCard Implementation of 3-D Secure for MasterCard® *SecureCode*™.

#### Attributes

Data Representation:	ans-28 (base 64 encoded)
Data Field:	The MasterCard 3-D Secure SPA AAV

#### Values

### **Attributes**

---

Transaction specific. Position 1 of the MasterCard 3-D Secure SPA AAV is a control byte indicating the *SecureCode* platform that created the field contents.

j = MasterCard 3-D Secure SPA AAV for first and subsequent transactions

h = MasterCard 3-D Secure SPA AAV for attempts. Acquirer should remove subelement 43 from an Authorization Request/0100 before submitting message to MasterCard.

---

### **Application Notes**

---

The following is an example of a properly coded DE 48, subelement 43 for MasterCard *SecureCode* for Fully Authenticated Authorization.

Please refer to the *SecureCode Member Enrollment and Implementation Guide* for more information.

For transactions that use the Maestro or MasterCard Advance Registration Program, a static AAV is used in place of *SecureCode*. The names of merchants enrolled in the Maestro or MasterCard Advance Registration Program and the static AAV assigned by MasterCard to each participating merchant are published as necessary in the *Global Operations Bulletin*, *Europe Region Operations Bulletin*, and the *Global Debit Operations Bulletin*. Additionally, this information is available on MasterCard OnLine, e-Business, e-Commerce, MasterCard, and Maestro Advance Registration Program.

MasterCard does not support “attempt” AAVs, and subelement 43 should be removed from the authorization request before submitting to MasterCard.

### **NOTE**

**Issuers should not perform *SecureCode* validation on static AAVs in DE 48, subelement 43.**

---

T420701032124328jJLtQa+Iws8AREAEbjjsA1MAAAA=820252

The UCAF field (DE 48, sublement 43) is a variable length field up to a maximum of 32 positions. The MasterCard *SecureCode* AAV is 28 characters in length. There must be no trailing spaces in the UCAF field.

---

Please refer to the Visa Base I Technical Specifications manual for the specific formats for Visa 3-D Secure CAVV.

---

## **Subelement 43—Static AAV for Maestro or MasterCard Advance Registration Program**

DE 48, subelement 43 (Static AAV for Maestro or MasterCard Advance Registration Program) is the MasterCard implementation of the Static AAV for MasterCard or Maestro Advance Registration Program.

---

### **Attributes**

---

Data Representation: ans-28

---

Data Field: The MasterCard assigned Static AAV

---

### **Values**

---

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Position 1 = Position 1 equals one of the following values:

- 3 = Transaction processed under the Maestro Advance Registration Program
- 4 = Transaction processed under the MasterCard Advance Registration Program
- 5 = Transaction processed under the Maestro Advance Registration Program, MasterCard Advance Registration Program, or the MasterCard Utility Payment Program.

Position 2–7 = The MasterCard Assigned ID which uniquely identifies the merchant.

Position 8–28 = The merchant name, padded to the right with nines (9).

---

#### Application Notes

When subelement 43 contains a Static AAV, subelement 32 (MasterCard Assigned ID) is mandatory. Issuers should not attempt SecureCode validation on a Static AAV.

---

## Subelement 43—Secure Electronic Commerce Verification Service (Visa Only)

Subelement 43 (Visa 3-D Secure Electronic Commerce Verification Service) is for Visa 3-D Secure Electronic Commerce Verification Service (Visa Only).

---

#### Attributes

---

##### Position 1 (Visa 3-D Secure Electronic Commerce Transaction Indicator)

---

Data Representation:	n-1
Data Field:	Indicates a Visa 3-D Secure Electronic Commerce transaction
Values:	8 = Visa 3-D Secure Electronic Commerce transaction

---

##### Position 2–21 (Visa 3-D Secure Electronic commerce Cardholder Authentication Verification Value [CAVV]) Visa Field 126.9)

---

Data Representation:	b-20
Data Field:	The Visa 3-D Secure Electronic Commerce CAVV value in binary format for usage 2 and 3.
Values:	Transaction specific

---

## Subelement 44—Visa 3-D Secure Electronic Commerce Transaction Identifier (XID) (Visa Only)

Subelement 44 (Visa 3-D Secure Electronic Commerce Transaction Identifier [XID]) contains the 3-D Secure Electronic Commerce Transaction Identifier (XID).

**Attributes**

Subelement ID:	44
Length of Length Field:	2
Data Representation:	b-20
Data Field:	The Visa XID value in binary format
Subfields:	N/A
Justification:	N/A

**Usage**

Following is the usage of subelement 44 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE

**Values**

The Visa XID value in binary format. Visa field 126.8.

**Application Notes**

The Visa XID value is optional in authorization messages for Visa usage 3 TransStain. Please refer to the Visa Base I Technical Specifications manual for the specific formats for Visa 3-D Secure Electronic Commerce Transaction Identifier (XID).

## **Subelement 45—Visa 3-D Secure Electronic Commerce Transaction Response Code (Visa Only)**

Subelement 45 (Visa 3-D Secure Electronic Commerce Transaction Response Code) is the 3-D Secure Electronic Commerce Transaction Response Code that contains the Visa Cardholder Authentication Verification Value (CAVV) results code.

**Attributes**

Subelement ID:	45
Length of Length Field:	2
Data Representation:	an-1
Data Field:	The Visa 3-D Secure CAVV results code

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

#### Usage

---

Following is the usage of subelement 45 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Org    Sys    Dst

Authorization Request Response/0110	C	•	C
-------------------------------------	---	---	---

#### Values

---

Please refer to the Visa Base I Technical Specifications manual for field 44.13 (CAVV Results Code) for a complete list of values available for this field.

---

## Subelement 46—Card-Level Result (Visa Only)

Subelement 46 (Card-Level Result) contains the Visa Card-level results value (Visa Only).

---

#### Attributes

---

Subelement ID:	46
----------------	----

Length of Length Field:	2
-------------------------	---

Data Representation:	an-2
----------------------	------

Data Field:	Contents of positions 1–2
-------------	---------------------------

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

#### Usage

---

Following is the usage of subelement 46 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

Org    Sys    Dst

Authorization Request Response/0110	C	•	C
-------------------------------------	---	---	---

Reversal Request Response/0410	C	•	C
--------------------------------	---	---	---

#### Values

---

Refer to the Visa Base I Technical Specifications manual for a complete list of values for field 62.23 (Card Level Results).

---

#### **Application Notes**

Acquirers should be prepared to receive subelement 46 in the Authorization Request Response/0110 message when one of the following occurs:

- Subelement 90 (Custom Payment Service Request [Visa]) is included in the Authorization Request/0100, which the Authorization Platform forwards to the Visa network.
- Subelement 90 is not included in the Authorization Request/0100 message and the Authorization Platform sends the message non-peer-to-peer to the Visa issuer via the Visa network.

### **Subelement 47—MasterCard Payment Gateway Transaction Indicator**

Subelement 47 (MasterCard Payment Gateway Transaction Indicator) indicates that the transaction is a MasterCard Payment Gateway transaction.

---

#### **Attributes**

---

Subelement ID:	47
Length of Length Field:	2
Data Representation:	ans-8
Data Field:	Contents of positions 1-8
Subfields:	N/A
Justification:	N/A

---

#### **Usage**

---

Following is the usage of subelement 47 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	•	C	C
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	•

---

#### **Values**

---

MC-MPG/W

---

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

If...	Then the Authorization Platform...
The account range does not participate in the MPG Authorization Blocking Service and DE 48, subelement 47 is present but does not contain value MC-MPG/W	Sends to the acquirer an Authorization Request Response/0110 message containing: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30</li><li>• DE 44 (Additional Data) = 048</li></ul>

## Subelement 48—Mobile Program Indicators

DE 48, subelement 48 (Mobile Program Indicators) identifies the service manager of the Mobile Remote Payments Program.

Attribute	Description
Subelement ID:	48
Length of Length Field:	2
Data Representation:	ans...73; LLVAR
Data Field:	Contents of subfields 1–4
Subfields:	4
Justification:	N/A

### Usage

Following is the usage of subelement 48 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C

### Values

See subfields.

### Application Notes

DE 48, subelement 48 (Mobile Program Indicators) must be present in all Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages for Mobile Remote Payments program transactions.

### **Subfield 1—Remote Payments Program Type Identifier**

DE 48, subelement 48 (Mobile Program Indicators), subfield 1 (Remote Payments Program Type Identifier) indicates the Service Manager (or program originator) of the Mobile Remote Payments program.

<b>Attribute</b>	<b>Description</b>
Subfield ID:	01
Length of Length Field:	2
Data Representation:	n...1; LLVAR
Data Field:	Contents of position 1
Justification:	N/A

<b>Values</b>
1 = Issuer domain
2 = Acquirer domain

### **Subfield 2—Reserved for Future Use**

DE 48, subelement 48 (Mobile Program Indicators), subfield 2 is reserved for future use.

<b>Attribute</b>	<b>Description</b>
Subfield ID:	02
Length of Length Field:	2
Data Representation:	n...1; LLVAR
Data Field:	Contents of subfield 2
Justification:	N/A

<b>Values</b>
Reserved for future use.

### **Subfield 3—Mobile Phone Number**

DE 48, subelement 48 (Mobile Program Indicators), subfield 3 (Mobile Phone Number) contains the customer mobile phone number.

<b>Attribute</b>	<b>Description</b>
Subfield ID:	03

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Length of Length Field:	2
Data Representation:	n...15; LLVAR
Data Field:	Contents of subfield 3
Justification:	N/A
<b>Values</b>	
Customer mobile phone number	

#### Subfield 4—Convenience Fee

DE 48, subelement 48 (Mobile Program Indicators), subfield 4 (Convenience Fee) contains customer convenience fee data.

Attribute	Description
Subfield ID:	04
Length of Length Field:	2
Data Representation:	ans...40; LLVAR
Data Field:	Contents of subfield 4
Justification:	N/A
<b>Values</b>	
Customer convenience fee data.	
<b>Application Note</b>	
The Convenience Fee amount that is present in subfield 4 must not be included in DE 4 (Amount, Transaction).	

#### Subelement 51—Merchant On-behalf Services

DE 48, subelement 51 (Merchant On-behalf [OB] Services) notifies the acquirer of the On-behalf Service performed on the transaction, and the results. DE 48 will support multiple occurrences of subelement 51 up to the maximum services for a transaction.

Attribute	Description
Subelement ID:	51
Length of Length Field:	2

---

Data Representation:	ans...99; LLVAR The “LL” length field of LLVAR must be an integral multiple of 4, not to exceed 96.
----------------------	--

Data Field:	Contents of subfields 1–3
-------------	---------------------------

Subfields:	3
------------	---

Justification:	N/A
----------------	-----

---

**Usage**

Following is the usage of subelement 51 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	•	X	C

---

**Values**

See subfields.

---

### **Subfield 1—Merchant On-behalf [OB] Service**

DE 48, subelement 51, subfield 1 (Merchant On-behalf [OB] Service) indicates the service performed on the transaction.

---

**Attributes**

---

Data Representation:	an-2
----------------------	------

Data Field:	Contents of positions 1-2
-------------	---------------------------

Justification:	Left-justified
----------------	----------------

---

**Values**

---

90	=	EMS Real-time Fraud Scoring Service for Merchants
----	---	---

### **Subfield 2—Merchant On-behalf [OB] Result 1**

DE 48, subelement 51, subfield 2 (Merchant On-behalf [OB] Result 1) indicates the results of the service processing.

---

**Attributes**

---

Data Representation:	an-1
----------------------	------

Data Field:	Contents of position 3
-------------	------------------------

Justification:	N/A
----------------	-----

---

**Values**

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

C	=	EMS Real-time Fraud Scoring Service for Merchants was performed successfully.
I	=	Invalid; transaction does not qualify for the EMS Real-time Fraud Scoring Service for Merchants due to one of the following: <ul style="list-style-type: none"><li>• Transaction is card present, or</li><li>• Card issuance is outside of the valid issuing region</li></ul>
U	=	EMS Real-time Fraud Scoring Service for Merchants was not performed successfully.

---

#### Application Notes

---

Subfield 2 will have values that identify the results from the EMS Real-time Fraud Scoring Service for Merchants processing result.

---

### Valid Subfield 1 and Subfield 2 Value Combinations

Following is the valid value combinations for DE 48, subelement 51, subfield 1 (Merchant On-behalf [OB] Service) and subfield 2 (Merchant On-behalf [OB] Result 1). The contents of subfield 2 depend on the contents of subfield 1 as shown below.

IF subfield 1 contains...	THEN subfield 2 will contain...
90	C, I, or U

---

#### Application Notes

---

If value of subfield 1 and subfield 2 is 90C, then DE 48, SE 55, subfield 1 and subfield 2 will be populated.

---

### Subfield 3—Additional Information

DE 48, subelement 51, subfield 3 (Additional Information) indicates if the acquirer in the transaction is enrolled with the service and if the service was requested.

---

#### Attributes

---

Data Representation: an-1

Data Field: Contents of position 4

Justification: N/A

---

#### Values

---

N	=	Not qualified for EMS Real-time Fraud Scoring Service for Merchants
blank	=	No value present

---

#### **Application Notes**

---

Subfield 3 will have an indicator of N if the score was not delivered to the acquirer but the acquirer had requested the transaction be scored. This is based on service participation.

---

## **Subelement 55—Merchant Fraud Scoring Data**

DE 48, subelement 55 (Merchant Fraud Scoring Data) indicates the fraud score on a fraud scoring service transaction when the acquirer requested the transaction to be scored.

<b>Attribute</b>	<b>Description</b>
Subelement ID:	55
Length of Length Field:	2
Data Representation:	an...32; LLVAR
Data Field:	Contents of subfields 1–5
Subfields:	5
Justification:	See “Subfields”

---

#### **Usage**

---

Following is the usage of subelement 55 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	•	X	C

---

#### **Values**

---

Contents of subfield 1–5

---

#### **Application Notes**

---

The Authorization Platform inserts this subelement when EMS Real-time Fraud Scoring Service for Merchants is performed on the transaction.

---

## **Subfield 1—Merchant Fraud Score**

DE 48, subelement 55, subfield 1 (Merchant Fraud Score) indicates the transaction risk score.

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Attribute	Description
Subfield ID:	01
Length of Length Field:	2
Data Representation:	an-3
Data Field:	Contents of positions 1–3
Justification:	N/A

#### Values

---

The EMS Real-time Fraud Scoring Service for Merchants provides the risk score of 001–998, where 001 indicates the least likely fraudulent transaction and 998 indicates the most likely fraudulent transaction.

---

### Subfield 2—Merchant Score Reason Code

DE48, subelement 55, subfield 2 (Merchant Score Reason Code) indicates the key factors that influenced the fraud score.

Attribute	Description
Subfield ID:	02
Length of Length Field:	2
Data Representation:	an-2
Data Field:	Contents of positions 1–2
Justification:	N/A

#### Values

---

The EMS Real-time Fraud Scoring Service for Merchants provides the score reason code, an alphanumeric code identifying the data used to derive the fraud score.

---

#### Application Notes

---

Participating acquirers may contact the Risk Solutions Team for a list of the specific score reason codes that apply to their institution.

---

### Subfield 3—Reserved for Future Use

DE48, subelement 55, subfield 3 (Reserved for Future Use) is reserved for future use.

Attribute	Description
Subfield ID:	03

Length of Length Field:	2
Data Representation:	an-3
Data Field:	Contents of positions 1–3
Justification:	N/A
<b>Values</b>	
Reserved for Future Use	

#### **Subfield 4—Reserved for Future Use**

DE48, subelement 55, subfield 4 (Reserved for Future Use) is reserved for future use.

<b>Attribute</b>	<b>Description</b>
Subfield ID:	04
Length of Length Field:	2
Data Representation:	an-2
Data Field:	Contents of positions 1–2
Justification:	N/A
<b>Values</b>	
Reserved for Future Use	

#### **Subfield 5—Reserved for Future Use**

DE48, subelement 55, subfield 5 (Reserved for Future Use) is reserved for future use.

<b>Attribute</b>	<b>Description</b>
Subfield ID:	05
Length of Length Field:	2
Data Representation:	an-2
Data Field:	Contents of positions 1–2
Justification:	N/A
<b>Values</b>	
Reserved for Future Use	

**Data Element Definitions****DE 48—Additional Data—Private Use****Subelement 58—ATM Additional Data**

Subelement 58 (ATM Additional Data) only applies to Swedish Domestic Authorization Switching Service (SASS). Subelement 58 contains watermark data captured at an ATM. Watermark data is a card authentication technology supported by Swedish ATMs.

**Attributes**

Subelement ID:	58
Length of Length Field:	2
Data Representation:	ans-33
Data Field:	Contents of subfields
Subfields:	8
Justification:	N/A

**Usage**

Following is the usage of subelement 58 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	O	X	C
Reversal Request/0400	O	X	C

**Values**

See “Subfields.”

**Subfield 1—ATM Time**

DE 48, subelement 58, subfield 1 (ATM Time) indicates the ATM time.

**Attributes**

Data Representation:	n-4
Data Field:	Contents of positions 1–4 (hhmm)
Justification:	N/A

**Subfield 2—ATM Date**

DE 48, subelement 58, subfield 2 (ATM Date) indicates the ATM date.

**Attributes**

Data Representation:	n-6
Data Field:	Contents of positions 5–10 (YYMMDD)
Justification:	N/A

**Subfield 3—Watermark**

DE 48, subelement 58, subfield 3 (Watermark) is the watermark value.

**Attributes**

Data Representation:	n-12
Data Field:	Contents of positions 11-22
Justification:	N/A

**Subfield 4—Mark 1**

DE 48, subelement 58, subfield 4 (Mark 1) indicates the card and the watermark status.

**Attributes**

Data Representation:	ans-2
Data Field:	Contents of positions 23–24
Justification:	N/A

**Values**

0-	=	National card
4-	=	National card, foreign currency
8-	=	International card
C-	=	International card, foreign currency
-0	=	Watermark readable
-B	=	Watermark unreadable
-C	=	Watermark missing
-D	=	Test mode
-E	=	Test mode

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Subfield 5—Mark 2

DE 48, subelement 58, subfield 5 (Mark 2) indicates the reason code for reversal from ATM.

---

##### Attributes

---

Data Representation: an-2

---

Data Field: Contents of positions 25–26

---

Justification: N/A

---

##### Values

---

00 = Dispensing error for bank notes or receipts

---

02 = Error in response

---

08 = Failure to return card, response received from host

---

48 = Failure to return card, single reversal

---

04 = Timeout—card not picked up, response received from host

---

80 = Timeout—card not picked up, response received from host

---

44 = Timeout—card not picked up, single reversal

---

40 = Single reversal, unknown reason

---

06 = Error in response and timeout picking up card

---

0A = Error in response and failure to return card

---

#### Subfield 6—Mark 3

DE 48, subelement 58, subfield 6 (Mark 3) indicates stock of bank notes and receipt status.

---

##### Attributes

---

Data Representation: ans-2

---

Data Field: Contents of positions 27–28

---

Justification: N/A

---

##### Values

---

0- = Both SEK 100 and SEK 500 notes available

---

4- = SEK 500 notes not available

---

8- = SEK 100 notes not available

---

C- = No money available

---

---

**Attributes**

---

-0	=	Receipt OK
-4	=	Receipt low
-8	=	Receipt paper empty
-C	=	Receipt technical error

---

**Subfield 7—Card Swallowed Status**

DE 48, subelement 58, subfield 7 (Card Swallowed Status) indicates if the ATM took the card or not.

---

**Attributes**

---

Data Representation:	n-1
Data Field:	Contents of position 29
Justification:	N/A

---

**Values**

---

0	=	Card not swallowed
1	=	Card swallowed

---

**Subfield 8—Posting Date**

DE 48, subelement 58, subfield 8 (Posting Date) is the posting date.

---

**Attributes**

---

Data Representation:	n-4
Data Field:	Contents of position 30–33
Justification:	N/A

---

**Subelement 61—POS Data Extended Condition Codes**

Subelement 61 (POS Data, Extended Condition Codes) indicates whether the merchant terminal supports a specific program or service.

---

**Attributes**

---

Subelement ID:	61
Length of Length Field:	2
Data Representation:	n-5

---

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Data Field:	Contents of positions 1–5
Subfields:	5
Justification:	See “Subfields”

#### Usage

---

Following is the usage of subelement 61 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	X	C
Authorization Advice/0120—Acquirer-generated	C	X	C
Authorization Advice/0120—System-generated	•	C	C

#### Values

---

See “Subfields”

#### Application Notes

---

This subelement should be provided to indicate the merchant terminal’s capabilities in supporting specific programs and services.

## Subfield 1—Partial Approval Terminal Support Indicator

DE 48, subelement 61, subfield 1 (Partial Approval Terminal Support Indicator) indicates if the merchant terminal supports partial approvals.

---

#### Attributes

---

Data Representation:	n-1
Data Field:	Contents of position 1
Justification:	N/A

#### Values

---

0	=	Merchant terminal does not support receipt of partial approvals
1	=	Merchant terminal supports receipt of partial approvals

## Subfield 2—Purchase Amount Only Terminal Support Indicator

DE 48, subelement 61, subfield 2 (Purchase Amount Only Terminal Support Indicator) indicates if the merchant terminal supports purchase only approvals.

---

#### Attributes

---

Data Representation:	n-1
----------------------	-----

Data Field:	Contents of position 2
Justification:	N/A
<b>Values</b>	
0 =	Merchant terminal does not support receipt of purchase only approvals
1 =	Merchant terminal supports receipt of purchase only approvals

### **Subfield 3—Real-time Substantiation Indicator**

DE 48, subelement 61, subfield 3 (Real-time Substantiation Indicator) indicates if the merchant terminal verified the purchased items against the Inventory Information Approval System (IIAS).

---

#### **Attributes**

---

Data Representation:	n-1
Data Field:	Contents of position 3
Justification:	N/A
<b>Values</b>	
0 =	Merchant terminal did not verify the purchased items against an Inventory Information Approval System (IIAS)
1 =	Merchant terminal verified the purchased items against an Inventory Information Approval System (IIAS)
2 =	Merchant claims exemption from using an IIAS based on the IRS 90 percent rule
4 =	Transaction was submitted as real-time substantiated but from a non-IIAS-certified merchant. MasterCard uses this value to notify the issuer that the merchant could not be substantiated. Acquirers may not use this value.

### **Subfield 4—Merchant Transaction Fraud Scoring Indicator**

DE 48, subelement 61, subfield 4 (Merchant Transaction Fraud Scoring Indicator) indicates if the acquirer requested the transaction to be scored by the Expert Monitoring System (EMS).

---

#### **Attributes**

---

Data Representation:	an-1
Data Field:	Contents of position 4
Justification:	N/A

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Values

0 = No action required

1 = Transaction to be scored

#### Application Notes

Only a value of zero is passed to the issuer on the Authorization Request/0100 message.

The Acquirer Generated Authorization Advice/0120 is rejected and will not be sent to EMS for scoring if it is any other value than zero.

---

### Subfield 5—Reserved for Future Use

DE 48, subelement 61, subfield 5 (Reserved for Future Use) is reserved for future use.

---

#### Attributes

Data Representation: n-1

Data Field: Contents of position 5

Justification: N/A

---

#### Values

0 = Reserved for Future Use

---

### Subelement 63—Trace ID

DE 48, subelement 63 (Trace ID) contains data from DE 63 (Network Data), subfield 1 (Financial Network Code) and subfield 2 (Banknet Reference Number) and DE 15 (Date, Settlement) that is in the original Authorization Request Response/0110 message.

---

#### Attributes

Subelement ID: 63

Length of Length Field: 2

Data Representation: ans-15

Data Field: Contents of positions 1-15

Subfields: N/A

Justification: N/A

---

#### Usage

Following is the usage of subelement 63 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	M	•	M
Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	M	M

#### **Values**

Contains the contents of positions 1–15 as defined below:

#### **Positions 1–9 (Network Data)**

Data Representation:	ans-9
Data Field	Contents of positions 1–9
Values:	Contents of DE 63, subfield 1 (Financial Network Code) and subfield 2 (Banknet Reference Number) in the original Authorization Request Response/0110 message. The Banknet Reference number is a minimum of six characters and a maximum of nine characters.
	Positions 1–3        =        DE 63, subfield 1
	Positions 4–9        =        DE 63, subfield 2

#### **Positions 10–15 (Date Settlement)**

Data Representation:	ans-6
Data Field	Contents of positions 10–15
Values:	Contents of DE 15 (Date, Settlement) in the original Authorization Request Response/0110 message. The four-digit Settlement Date is in MMDD format followed by two spaces.

#### **Application Notes**

DE 48, subelement 63 must be present in Reversal Request/0400 messages and must contain data in positions 1–15, otherwise the message will be rejected with a format error response where DE 39 is 30 and DE 44 is 048. DE 48, subelement 63 may contain a value of zeros in Reversal Request/0400 message or Reversal Advice/0420 messages when an Authorization Request Response/0110 was not successfully processed by the acquirer.

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Subelement 64—Transit Program

DE 48, subelement 64 (Transit Program) is used to identify transit transactions in authorization messages.

---

##### Attributes

---

Subelement ID:	64
Length of Length Field:	2
Data Representation:	n-4
Data Field:	Contents of subfields 1–2
Subfields:	2
Justification:	N/A

---

##### Usage

---

Following is the usage of subelement 64 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C

---

##### Values

---

Contains the Transit Program values in subfields 1 and 2.

---

#### Subfield 1—Transit Transaction Type Indicator

DE 48, subelement 64, subfield 1 (Transit Transaction Type Indicator) indicates the transit transaction type identifier.

---

##### Attributes

---

Data Representation:	n-2
Data Field:	Contents of positions 1–2
Justification:	N/A

---

##### Values

---

01	=	Prefunded
02	=	Real-time Authorized
03	=	Post-Authorized Aggregated

---

04	=	Authorized Aggregated Split Clearing
05	=	Other
06–99	=	Reserved for Future Use

### **Subfield 2—Transportation Mode Indicator**

DE 48, subelement 64, subfield 2 (Transportation Mode Indicator) indicates the transportation mode for a transit transaction.

---

#### **Attributes**

---

Data Representation:	n-2
Data Field:	Contents of positions 3–4
Justification:	N/A

---

#### **Values**

---

00	=	Unknown
01	=	Urban Bus
02	=	Interurban Bus
03	=	Light Train Mass Transit (Underground Metro, LTR)
04	=	Train
05	=	Commuter Train
06	=	Water Borne Vehicle
07	=	Toll
08	=	Parking
09	=	Taxi
10	=	High Speed Train
11	=	Rural Bus
12	=	Express Commuter Train
13	=	Para Transit
14	=	Self Drive Vehicle
15	=	Coach
16	=	Locomotive
17	=	Powered Motor Vehicle

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

18	=	Trailer
19	=	Regional Train
20	=	Inter City
21	=	Funicular Train
22	=	Cable Car
23–99	=	Reserved for Future Use

### Subelement 71—On-behalf Services

DE 48, subelement 71 (On-behalf [OB] Services) notifies the issuer of the On-behalf Service performed on the transaction and the results. Subelement 71 will support up to ten services for a transaction.

---

#### Attributes

---

Subelement ID:	71
Length of Length Field:	2
Data Representation:	ans...40; LLVAR The “LL” length field of LLVAR must be an integral multiple of 4, not to exceed 40.
Data Field:	Contents of subfields 1–3
Subfields:	3
Justification:	N/A

---

#### Usage

---

Following is the usage of subelement 71 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Request Response/0110	CE	CE	•
Authorization Advice/0120—Acquirer-generated	•	X	C
Authorization Advice/0120—System-generated	•	X	C
Reversal Request/0400	•	X	C

---

#### Values

---

See subfields.

---

## **Subfield 1—On-behalf (OB) Service**

DE 48, subelement 71, subfield 1 (On-behalf [OB] Service) indicates the service performed on the transaction.

---

### **Attributes**

---

Data Representation:	an-2
Data Field:	Contents of positions 1–2
Justification:	Left-justified

---

### **Values**

---

01	=	Chip to Magnetic Stripe Conversion Service
02	=	M/Chip Cryptogram Pre-validation Service
03	=	M/Chip Cryptogram Validation in Stand-In Processing
04	=	Reserved for Future Use
05	=	MasterCard® <i>SecureCode</i> ™ AAV Verification Service
06	=	MasterCard® <i>SecureCode</i> ™ Dynamic AAV Verification in Stand-In Processing
08	=	Online PIN Pre-validation (Europe Only)
09	=	Online PIN Validation in Stand-In (Europe only)
13	=	Static CVC 3 Validation in Stand-In Processing
14	=	<i>PayPass</i> Mapping Service
15	=	Dynamic CVC 3 Pre-validation (with or without <i>PayPass</i> Mapping Service)
16	=	Dynamic CVC 3 Validation in Stand-In Processing
17	=	inControl Virtual Card Service
18	=	Fraud Scoring Service
20	=	inControl RCN Spend Control Service
25	=	Expert Monitoring Compromised Account Service Information
27	=	Pay with Rewards Service

---

## **Subfield 2—On-behalf Result 1**

DE 48, subelement 71, subfield 2 (On-behalf [OB] Result 1) indicates the results of the service processing.

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Attributes

---

Data Representation: an-1

---

Data Field: Contents of position 3

---

Justification: N/A

---

#### Values

---

A = ATC outside allowed range (applicable when ATC value is dynamic [varying] value)

---

A = Virtual Card Number (expiration date does not match)

---

B = Virtual Card Number (expiration date expired)

---

C = Conversion of the M/Chip transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 05 [PAN auto-entry via chip] or 79 [Chip card/PAN entry via manual entry]

---

C = Conversion of *PayPass* account number to PAN was completed

---

C = Virtual Card Number Virtual CVC 2 does not match

---

C = Expert Monitoring Fraud Scoring Service was performed successfully

---

D = inControl Validity Period Limit

---

E = CVC 3 ATC Replay

---

E = inControl Transaction Amount Limit Check

---

F = Format error (MasterCard use only)

---

F = inControl Cumulative Amount Limit Check

---

G = Application Cryptogram is valid but not an ARQC, status of TVR/CVR unknown

---

G = inControl Transaction Number Usage

---

H = inControl Merchant ID Limit

---

I = Invalid

---

I = inControl Invalid Virtual Card Number—Real Card Number mapping relationship

---

I = Pay with Rewards transaction declined on issuer's behalf for insufficient points balance

---

J = inControl MCC Limit

---

K = inControl Database Status Bad

---

L = inControl Geographic Restriction

---

L = Pay with Rewards transaction funded using consumer loyalty points

---

**Attributes**

M	=	inControl Transaction Type Restriction
M	=	Conversion of the M/Chip fallback transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 80—PAN auto-entry with magnetic stripe
N	=	Unpredictable Number Mismatch (applicable when the UN is dynamic [varying] value)  (Indicates that the number/length in the discretionary data in DE 45 or DE 35 does not match the number/length provided by the issuer during personalization)
N	=	Compromised Event Data Not Found
N	=	Pay with Rewards transaction declined—Card not registered for service
P	=	Mandatory PVV not on file
P	=	inControl Transaction Time/Date Restriction
R	=	PIN retry Exceeded (invalid PIN)
R	=	Pay with Rewards transaction declined on issuer's behalf for failing rules
S	=	Conversion of the M/Chip transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 07—PAN auto-entry via contactless M/Chip
T	=	Valid ARQC, TVR/CVR invalid
U	=	Expert Monitoring Fraud Scoring Service was not performed successfully
U	=	Pay with Rewards service was not performed successfully
U	=	Unable to process
V	=	Valid
Y	=	Compromised Event Data Found
blank	=	No value present

**Subfield 3—On-behalf Result 2**

DE 48, subelement 71, subfield 3 (On-behalf Result 2) identifies the results of the service processing.

**Attributes**

Data Representation: ans-1

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Data Field:	Contents of position 4
Justification:	N/A
<b>Values</b>	
MasterCard use only. May contain a space or a value.	

### Valid Subfield 1 and Subfield 2 Value Combinations

Following is the valid DE 48, subelement 71, subfield 1 (OB Service) and subfield 2 (OB Result 1) value combinations. The contents of subfield 2 depend on the contents of subfield 1 as described here.

IF subfield 1 contains...	THEN... subfield 2 may contain...
01	C, M, or S
02	F, G, I, T, U, or V
03	F, G, I, T, U, or V
05	I, U, or V
06	I, U, or V
08	I, P, R, U, or V
09	I, P, R, U, or V
12	I, U, or V
13	I, U, or V
14	C, I, or U
15	A, E, I, N, U, or V
16	A, E, I, N, U, or V
17	A, B, C, D, E, F, G, H, I, J, K, L, M, P, U, or V
18	C or U
20	D, E, F, G, H, J, K, L, M, P, U, or V
25	Y, N, U
27	I, L, N, R, or U

### Subelement 72—Issuer Chip Authentication

DE 48, subelement 72 (Issuer Chip Authentication) carries data used during cryptogram processing.

**Attributes**

Subelement ID:	72
Length of Length Field:	2
Data Representation:	b...16; LLVAR (the “LL” length field of LLVAR must be between 8–16 positions.)
Data Field:	Contents of subelement
Subfields:	N/A
Justification:	N/A

**Usage**

Following is the usage of subelement 72 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	C	C
Authorization Request Response/0110	CE	X	•
Authorization Advice/0120—System-generated	•	C	C

**Values**

MasterCard generated.

## **Subelement 74—Additional Processing Information**

DE 48, subelement 74 (Additional Processing Information) provides additional information about chip transaction processing and results.

**Attributes**

Subelement ID:	74
Length of Length Field:	2
Data Representation:	an...30; LLVAR The “LL” length field of LLVAR must be an integral multiple of 3 not to exceed 30.
Data Field:	Contents of “Subfields”
Subfields:	2
Justification:	See “Subfields”

**Usage**

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Following is the usage of subelement 74 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	O	X	C
Reversal Request Response/0410	O	X	C

#### Values

---

See “Subfields”

#### Application Notes

---

DE 48, subelement 74 is not applicable in the 0120/0130 and 0420/0430 messages. If present, it will be removed before forwarding to its destination.

#### Chip Cryptogram Validation

---

Issuers performing chip cryptogram validation may include their validation results in DE 48, subelement 74 in the Authorization Request Response/0110 message.

#### When the issuer sends an Authorization Request Response/0110 message containing DE 48, subelement 74 and...

#### THEN the Authorization Platform...

Subfield 1 does not contain 50	Will remove DE 48, subelement 74 before forwarding the message to the acquirer.
Subfield 2 contains an invalid value	Will replace the invalid subfield 2 value with an X to indicate an unknown issue before forwarding the message to the acquirer
DE 48 (Additional Data—Private Use), subelement 74 (Additional Processing Information) in the Authorization Advice Response/0130 is received from the issuer contains: <ul style="list-style-type: none"><li>• Subfield 1 = value 90 (Chip Fallback Transaction Downgrade Process)</li><li>• Subfield 2 = value C (Completed Successfully)</li></ul>	Removes this data from transaction before forwarding to the acquirer

#### Subfield 1—Processing Indicator

DE 48, subelement 74, subfield 1 (Processing indicator) indicates the transaction processing type.

---

#### Attributes

---

Data Representation: an-2

Data Field: Identifies the service performed

Justification:	N/A
<b>Values</b>	
02	= MasterCard On-behalf Service—M/Chip Cryptogram Pre-validation
03	= MasterCard On-behalf Service—M/Chip Cryptogram Validation in Stand-in Processing
50	= Issuer Chip Validation
90	= Chip Fall-back Transaction Downgrade Process

### **Subfield 2—Processing Information**

DE 48, subelement 74, subfield 2 contains additional information about the issuer incurred during the cryptogram validation.

<b>Attributes</b>	
Data Representation:	an-1
Data Field:	Additional information being provided about the service
Justification:	N/A
<b>Values</b>	
C	= Completed Successfully
F	= Format error in DE 55
G	= Application Cryptogram is valid but is not an ARQC
I	= Application Cryptogram invalid
T	= Application Cryptogram is valid but TVR/CVR was invalid
U	= Application Cryptogram could not be validated due to technical error
X	= Issuer provided incorrect subfield 2 value

### **Valid Subfield 1 and Subfield 2 Value Combinations**

Following is the valid DE 48, subelement 74, subfield 1 (Processing Indicator) and subfield 2 (Processing Information) value combinations. The contents of subfield 2 depend on the contents of subfield 1 as described here.

<b>IF subfield 1 contains...</b>	<b>THEN subfield 2 may contain...</b>
02	F, G, I, T, or U
03	F, G, I, T, or U

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

IF subfield 1 contains...	THEN subfield 2 may contain...
50	F, G, I, T, or U
90	C

### Subelement 75—Fraud Scoring Data

DE 48, subelement 75 (Fraud Scoring Data) indicates the fraud score on a fraud scoring service transaction.

Attribute	Description
Length of Length Field:	2
Data Representation:	an...32; LLVAR
Data Field:	Contents of subfields 1–5
Subfields:	5
Justification:	See subfields

#### Usage

Following is the usage of subelement 75 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Advice/0120—System-generated	•	C	C

#### Values

Contents of subfield 1–2

#### Application Notes

The Authorization Platform inserts this subelement when Expert Monitoring Fraud Scoring Service is performed or when both Expert Monitoring Fraud Scoring Service and Business Rules Management Service are performed on the transaction.

**When a rule adjusted score is provided in subfield 3, at least one or more rule reason code values will be provided in subfields 4–5. However, rule reason code values may be provided in subfields 4 or 5 with or without a rule adjusted score in subfield 3.**

### Subfield 1—Fraud Score

DE 48, subelement 75, subfield 1 (Fraud Score) indicates the transaction risk score.

---

**Attribute**

Subfield ID:	01
Length of Length Field:	2
Data Representation:	an-3
Data Field:	Contents of positions 1-3
Justification:	N/A

**Values**

---

Fraud Scoring System provides the risk score of 000–999, where 000 indicates the least likely fraudulent transaction and 999 indicates the most likely fraudulent transaction.

### **Subfield 2—Score Reason Code**

DE 48, subelement 75, subfield 2 (Score Reason Code) indicates the key factors that influenced the fraud score.

---

**Attribute**

Subfield ID:	02
Length of Length Field:	2
Data Representation:	an-2
Data Field:	Contents of positions 1–2
Justification:	N/A

**Values**

---

The Expert Monitoring Fraud Scoring Service provides the score reason code, an alphanumeric code identifying the data used to derive the fraud score.

**NOTE**

---

**Participating issuers may contact the Risk Solutions team for a list of the specific score reason codes that apply to their institution.**

### **Subfield 3—Rules Adjusted Score**

DE 48, subelement 75, subfield 3 contains the Expert Monitoring Business Rules Management Service, rules adjusted score.

---

**Attributes**

Subfield ID:	03
Length of Length Field:	2
Data Representation:	an-3

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Attributes

---

Data Field:                   Contents of positions 1–3

---

Justification:               N/A

---

Values

---

The Expert Monitoring Business Rules Management Service provides a rule adjusted score of 000–999, where 000 indicates the least likely fraudulent transaction and 999 indicates the most likely fraudulent transaction.

---

### Subfield 4—Rules Reason Code 1

DE 48, subelement 75, subfield 4 indicates the data used to derive the rule adjusted score.

#### Attributes

---

Subfield ID:               04

---

Length of Length Field:   2

---

Data Representation:      an-2

---

Data Field:               Contents of positions 1–2

---

Justification:               N/A

---

Values

---

The Expert Monitoring Business Rules Management Service provides the rule reason code, an alphanumeric code where the information provided gives the data used to derive the rules adjusted score.

---

### Subfield 5—Rules Reason Code 2

DE 48, subelement 75, subfield 5 indicates the data used to derive the rule adjusted score.

#### Attributes

---

Subfield ID:               05

---

Length of Length Field:   2

---

Data Representation:      an-2

---

Data Field:               Contents of positions 1–2

---

Justification:               N/A

---

---

**Attributes**

---

**Values**

---

The Expert Monitoring Business Rules Management Service provides the rule reason code, an alphanumeric code where the information provided gives the data used to derive the rules adjusted score.

---

## **Subelement 76—MasterCard Electronic Acceptance Indicator**

DE 48, subelement 76 (MasterCard Electronic Acceptance Indicator) identifies that the transaction is a MasterCard Electronic transaction. It indicates that the acquirer participates or does not participate in MasterCard Electronic card processing.

---

**Attributes**

---

Subelement ID:	76
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

---

**Usage**

---

Following is the usage of subelement 76 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	X	C
Authorization Request Response/0110	O	X	•
Authorization Advice/0120—Acquirer-generated	O	X	C
Authorization Advice/0120—Issuer-generated	C	X	•
Authorization Advice/0120—System-generated	•	C	C

---

**Values**

---

C	=	MasterCard only participant (not considered a MasterCard Electronic card transaction).
E	=	Acquirer and its merchant both participate in MasterCard Electronic card processing (considered as a MasterCard Electronic transaction).

---

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

M	=	Acquirer participates in MasterCard Electronic card processing, but the merchant that processed this specific transaction does not participate in MasterCard Electronic (considered not to be a MasterCard Electronic transaction).
U	=	Unidentified acquirer. It is unknown if the acquirer is a MasterCard Electronic card participant.

#### Application Notes

---

If acquirers do not populate subelement 76 with a valid value or a value is not present, MasterCard will populate DE 48, subelement 76 on behalf of the acquirer based on the acquirer's participation in MasterCard Electronic Program and forward the transaction to the issuer.

---

#### Acquirers

---

When the merchant participates in the MasterCard Electronic Card Program, the participating acquirer should send DE 48, subelement 76 with a value of E in the Authorization Request/0100 message.

---

When the merchant does not participate in the MasterCard Electronic Card Program, the participating acquirer should send DE 48, subelement 76 with a value of M in the Authorization Request/0100 message.

---

When participating acquirers do not provide a value or provide an incorrect value in subelement 76, MasterCard will default subelement 76 to the value of E in the Authorization Request/0100 message.

---

#### Issuers

---

Issuers participating in MasterCard Electronic Card must be prepared to receive DE 48, subelement 76 with values of C, E, or U in the Authorization Request/0100 and Authorization Advice/0120 messages.

---

Issuers participating in MasterCard Electronic Card must be prepared to send DE 48, subelement 76 with values of C, E, or U in Authorization Request Response/0110 messages.

---

**MasterCard will convert the subelement value of M to the value C in the Authorization Request/0100 sent to the issuer. Therefore, the issuer will not receive a value of M.**

---

## Subelement 77—Payment Transaction Type Indicator

DE 48, subelement 77 (Payment Transaction Type Indicator) indicates the type of Payment Transaction taking place.

---

#### Attributes

---

Subelement ID: 77

---

Length of Length Field: 2

---

Data Representation: an-3

---

Data Field: Contents of positions 1-3

---

---

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

#### **Usage**

Following is the usage of subelement 77 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	C
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	C
Reversal Advice/0420	•	C	C

#### **Values**

C01	=	Person-to-Person
C02	=	Rebate
C03	=	Load value
C04	=	Gaming Re-pay
C05	=	Payment Transaction for a reason other than those defined in values C01–C04
C06	=	Payment of a credit card balance with cash or check
C07	=	MasterCard <i>MoneySend</i>
C09	=	Card Activation

#### **Application Notes**

If DE 3, subfield 1 contains value 28 (Payment Transaction), then DE 48, subelement 77 must be present.

Usage of value C04 is limited to eligible acquirers and issuers in eligible countries.

Usage of value C07 is limited to eligible countries and eligible acquirers. Please refer to the *MasterCard MoneySend Global Platform Guide*.

Usage of value C09 is limited to Private Label Prepaid Cards issued in Europe.

## **Subelement 78—U.S. Deferred Billing Indicator (Visa Only)**

DE 48, subelement 78 (U.S. Deferred Billing Indicator) indicates a transaction for which the billing for merchandise occurred after the merchandise was delivered to the cardholder.

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Attributes

Subelement ID:	78
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

#### Usage

Subelement 78 contains an indicator to denote a deferred billing transaction on a Visa account number when applicable. Following is the usage of subelement 78 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE

#### Values

D = U.S. Deferred Billing

## Subelement 79—Chip CVR/TVR Bit Error Results

Subelement 79 (Chip CVR/TVR Bit Error Results) provides the Terminal Verification Results (TVR) and Card Verification Results (CVR) bitmask, and expected values registered by the issuer. This serves as notification of bit validation errors detected in the CVR/TVR within the Issuer Application data during M/Chip Cryptogram Validation processing.

#### Attributes

Subelement ID	79
Length of Length Field:	2
Data Representation:	an...50; LLVAR The “LL” length field of LLVAR must be an integral multiple of 5, not to exceed 50.
Data Field:	Contents of subfields 1-4
Subfields:	4
Justification:	N/A

#### Usage

Following is the usage of subelement 79 (whether it is mandatory, conditional, optional, system provided, or not required) in all applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Advice/0120—System-generated	•	X	C

#### **Values**

See “Subfields.”

#### **Application Notes**

The Authorization Platform will stop verification of CVR/TVR bits when 10 errors are detected.

See the following example. In the example:

- The binary representation of the TVR Bit Mask for Byte 3 is “10101000”
- The binary representation of the Expected Result for Byte 3 is “00000000”
- The binary representation of the Validation Result for Byte 3 is “10000000”

The Validation Result indicates that the cardholder verification was not successful.

See the *M/Chip Processing Services—Service Description* document for recommended bit mask settings.

	<b>Byte 1</b>	<b>Byte 2</b>	<b>Byte 3</b>	<b>Byte 4</b>	<b>Byte 5</b>
TVR Bit Mask—Hex	00	00	A8	00	00
Expected Result	00	00	00	00	00
Validation Result	00	00	80	00	00

Subfield 1	CVR or TVR Identifier	T
Subfield 2	Byte ID	03
Subfield 3	Bit Identifier	8
Subfield 4	Value of Bit in Error	1

#### **Subfield 1—CVR or TVR Identifier**

DE 48, subelement 79, subfield 1 indicates whether bit reported in error is part of CVR or TVR.

#### **Attributes**

Data Representation: an-1

Data Field: Contents of position 1

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Justification:	Left justified
----------------	----------------

#### Values

C = CVR
---------

T = TVR
---------

### Subfield 2—Byte ID

DE 48, subelement 79, subfield 2 identifies the byte number of the associated bit reported in error.

---

#### Attributes

Data Representation:	an-2
----------------------	------

Data Field:	Contents of positions 2-3
-------------	---------------------------

Justification:	N/A
----------------	-----

#### Values

01-99
-------

### Subfield 3—Byte Identifier

DE 48, subelement 79, subfield 3 (Byte Identifier) identifies the bit number in error within the byte identified in subfield 2.

---

#### Attributes

Data Representation:	an-1
----------------------	------

Data Field:	Contents of position 4
-------------	------------------------

Justification:	N/A
----------------	-----

#### Values

1-8
-----

### Subfield 4—Value of Bit in Error

DE 48, subelement 79, subfield 4 identifies the value of the bit in error that was submitted in transaction.

---

#### Attributes

Data Representation:	an-1
----------------------	------

Data Field:	Contents of position 5
-------------	------------------------

Justification:	N/A
<b>Values</b>	
0–1	

## **Subelement 80—PIN Service Code**

DE 48, subelement 80 (PIN Service Code) indicates the results of PIN processing by the Authorization Platform.

---

### **Attributes**

---

Subelement ID:	80
Length of Length Field:	2
Data Representation:	a-2
Data Field:	Contents of positions 1–2
Subfields:	N/A
Justification:	N/A

---

### **Usage**

---

Subelement 80 is provided by the Authorization Platform in the Authorization Request/0100 message whenever PIN data is present in the Authorization Request/0100 message.

Following is the usage of subelement 80 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	C	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Issuer-generated	•	C	C
Authorization Advice/0120—System-generated	C	C	•

---

### **Values**

---

PV = The Authorization Platform verified the PIN.

TV = The Authorization Platform translated the PIN for issuer verification.

PI = The Authorization Platform was unable to verify the PIN.

TI = The Authorization Platform was unable to translate the PIN.

**Data Element Definitions****DE 48—Additional Data—Private Use****Subelement 82—Address Verification Service Request**

DE 48, subelement 82 (Address Verification Service Request) indicates that verification of the cardholder billing address is requested in the authorization message.

**Attributes**

Subelement ID:	82
Length of Length Field:	2
Data Representation:	n-2
Data Field:	Contents of positions 1–2
Subfields:	N/A
Justification:	N/A

**Usage**

Subelement 82 must be present in the authorization request message whenever cardholder address verification is requested by the acquirer.

Following is the usage of subelement 82 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C

**Values**

52 = AVS and Authorization Request/0100

**Subelement 83—Address Verification Service Response**

DE 48, subelement 83 (Address Verification Service Response) contains the AVS verification response code in the Authorization Request Response/0110 message.

**Attributes**

Subelement ID:	83
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1

**Data Element Definitions**  
**DE 48—Additional Data—Private Use**

---



---

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

**Usage**

---

Subelement 83 must be provided by the issuer in the Authorization Request Response/0110 message whenever AVS is requested by the acquirer.

Following is the usage of subelement 83 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Issuer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C

**Values**

---

A =	Address matches, postal code does not.
-----	--

B =	Visa only. Street address match. Postal code not verified because of incompatible formats. (Acquirer sent both street address and postal code.)
-----	---

C =	Visa only. Street address and postal code not verified because of incompatible formats. (Acquirer sent both street address and postal code.)
-----	--

D =	Visa only. Street addresses and postal code match.
-----	--

F =	Visa only. Street address and postal code match. Applies to U.K. only.
-----	--

G =	Visa only. Non-AVS participant outside the U.S.; address not verified for international transaction.
-----	--

I =	Visa only. Address information not verified for international transaction.
-----	--

M =	Visa only. Street addresses and postal code match.
-----	--

N =	Neither address nor postal code matches.
-----	--

P =	Visa only. Postal codes match. Street address not verified because of incompatible formats. (Acquirer sent both street address and postal code.)
-----	--

R =	Retry, system unable to process.
-----	----------------------------------

S =	AVS currently not supported.
-----	------------------------------

U =	No data from issuer/Authorization Platform
-----	--

W =	For U.S. addresses, nine-digit postal code matches, address does not; for address outside the U.S., postal code matches, address does not.
-----	--

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

X	=	For U.S. addresses, nine-digit postal code and address matches; for addresses outside the U.S., postal code and address match.
---	---	--

Y	=	For U.S. addresses, five-digit postal code and address matches.
---	---	---

Z	=	For U.S. addresses, five-digit postal code matches, address does not.
---	---	---

### Subelement 84—Merchant Advice Code

DE 48, subelement 84 (Merchant Advice Code) contains the merchant advice code.

---

#### Attributes

---

Subelement ID:	84
----------------	----

Length of Length Field:	2
-------------------------	---

Data Representation:	an-2
----------------------	------

Data Field:	Contents of positions 1–2
-------------	---------------------------

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

---

#### Usage

---

Subelement 84 is optionally provided by the issuer in the Authorization Request Response/0110 message.

Following is the usage of subelement 84 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	O	•	O
Authorization Advice/0120—Issuer-generated	C	•	C

---

#### Values

---

01	=	New account information available
----	---	-----------------------------------

02	=	Cannot approve at this time, try again later
----	---	--

03	=	Do not try again
----	---	------------------

21	=	Recurring Payment Cancellation Service (MasterCard use only)
----	---	--

### Subelement 84—Visa Response Codes (Visa Only)

DE 48, subelement 84 (Visa Response Codes) will contain the following new values when a Visa issuer provides an alpha-numeric value in Visa Field 39 (Response Code).

**Attributes**

Subelement ID:	84
Length of Length Field:	2
Data Representation:	an-2
Data Field:	Contents of position 1–2
Subfields:	N/A
Justification:	N/A

**Usage**

Following is the usage of subelement 84 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	•	X	C

**Values**

R0 = Stop Payment Order
R1 = Revocation of Authorization Order
R3 = Revocation of All Authorizations Order

## **Subelement 85—U.S. Existing Debt Indicator (Visa Only)**

DE 48, subelement 85 (U.S. Existing Debt Indicator) indicates the transaction is a payment for an existing U.S. debt.

**Attributes**

Subelement ID:	85
Length of Length Field:	2
Data Representation:	n-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

**Usage**

Subelement 85 contains an indicator to denote a payment for an existing debt on a Visa account, when applicable.

Following is the usage of subelement 85 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Org    Sys    Dst

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
<b>Values</b>			
9 = Existing U.S. Debt			

### Subelement 86—Relationship Participant Indicator (Visa Only)

DE 48, subelement 86 (Relationship Participant Indicator) indicates the transaction is with a cardholder with whom the merchant has had a long-term relationship and from whom the merchant regularly collects recurring payments.

---

#### Attributes

---

Subelement ID:	86
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

---

#### Usage

---

Subelement 86 contains an indicator to denote a recurring payment transaction on a Visa account for a cardholder with a long standing relationship.

Following is the usage of subelement 86 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE

---

#### Values

---

I = Installment Payment

R = Merchant/Cardholder Relationship

### Subelement 87—Card Validation Code Result

DE 48, subelement 87 (Card Validation Code Result) indicates the CVC 1, CVC 2, or CVC 3 result code.

### **Attributes**

Subelement ID:	87
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

### **Usage**

Subelement 87 must be provided by the issuer in the Authorization Request Response/0110 message whenever CVC 2 verification is requested by the acquirer.

Subelement is optional whenever DE 45 (Track 1 Data) or DE 35 (Track 2 Data) is present in the Authorization Request/0100 message and CVC 1 is invalid.

Subelement 87 is optionally provided in the Authorization Request Response/0110 message when an issue is encountered during CVC 3 validation.

Following is the usage of subelement 87 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	C	•	C
Authorization Advice/0120	•	C	C

### **Values**

#### **CVC 1**

Y = Invalid CVC 1 (only if DE 35 (Track 2 Data) or DE 45 (Track 1 Data) is present in the Authorization Request/0100 message.)

#### **CVC 2**

M = Valid CVC 2 (match)

N = Invalid CVC 2 (non-match)

P = CVC 2 not processed (issuer temporarily unavailable)

U = CVC 2 Unverified—MasterCard Use Only

#### **CVC 3**

E = Length of unpredictable number was not a valid length

P = Unable to process

Y = Invalid

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Subelement 87—CVV2 Response (Visa Only)

DE 48, subelement 87 (CVV2 Response) indicates the CVV2 response on a Visa account.

---

##### Attributes

---

Subelement ID: 87

---

Length of Length Field: 2

---

Data Representation: a-1

---

Data Field: Contents of position 1

---

Subfields: N/A

---

Justification: N/A

---

##### Usage

---

Following is the usage of subelement 87 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
--	-----	-----	-----

Authorization Request Response/0110	C	•	C
-------------------------------------	---	---	---

---

##### Values

---

M = CVV2 match

---

N = CVV2 no match

---

P = Not processed

---

S = CVV2 is on the card, but the merchant has indicated that CVV2 is not present.

---

U = Issuer is not Visa-certified for CVV2, has not provided Visa encryption keys, or both.

---

#### Subelement 88—Magnetic Stripe Compliance Status Indicator

DE 48, subelement 88 (Magnetic Stripe Compliance Status Indicator) indicates that the Authorization Platform replaced the DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) value of 90 or 91 with value of 02.

---

##### Attributes

---

Subelement ID: 88

---

Length of Length Field: 2

---

Data Representation: a-1

---

Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

#### **Usage**

Subelement 88 is provided by the Authorization Platform whenever the Authorization Platform replaces the DE 22, subfield 1, value of 90 or 91 to a value of 02 due to magnetic stripe compliance downgrade of the acquirer.

Following is the usage of subelement 88 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request /0100	•	C	C
Authorization Request Response/0110	CE	C	C
Authorization Advice/0120—Issuer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C

#### **Values**

Y = Authorization Platform replaced DE 22, subfield 1, value 90 or 91 with value 02.

## **Subelement 89—Magnetic Stripe Compliance Error Indicator**

DE 48, subelement 89 (Magnetic Stripe Compliance Error Indicator) indicates magnetic stripe compliance errors.

---

#### **Attributes**

Subelement ID:	89
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

#### **Usage**

Subelement 89 is provided by the Authorization Platform whenever errors are detected while editing transactions for magnetic stripe compliance. Following is the usage of subelement 89 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Org    Sys    Dst

## Data Element Definitions

### DE 48—Additional Data—Private Use

Authorization Request/0100	•	C	C
Authorization Request Response/0110	CE	C	C
Authorization Advice/0120—Issuer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C
<b>Values</b>			
A =	Track 1 or Track 2 not present in the message		
B =	Track 1 and Track 2 present in the message		
C =	DE 2 (Primary Account Number [PAN]) not equal in track data		
D =	DE 14 (Expiration Date) not equal in track data		
E =	Service code invalid in track data		
F =	Field separator(s) invalid in track data		
G =	A field within the track data has an invalid length		
H =	DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) is 80, 90, or 91 when DE 48, Transaction Category Code (TCC) is T		
I =	DE 61 (Point-of-Service Data), subfield 4 (POS Cardholder Presence) is 1, 2, 3, 4, or 5		
J =	DE 61 Point-of-Service Data), subfield 5 (POS Card Presence ) is 1		

### Subelement 90—Lodging and Auto Rental Indicator

DE 48, subelement 90 (Lodging and Auto Rental Indicator) indicates the presence of Lodging and Auto Rental Service interchange program.

#### Attributes

Subelement ID:	90
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

#### Usage

Subelement 90 is provided whenever the cardholder is a preferred customer of the merchant.

Following is the usage of subelement 90 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request /0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Issuer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C

#### **Values**

P = Cardholder is enrolled in a merchant preferred customer program and magnetic stripe data may be absent

## **Subelement 90—Custom Payment Service Request (Visa Only)**

DE 48, subelement 90 (Custom Payment Service Request) contains the Authorization Characteristics Indicator (Visa field 62.1).

---

#### **Attributes**

Subelement ID:	90
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

---

#### **Usage**

Subelement 90 is used to indicate a custom payment service transaction on a Visa account whenever applicable.

Following is the usage of subelement 90 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Reversal Request/0400	C	•	C

---

#### **Values**

Y = Request for Custom Payment Service participation

**Data Element Definitions****DE 48—Additional Data—Private Use****Subelement 90—Custom Payment Service Request Response  
(Visa Only)**

DE 48, subelement 90 (Custom Payment Service Request Response) contains the Authorization Characteristics Indicator (Visa field 62.1).

**Attributes**

Subelement ID:	90
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

**Usage**

	Org	Sys	Dst
Authorization Request Response/0110	C	•	C
Reversal Request Response/0410	C	•	C

**Values**

Acquirer Receives		
Qualified	Not Qualified	
A	N or T <sup>9</sup>	Card present; magnetic stripe read and sent, CVV requested.
C	N or T	Meets requirements for A, plus merchant name, location present, and UCAT indicator set, but no signature required: AFD.
E	N or T	Meets requirements for A, plus merchant/ATM owner name and location (enriched name and location data) present.
V	N or T	Meets address verification requirements; verification requested for card-not-present transactions (Direct Marketing, Passenger Transport).

**Application Notes**

If the request qualifies for Visa CPS and is approved, the acquirer receives an “A”, “E”, “V”, or “C” in the 0110 or 0410 response. If the original request does not qualify for CPS, Visa returns an “N” or “T” in the response.

9. “T” applies to U.S. transactions only, including those from non-U.S. acquirers to U.S. issuers.

## **Subelement 91—Acquirer Reference Data (American Express Only)**

DE 48, subelement 91 (Acquirer Reference Data) contains the 15-digit Transaction Identifier (TID), a unique American Express tracking number. The TID is used to identify and track a card customer transaction throughout its life cycle.

---

### **Attributes**

---

Subelement ID:	91
Length of Length Field:	2
Data Representation:	ans...15
Data Field:	Contents of positions 1–15
Subfields:	N/A

---

### **Usage**

---

Following is the usage of subelement 91 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	M	•	M

---

### **Values**

---

A unique 15 digit TID.

---

## **Subelement 91—Custom Payment Service Request Transaction ID (Visa Only)**

DE 48, subelement 91 (Custom Payment Service Request Transaction ID) indicates the presence of Custom Payment Service Request response data.

---

### **Attributes**

---

Subelement ID:	91
Length of Length Field:	2
Data Representation:	an...19
Data Field:	Contents of positions 1–19
Subfields:	N/A

---

### **Usage**

---

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Subelement 91 is used to provide transaction ID and Validation Code when incremental authorization and partial reversals (subelement 90) are requested on a Visa account.

Following is the usage of subelement 91 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Reversal Request/0400	C	•	C

#### Values

Subelement 91 must contain the transaction ID (Visa field 62.2, 15 byte numeric) and validation code (Visa field 62.3, 4 bytes alphanumeric) when subelement 90 indicates an incremental authorization and partial reversal on a Visa account.

## Subelement 91—Custom Payment Service Response Transaction ID (Visa Only)

DE 48, subelement 91 (Custom Payment Service Response Transaction ID) provides authorization response data when custom payment service (subelement 90) is requested on a Visa account.

---

#### Attributes

---

Subelement ID:	91
Length of Length Field:	2
Data Representation:	ans...19
Data Field:	Contents of positions 1–2, 1–6, 1–15, or 1–19 depending on the length field
Subfields:	N/A

---

#### Usage

---

Following is the usage of subelement 91 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	C	C	C

---

#### Values

---

##### When length field is 02:

---

Subelement 90 contains N and subelement 91 contains one of the following MasterCard assigned reason codes:

MS = MasterCard Stand-In processed the transaction; custom payment service-qualified information unavailable.

MX = MasterCard X-Code processed the transaction; custom payment service-qualified information unavailable

VS = Visa did not supply a downgrade reason code.

---

**When length field is 06:**

---

VS = Downgraded by Visa (two bytes alphanumeric), followed by either:

- Visa validation code (four bytes alphanumeric) or
- Downgrade reason code (two bytes alphanumeric code followed by two spaces)

Refer to the Visa Base I Technical Specifications manual for more information on Visa CPS validation codes and specific CPS downgrade reason codes and meanings.

---

**When length field is 15:**

---

Subelement 91 contains the transaction ID (Visa field 62.2, 15 bytes numeric) for an incremental or reversal response.

---

**When length field is 19:**

---

Subelement 91 contains the transaction ID (Visa field 62.2, 15 byte numeric) and validation code (Visa field 62.3, 4 bytes alphanumeric) for the appropriate characteristics indicator.

---

## **Subelement 92—CVC 2**

DE 48, subelement 92 (CVC 2) contains the CVC 2 value from the signature panel of the card.

---

**Attributes**

---

Subelement ID: 92

---

Length of Length Field: 2

---

Data Representation: n-3

---

Data Field: Contents of positions 1–3

---

Subfields: N/A

---

Justification: N/A

---

**Usage**

---

Subelement 92 contains the CVC 2 value from the signature panel of the card when applicable.

Following is the usage of subelement 92 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Org    Sys    Dst

## Data Element Definitions

### DE 48—Additional Data—Private Use

Authorization Request /0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120	•	C	C
Authorization Advice/0120—Issuer-generated	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C

#### Values

Acquirers must not use 000 as a default when sending this subelement. Acquirers must only provide this subelement when requesting CVC 2 verification.

## Subelement 92—CVV2 Data (Visa Only)

DE 48, subelement 92 (CVV2 Data) consists of the Visa CVV2 presence ID, response type, and CVV2 value.

#### Attributes

Subelement ID:	92
Length of Length Field:	2
Data Representation:	n-6
Data Field:	Contents of positions 1, 2, and 3
Subfields:	3
Justification:	See “Subfields”

#### Usage

Subelement 92 contains the CVV2 value from the signature panel of the card when applicable.

Following is the usage of subelement 92 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request /0100	C	•	C
Authorization Request Response/0110	CE	•	CE

#### Values

##### Position 1 (CVV2 Presence ID)

Data Representation:	n-1
Data Field:	Contents of position 1
Values:	0 = Merchant did not provide CVV2 or it was deliberately bypassed

1	=	CVV2 value present
2	=	CVV2 is on card, but not legible
9	=	Cardholder states no CVV2 is on card

#### **Position 2 (CVV2 Response Code)**

Data Representation:		n-1
Data Field:		Contents of position 2
Values:	0	= Only the normal response code in DE 39 should be returned by the issuer
	1	= The normal response code and CVV2 response code should be returned by the issuer

#### **Position 3 (CVV2 Value)**

Data Representation:		n-4; Right justified, blank-filled
Data Field:		Contents of positions 3–6
Values:		CVV2 value from the signature panel of the card.

### **Subelement 93—Fleet Card ID Request Data (Visa Only)**

DE 48, subelement 93 (Fleet Card ID Request Data) contains the Fleet Card ID information on a Visa account, when applicable.

#### **Attributes**

Subelement ID:		93
Length of Length Field:		2
Data Representation:		ans...19
Data Field:		Contents of subfields
Subfields:		2
Justification:		N/A

#### **Usage**

Following is the usage of subelement 93 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Org      Sys      Dst

Authorization Request /0100	C	•	C
-----------------------------	---	---	---

#### **Values**

See “Subfields”

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Subfield 1—Fleet Card ID Request Indicator

DE 48, subelement 93, subfield 1 (Fleet Card ID Request Indicator) identifies the Fleet Card ID.

---

##### Attributes

---

Data Representation: ans-2

---

Data Field: Contents of position 1–2

---

Values: \$\$ = Fleet Card ID

---

#### Subfield 2—Optional Free-form Informational Text

DE 48, subelement 93, subfield 2 (Optional Free-form Informational Text) provides additional Point-of-Service (POS) information.

---

##### Attributes

---

Data Representation: ans...17

---

Data Field: Contents of positions 3–19

---

Values: Additional Point-of-Service (POS) information (optional)

---

### Subelement 94—Commercial Card Inquiry Request (Visa Only)

Subelement 94 (Commercial Card Inquiry Request) contains an indicator requesting a commercial card inquiry on a Visa account, when applicable.

---

##### Attributes

---

Subelement ID: 94

---

Length of Length Field: 2

---

Data Representation: ans-4

---

Data Field: Contents of positions

---

Subfields: N/A

---

Justification: N/A

---

---

##### Usage

---

Following is the usage of subelement 94 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
--	-----	-----	-----

Authorization Request /0100	C	•	C
Reversal Request/0400	C	•	C

**Values**

Positions 1–3 (Card Request Indicator)

Data Representation: ans-3

Data Field: Contents of positions 1–3 (Hexadecimal value: 5AF0F1)

Values: !01 (where 0 is zero) = Commercial Card Inquiry

Position 4 (Merchant Request for Commercial Card Type)

Data Representation: ans-1

Data Field: Contents of position 4

Values: 0 (where 0 is zero) = Request Indicator

## **Subelement 94—Commercial Card Inquiry Response (Visa Only)**

DE 48, subelement 94 (Commercial Card Inquiry Response) contains the commercial card inquiry response data as a result of a commercial card inquiry on a Visa account.

**Attributes**

Subelement ID: 94

Length of Length Field: 2

Data Representation: ans-4

Data Field: Contents of positions

Subfields: N/A

Justification: N/A

**Usage**

Following is the usage of subelement 94 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
--	-----	-----	-----

Authorization Request Response/0110

C	•	C
---	---	---

**Values**

Positions 1–3 (Card Request Indicator)

Data Representation: ans-3

Data Field: Contents of positions 1–3 (Hexadecimal value: 5AF0F1)

Values: !01 (where 0 is zero) = Commercial Card Inquiry

Position 4 (Visa Commercial Card Response)

## Data Element Definitions

### DE 48—Additional Data—Private Use

Data Representation:	a-1
Data Field:	Contents of position 4
Values:	0 (where 0 is zero) = Not a Commercial Card B = Business Card R = Corporate Card S = Purchasing Card

### Subelement 95—MasterCard Promotion Code

DE 48, subelement 95 (MasterCard Promotion Code) contains the promotion code to identify unique use of a MasterCard® card for a specific program or service established between issuers and merchants.

#### Attributes

Subelement ID:	95
Length of Length Field:	2
Data Representation:	an-6
Data Field:	Contents of positions 1–6
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of subelement 95 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request /0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Issuer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE

#### Values

Program or service specific.

ARGCTA = Installment payment transaction within Argentina

GREECE = Installment payment transaction within Greece

MCGARS	=	Identifies Global Automated Service (GARS) Stand-In activity
MEXCTA	=	Installment payment transaction within Mexico
PARCEL	=	Installment payment transaction within Brazil
PERCTA	=	Installment payment transaction within Peru
PHINST	=	Installment payment transaction within Philippines
PRYCTA	=	Installment payment transaction within Paraguay
URYCTA	=	Installment payment transaction within Uruguay

## **Subelement 95—American Express Customer ID Number (American Express Only)**

DE 48, subelement 95 (American Express Customer ID Number) contains the American Express Customer ID Number (CIN) from the face of the American Express card, when applicable.

---

### **Attributes**

---

Subelement ID:	95
Length of Length Field:	2
Data Representation:	n-4
Data Field:	Contents of positions 1–4
Subfields:	N/A
Justification:	N/A

---

### **Usage**

---

Following is the usage of subelement 95 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE

---

### **Values**

---

The four-digit customer ID number on the front of the American Express card.

---

## **Subelement 96—Visa Market-Specific Data Identifier (Visa Only)**

DE 48, subelement 96 (Visa Market-Specific Data Identifier) contains the market-specific data identifier.

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

#### Attributes

Subelement ID:	96
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of subelement 96 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request /0100	C	•	C
Authorization Request Response/0110	CE/C	•	CE/C
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE

#### Values

A	=	Automobile rental
B	=	Bill Payment Transaction
H	=	Hotel rental
M	=	Healthcare—Medical
N	=	Failed market-specific data edit

## Subelement 97—Prestigious Properties Indicator (Visa Only)

DE 48, subelement 97 (Prestigious Properties Indicator) contains the prestigious property indicator. For participants in the Visa Prestigious Lodging program (conditional).

#### Attributes

Subelement ID:	97
Length of Length Field:	2
Data Representation:	a-1
Data Field:	Contents of position 1
Subfields:	N/A

Justification:	N/A
----------------	-----

**Usage**

Following is the usage of subelement 97 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE

**Values**

D	=	Visa established limits
B	=	Visa established limits
S	=	Visa established limits

## **Subelement 98—MasterCard Corporate Fleet Card ID/Driver Number**

DE 48, subelement 98 (MasterCard Corporate Fleet Card ID/Driver Number) allows the corporate customer to verify the user of the card and enables more detailed reporting. It contains the ID of the user of a Fleet card, when applicable.

**Attributes**

Subelement ID:	98
Length of Length Field:	2
Data Representation:	n-6
Data Field:	Contents of positions 1–6
Subfields:	N/A
Justification:	N/A

**Usage**

Following is the usage of subelement 98 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request /0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	•	C

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	•	CE

#### Values

---

Cardholder unique.

---

#### Application Notes

---

If DE 48, subelement 98 (MasterCard Corporate Fleet Card ID/Driver Number) was present in the original 0100 AFD authorization message, subelement 98 must be the same value in acquirer-generated 0120 completion advice.

---

## Subelement 99—MasterCard Corporate Fleet Card Vehicle Number

DE 48, subelement 99 (MasterCard Corporate Fleet Card Vehicle Number) allows the corporate customer to verify the user of the card and enables more detailed reporting. It contains the ID of the vehicle used in conjunction with a Fleet card purchase, when applicable.

---

#### Attributes

---

Subelement ID:	99
Length of Length Field:	2
Data Representation:	n-6
Data Field:	Contents of positions 1–6
Subfields:	N/A
Justification:	N/A

---

#### Usage

---

Following is the usage of subelement 99 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request /0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	•	CE

#### Values

---

---

Vehicle-specific

---

**Application Notes**

---

If subelement 99 was present in the original 0100 AFD authorization message, subelement 99 must be the same value in acquirer-generated 0120 completion advice.

---

## **DE 48—Authorization Platform Edits**

The Authorization Platform performs edits as described in this section.

### **DE 48, TCC**

The Authorization Platform performs the following edit.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
An Authorization Request/0100, Authorization Advice/0120, or Reversal Request/0400 message contains DE 48, TCC with an invalid value in position 1	<p>Rejects the message and forwards the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 message where:</p> <ul style="list-style-type: none"><li>• DE 39 = 30 (Format Error)</li><li>• DE 44 = 048</li></ul>

### **DE 48, TCC and DE 3**

The Authorization System performs the following edits.

<b>WHEN TCC contains...</b>	<b>THEN the first two positions of DE 3 (Processing Code) must contain one of the following values...</b>
C = Cash Disbursement	01 = Withdrawal 17 = Cash Disbursement 30 = Balance Inquiry
P = Payment Transaction	28 = Payment Transaction
Z = ATM Cash Disbursement	00 = Purchase 01 = Withdrawal 30 = Balance Inquiry 91 = PIN Unblock 92 = PIN Change Only eligible acquirers may use values 91 or 92.
<b>IF this edit...</b>	<b>THEN the Authorization Platform...</b>

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Fails	Rejects the transaction with a format error, indicated by: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30</li><li>• DE 44 (Additional Response Data = 003)</li></ul>
Passes	Goes to the next edit
WHEN...	THEN the Authorization Platform...
TCC contains a space	Assigns in an Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, and Reversal Request/0400 message, a TCC value based on the card acceptor business code/merchant category code (MCC) in DE 18 (Merchant Type) except under the following conditions
WHEN...	THEN the Authorization Platform...
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type) contains value 00 (Purchase) and DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) contains value 00 (PAN entry mode unknown) or value 01 (PAN manual entry) and DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence) <b>does not</b> contain value 0 (Cardholder Present)	Assigns TCC value T (Phone, Mail, or Electronic Commerce Order).

### DE 48, Subelement 32

The Authorization Platform will perform the following edits.

WHEN the issuer is set up for Private Label Merchant Verification Service and...	THEN the Authorization Platform...
The account range is set up as private label, but DE 42 (Card Acceptor ID Code) or DE 48 (Additional Data—Private Use) subelement 32 (MasterCard Assigned ID) in Authorization Request/0100 message does not find a match.	Rejects the transaction and sends the Authorization Request Response/0110 to acquirer where: <ul style="list-style-type: none"><li>• DE 39 = 58 (Transaction not permitted to acquirer or terminal)</li><li>• DE 44 = 042</li></ul>
WHEN the issuer is set up for Co-brand Proprietary Transaction Management Service and...	THEN the Authorization Platform...

The account range is set up as co-branded proprietary, and DE 48 (Additional Data—Private Use) subelement 32 (MasterCard Assigned ID) in Authorization Request/0100 message does find a match	Processes the transaction as a Private Label product and places the appropriate private label product code in the Authorization Request/0100 message containing DE 63 (Network Data), subfield 1 (Financial Network Code) before routing the transaction to the issuer.
The account range is set up as co-branded proprietary, and DE 48 (Additional Data—Private Use) subelement 32 (MasterCard Assigned ID) in Authorization Request/0100 message does not find a match	Processes the transaction as a MasterCard product and places the MasterCard product code in the Authorization Request/0100 message containing DE 63 (Network Data), subfield 1 (Financial Network Code) before routing the transaction to the issuer.

### **DE 48, Subelement 35**

The Authorization Platform performs the following edits.

Following are Authorization Request/0100 message edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The acquirer sends an Authorization Request/0100 message containing DE 48 (Additional Data—Private Use), subelement 35 ( <i>PayPass Non—Card Form Factor Request/Response</i> )	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30 (Format error)</li> <li>• DE 44 = 048</li> </ul>

The issuer-branded Web site will perform the following processing based on the Authorization Request Response/0110 messages.

<b>WHEN...</b>	<b>THEN the issuer-branded Web Site...</b>
The Authorization Request Response/0110 message contains DE 48, subelement 35, value A	Arranges for the request <i>PayPass</i> card or device to be sent to the cardholder

## Data Element Definitions

### DE 48—Additional Data—Private Use

The Authorization Request Response/0110 message contains DE 48, subelement 35, value D	Declines the cardholders' request for the <i>PayPass</i> card or device and instructs the cardholder to contact the issuer for more information
<p>The Authorization Request/0100 message contains DE 48, subelement 35 and the Authorization Request Response/0110 message does not contain DE 48, subelement 35</p> <p>or</p> <p>The Authorization Request Response/0110 message containing DE 48, subelement 35 does not contain a valid value of A or D</p>	<p>Arranges for the requested <i>PayPass</i> card or device to be sent to the cardholder when:</p> <p>Subelement 83 (Address Verification Service Response) is X or Y and</p> <p>Subelement 87 (Card Validation Code Result) is M</p>

### DE 48, Subelement 38

The Authorization Platform performs the following edits.

WHEN...	THEN...
<p>The Authorization Platform finds that the entire account range no longer participates in Enhanced Value, Product Graduation, or High Value</p> <p>and</p> <p>At least one cardholder account within the account range previously participated in Enhanced Value, Product Graduation, or High Value</p>	<p>The Authorization Platform adds DE 48, subelement 38 (Account Category), value Z to the Authorization Request/0100 message for the following transaction types:</p> <ul style="list-style-type: none"><li>• Purchases as indicated by DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) = 00</li><li>• Purchase with Cash Back as indicated by DE 3, subfield 1 = 09</li></ul> <p>and</p> <p>The Authorization Platform forwards the Authorization Request/0100 message to the issuer.</p>
<p>The Authorization Platform provides DE 48, subelement 38 in the Authorization Request/0100 message to the issuer</p> <p>and</p> <p>The issuer populates DE 39 (Response Code) in the Authorization Request Response/0110 message with one of the following values that indicate an authorization approval:</p> <ul style="list-style-type: none"><li>• 00 (Approved or completed successfully)</li><li>• 08 (Honor with ID)</li></ul>	<p>DE 38 (Authorization ID Response), position 6 in the Authorization Request Response/0110 message must equal the value of DE 48, subelement 38 of the original Authorization Request/0100 message that was provided to the issuer by the Authorization Platform.</p>

<b>WHEN...</b>	<b>THEN...</b>
<ul style="list-style-type: none"> <li>• 10 (Partial Approval)</li> <li>• 87 (Purchase Amount Only, No Cash Back Allowed)</li> </ul>	
<p>The Authorization Platform provides DE 48, subelement 38 in the Authorization Request/0100 message to the issuer and</p> <p>The issuer populates DE 39 (Response Code) in the Authorization Request Response/0110 message with the value 85 (Not declined) and</p> <p>DE 38 is present</p>	<p>DE 38 (Authorization ID Response), position 6 in the Authorization Request Response/0110 message must equal the value of DE 48, subelement 38 of the original Authorization Request/0100 message that was provided to the issuer by the Authorization Platform.</p> <p>If DE 38 is not present, the Authorization Platform will not perform this validation.</p>
<p>DE 38, position 6 in the Authorization Request Response/0110 message does not equal the value of DE 48, subelement 38 of the original Authorization Request/0100 message that was provided to the issuer by the Authorization Platform</p>	<p>The Authorization Platform rejects the Authorization Request /0100 message and sends the Authorization Request Response/0110 message to the Stand-In System for processing.</p> <p>Stand-In will ensure that DE 38, position 6 of the Authorization Request Response/0110 message matches the value provided by the Authorization Platform in DE 48, subelement 38 of the Authorization Request/0100 message.</p>
<p>DE 48, subelement 38 is included in the Authorization Request Response/0110 message from the issuer</p>	<p>The Authorization Platform removes DE 48, subelement 38 from the Authorization Request Response/0110 message before providing the 0110 message to the acquirer.</p>

### **DE 48, Subelement 42 and Subelement 43**

The Authorization Platform performs the following edits on Authorization Request/0100 and Authorization Advice/0120 messages.

<b>WHEN DE 48, subelement 42, subfield 01, position 3 is...</b>	<b>THEN DE 48, subelement 43...</b>
0 or is not present	Cannot contain UCAF data.
1	Cannot contain UCAF data.
2 or 3 and PAN is not MasterCard Electronic	Must contain UCAF data.
<b>IF this edit...</b>	<b>THEN the Authorization Platform...</b>

## Data Element Definitions

### DE 48—Additional Data—Private Use

---

Fails	Rejects the transaction with a format error, indicated by: DE 39 = 30 DE 44 = 048
Passes	The Authorization Platform goes to the next edit.
<hr/>	
<b>WHEN DE 48, subelement 43...</b>	<b>THEN DE 48, subelement 42, subfield 01, position 3 must equal...</b>
Contains UCAF data	2 or 3
Does not contains UCAF data	0 or 1, or not be present
<hr/>	
<b>IF this edit...</b>	<b>THEN the Authorization Platform...</b>
Fails	Rejects the transaction with a format error, indicated by: DE 39 (Response Code) = 30 DE 44 (Additional Response Data) = 048
Passes	The Authorization Platform goes to the next edit.
<hr/>	

### DE 48, Subelement 43 (Static AAV for Maestro or MasterCard Advance Registration Program)

The following edits on Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages are performed on transactions submitted under the MasterCard Advance Registration Program and the Maestro Advance Registration Program.

<b>WHEN the MasterCard assigned static AAV in DE 48, subelement 43, position 1 begins with...</b>	<b>THEN the Authorization System...</b>
3 and the acceptance brand is not Maestro	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: DE 39 (Response Code) = 30 (Format error) DE 44 = 048 (identifying the data element in error)
4 and the acceptance brand is not MasterCard	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: DE 39 = 30 DE 44 = 048

<b>WHEN the MasterCard assigned static AAV in DE 48, subelement 43, position 1 begins with...</b>	<b>THEN the Authorization System...</b>
5 and the acceptance brands are not MasterCard and Maestro	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where:  DE 39 = 30 DE 44 = 048
Any value other than 3, 4, or 5 and the acceptance brands are MasterCard, Maestro, or both	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where:  DE 39 = 30 DE 44 = 048

### **DE 48, Subelement 42 and DE 61**

The Authorization Platform performs the following edits.

The following edits apply on Electronic Commerce transactions.

<b>WHEN...</b>	<b>THEN...</b>
DE 48, subelement 42, subfield 1, position 3 contains value 1, 2, or 3, and  DE 61, subfield 10, contains value 6	DE 61, subfield 4 contains value 4 or 5 and DE 61, subfield 7, must not contain value 2
<b>IF this edit...</b>	<b>THEN the Authorization Platform...</b>
Fails	Generates a format error, indicated by:  DE 39 (Response Code) = 30 DE 44 (Additional Response Data) = 061
Passes	The Authorization Platform goes to the next edit.

The following edits apply on SecureCode Phone Order transactions.

<b>WHEN...</b>	<b>THEN...</b>
DE 48, subelement 42, subfield 1, position 3 contains value 1 or 2 and  DE 61, subfield 7 contains value 2	DE 61, subfield 4 must contain a value 3 or 4 and DE 61, subfield 10 must not contain value 6.
<b>IF this edit...</b>	<b>THEN the Authorization Platform...</b>

## Data Element Definitions

### DE 48—Additional Data—Private Use

WHEN...	THEN...
Fails	Generates a format error indicated by: DE 39 = 30 DE 44 = 061
Passes	The Authorization Platform goes to the next edit.

### DE 48, Subelement 61

The Authorization Platform performs the following edits.

WHEN...	THEN the Authorization Platform...
DE 48, subelement 61 is present and DE 4 contains all zeros	Drops DE 48, subelement 61 from the Authorization Request/0100 message to the issuer.
<hr/>	
WHEN DE 48, subelement 61, subfield 3 is...	THEN the Authorization Platform...
1 (Merchant terminal verified the purchase items against an Inventory Information Approval System [IIAS])	Validates that DE 48, subelement 32 (if present) contains a valid MasterCard Assigned ID for IIAS.
IF the...	THEN the Authorization Platform...
MasterCard Assigned ID is valid	Updates the value in DE 48, subelement 61, subfield 3 as follows: <ul style="list-style-type: none"><li>If the issuer participates in real-time substantiation, sends DE 48, subelement 61, subfield 3, value 1 (Merchant terminal verified the purchased items against an IIAS)</li><li>If the issuer does not participate in real-time substantiation sends DE 48, subelement 61, subfield 3, value 0 (Merchant terminal did not verify the purchased items against an IIAS).</li></ul>
MasterCard Assigned ID is not valid or not present in the Authorization Request/0100 message	Updates the value in DE 48, subelement 61, subfield 3 as follows: <ul style="list-style-type: none"><li>If the issuer participates in real-time substantiation, sends DE 48, subelement 61, subfield 3, value 4 (Transaction was submitted as real-time substantiated but from a non-IIAS certified merchant).</li><li>If the issuer does not participate in real-time substantiation sends DE 48,</li></ul>

subelement 61, subfield 3, value 0  
 (Merchant terminal did not verify the purchased items against an IIAS).

The following edits are on Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The acquirer sends DE 48, subelement 61, subfield 3 (Real-time Substantiation Indicator), value 2 (Merchant claims exemption from IIAS rules based on the IRS 90 percent rule) in an Authorization Request/0100 message or Authorization Advice/0120—Acquirer-generated message</p> <p>and</p> <p>The issuer does not participate in real-time substantiation</p>	<p>Forwards the issuer the Authorization Request/0100 or Authorization Advice/0120—Acquirer-generated message containing DE 48, subelement 61, subfield 3, value 0 (Merchant terminal did not verify the purchased items against an IIAS).</p>
<p>The acquirer sends DE 48, subelement 61, subfield 3 (Real-time Substantiation Indicator), value 2 (Merchant claims exemption from IIAS rules based on the IRS 90 percent rule) in an Authorization Request/0100 message or Authorization Advice/0120—Acquirer-generated message</p> <p>and</p> <p>The issuer does participate in real-time substantiation</p>	<p>Forwards the issuer the Authorization Request/0100 or Authorization Advice/0120—Acquirer-generated message containing DE 48, subelement 61, subfield 3, value 2 (Merchant claims exemption from using the IIAS, based on the IRS 90 percent rule).</p>
<p>The acquirer sends DE 48, subelement 61, subfield 3 (Real-time Substantiation Indicator), value other than 0, 1, or 2 in Authorization Request/0100 or Authorization Advice/0120—Acquirer-generated message</p>	<p>Declines the Authorization Request/0100 or Authorization Advice/0120—Acquirer-generated messages where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) is 30</li> <li>• DE 44 (Response Data) is 048</li> </ul>

## **DE 48, Subelement 78**

The Authorization Platform performs the following edits.

<b>WHEN DE 48, Subelement 78 is...</b>	<b>THEN DE 2...</b>
D (Deferred Billing)	DE 2 (Primary Account Number [PAN]) must be a Visa PAN

**Data Element Definitions**  
**DE 49—Currency Code, Transaction**

---

**DE 48, Subelement 82**

The Authorization Platform performs the following edits.

<b>WHEN DE 48, Subelement 82 is...</b>	<b>THEN the Authorization Platform...</b>
51 (AVS-Only)	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 12 (Invalid Transaction)

**DE 48, Subelement 86**

The Authorization Platform performs the following edits.

<b>WHEN DE 48, Subelement 86 is...</b>	<b>THEN DE 2...</b>
R (Relationship Participant)	DE 2 (Primary Account Number [PAN]) must be a Visa PAN

**DE 48, in Authorization Request Response**

The following edit applies to DE 48 and the Authorization Request Response/0110 message.

<b>WHEN the issuer...</b>	<b>THEN the Authorization Request Response/0110 message must...</b>
Provides response data, such as AVS response, Merchant Advice Code, CVC 2 response, and CVC 1 response, in DE 48 of the Authorization Request Response/0110 message	Contain the TCC as the first byte of data within DE 48 and Contain all the subelements present in DE 48 of the original Authorization Request/0100 message that also are defined in the Authorization Request Response/0110 message.
Does not provide response data	Not contain DE 48, including the TCC.

**DE 49—Currency Code, Transaction**

DE 49 (Currency Code, Transaction) is the local currency of the acquirer or source location of the transaction. It specifies the currency used in DE 4 (Amount, Transaction).

---

**Attributes**

---

Length of Length Field:	N/A
Data Representation:	n-3

Data Field:	Contents of positions 1–3
Subfields:	N/A
Justification:	N/A

#### **Usage**

Following is the usage of DE 49 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M
Authorization Request Response/0110	ME	•	ME
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	ME	ME
Reversal Request/0400	M	•	M
Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•

#### **Values**

All currency codes must be selected from the numeric ISO standard currency codes. ISO standard currency codes identify DE 49. A list of valid values is available in the *Quick Reference Booklet*.

#### **Application Notes**

This data element is defined and used identically within all MasterCard programs and services.

Acquirers will receive an Authorization Request Response/0110 message containing a format error in DE 39 when the currency code in DE 49 is a currency code other than those in the ISO Standard Currency Codes table.

## **DE 50—Currency Code, Settlement**

DE 50 (Currency Code, Settlement) defines the currency of DE 5 (Amount, Settlement) and DE 29 (Amount, Settlement Fee).

**Data Element Definitions**  
**DE 50—Currency Code, Settlement**

---

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-3
Data Field:	Contents of positions 1–3
Subfields:	N/A
Justification:	N/A

**Usage**

Following is the usage of DE 50 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Request Response/0110	CE	X	C
Authorization Advice/0120—Acquirer-generated	•	X	C
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice Response/0130—System-generated	•	X	C
Reversal Request/0400	•	X	C
Reversal Request Response/0410	CE	X	C
Reversal Advice/0420	•	C	C
Reversal Advice Response/0430	CE	CE	•

**Values**

All currency codes must be selected from the numeric ISO standard currency codes. ISO standard currency codes identify DE 50. A list of valid values is in the *Quick Reference Booklet*.

**Application Notes**

This data element is defined and used identically within all MasterCard programs and services.

As of the date of this publication, all MasterCard programs and services use U.S. dollars (840) as the currency of settlement for programs and services that the Authorization Platform supports.

The Authorization Platform includes this data element if the customer chooses to receive settlement amount-related data elements.

This data will be present, as defined, except when the Authorization Platform has declined an Authorization Request/0100 message and was unable to complete currency conversion processing.

## **DE 51—Currency Code, Cardholder Billing**

DE 51 (Currency Code, Cardholder Billing) defines the currency of DE 6 (Amount, Cardholder Billing) and DE 8 (Amount, Cardholder Billing Fee).

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-3
Data Field:	Contents of positions 1–3
Subfields:	N/A
Justification:	N/A

**Usage**

Following is the usage of DE 51 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	M
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	•	X	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	X	C
Reversal Request/0400	•	X	M

## Data Element Definitions

### DE 52—Personal ID Number (PIN) Data

Reversal Request Response/0410	C	X	C
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•

#### Values

All currency codes must be selected from the numeric ISO standard currency codes. ISO standard currency codes identify DE 51. A list of valid values is in the *Quick Reference Booklet*.

#### Application Notes

This data element is defined and used identically within all MasterCard programs and services.

This data will be present, as defined, except when the Authorization Platform has declined an Authorization Request/0100 message and was unable to complete currency conversion processing.

## DE 52—Personal ID Number (PIN) Data

DE 52 (Personal ID Number [PIN] Data) contains a number assigned to a cardholder intended to uniquely identify that cardholder at the point of interaction. The use of the PIN is subject to bilateral agreement. The data element may contain the PIN itself or a derivative. This data element transmits PIN information from acquirers to issuers (or to the network) for PIN verification or validation.

#### Attributes

Length of Length Field:	N/A
Data Representation:	b-8
Data Field:	Contents of bit positions 1-64 (8 bytes)
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of DE 52 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	X	C

#### Values

The network supports PINs from four to 12 characters long.

The encrypted PIN block always is eight bytes (64 bits) long regardless of the original PIN length.

CIS uses the Data Encryption Standard (DES) algorithm (ISO 9564-2) to translate PIN data. For purposes of PIN translation, DES requires that a 16-digit hexadecimal number and working key be provided. DE 52 houses the 16-digit number in the customer's PIN block format.

#### **Application Notes**

---

Because of strict security requirements implemented within the network environment, PINs are never transmitted "in the clear" as character data. In addition, PIN data is never included in Advice or Reversal messages. The primary reason for this is that PIN data is highly sensitive information that is never stored (even in encrypted form) as a permanent component of a transaction, for security reasons. The rules, bylaws, and procedures established for individual programs and services dictate the specific requirements for PIN usage.

This data element is supported for MasterCard transactions.

The Authorization Platform may perform PIN verification or validation services on behalf of customers that elect to use this optional service. Refer to the appropriate user manual and the *Security Rules and Procedures* manual to determine specific PIN verification/validation options that may be selected for individual MasterCard programs and services.

DE 52 is mandatory for all ATM transactions.

This data element is not applicable for UKDM transactions.

---

<b>IF...</b>	<b>THEN the Authorization Platform...</b>
An Authorization Request/0100 message contains DE 52 (PIN Data) and DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) is not 02, 05, 07, 80, 81, 82, 90, or 91	Rejects the message and forwards the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 052</li></ul>

## **DE 53—Security-Related Control Information**

DE 53 (Security-Related Control Information) is used with PIN data to provide specific information about PIN block encoding and PIN data encryption to assist the issuer (or its agent) in processing PINs entered at the point of interaction.

---

#### **Attributes**

---

Length of Length Field:	N/A
Data Representation:	n-16
Data Field:	Contents of subfields
Subfields:	6
Justification:	See "Subfields"

**Data Element Definitions**  
**DE 53—Security-Related Control Information**

---

**Usage**

Following is the usage of DE 53 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	X	C
Network Management Request/0800—Sign-On/Sign-Off	C	C	•

**Values**

See “Subfields.”

**For UK Domestic Maestro:** This data element is not applicable for UKDM transactions.

---

## Subfield 1—PIN Security Type Code

DE 53, subfield 1 (PIN Security Type Code) indicates the type of security processing used for the PIN data.

**Attributes**

Data Representation: n-2

Data Field: Contents of positions 1–2

Justification: N/A

**Values**

97 = Multiple (indexed) keys

---

## Subfield 2—PIN Encryption Type Code

DE 53, subfield 2 (PIN Encryption Type Code) indicates the type of security processing used for the PIN data.

**Attributes**

Data Representation: n-2

Data Field: Contents of positions 3–4

Justification: N/A

**Values**

01 = DES encryption

---

### **Subfield 3—PIN Block Format Code**

DE 53, subfield 3 (PIN Block Format Code) indicates the type of PIN block format used.

---

#### **Attributes**

---

Data Representation: n-2

---

Data Field: Contents of positions 5–6

---

Justification: N/A

---

#### **Values**

---

01 = ANSI 1

---

02 = ANSI 2

---

03 = ANSI 3

---

10 = ISO Format 0

---

11 = ISO Format 1

---

19 = ISO Format 0 or ISO Format 1

---

### **Subfield 4—PIN Key Index Number**

DE 53, subfield 4 (PIN Key Index Number) indicates the specific PIN key to be used when more than one key is available in a PIN key set.

---

#### **Attributes**

---

Data Representation: n-4

---

Data Field: Contents of positions 7–10

---

Justification: N/A

---

#### **Values**

---

0001–0099

---

### **Subfield 5—Reserved for Future Use**

DE 53, subfield 5 (Reserved) is reserved for future use.

---

#### **Attributes**

---

Data Representation: n-2

---

Data Field: Contents of positions 11–12

---

## Data Element Definitions

### DE 54—Additional Amounts

---

Justification: N/A

#### Values

Not used, default to zero.

### Subfield 6—Reserved for Future Use

DE 53, subfield 6 (Reserved) is reserved for future use.

---

#### Attributes

Data Representation: n-4

Data Field: Contents of positions 13–16

Justification: N/A

---

#### Values

Not used, default to zero.

## DE 54—Additional Amounts

DE 54 (Additional Amounts) provides information on up to two amount types and related account data.

---

#### Attributes

Length of Length Field: 3

Data Representation: an...120; LLLVAR

The “LLL” length field of LLLVAR must be an integral multiple of 20, not to exceed 120.

Data Field: Contents of subfields 1–4

Subfields: 4

Justification: See “Subfields”

---

#### Usage

Following is the usage of DE 54 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	X	C
Authorization Request Response/0110	C	X	C
Authorization Advice/0120—System-generated	•	C	C

Authorization Advice/0120—Acquirer-generated	C	X	C
Authorization Advice/0120—Issuer-generated	•	C	C
Reversal Request/0400	C	X	C
Reversal Advice/0420	•	C	C

**Values**

See “Subfields”

**Application Notes**

An “occurrence” is defined as one set of the four DE 54 subfields. Depending on the conditions of the message, DE 54 can be sent by the acquirer, issuer, or the Authorization Platform.

Currently, Authorization Platform programs and services do not use more than two “additional amounts” amount types within a single Authorization Platform message. The message initiator can send only two occurrences of the DE 54 subfields in a message. One occurrence is the first amount type in the message initiator’s currency. The other occurrence is the second amount type in the message initiator’s currency. The Authorization Platform will then provide an additional occurrence of each amount type to the message recipient in the message recipient’s currency. Therefore, the message recipient can receive a maximum of four occurrences of the DE 54 subfields. Each amount type will have two occurrences, one in the message initiator’s currency, and one in the message recipient’s currency.

When the Authorization Request Response/0110 message contains DE 39, value 10 (Partial Approval) or 87 (Purchase Amount Only, No Cash Back Allowed), the issuer can send only one occurrence of the DE 54 subfields in the issuer’s currency that is not equal to DE 54, subfield 2 value 57 (Original Amount). The Authorization Platform will provide two occurrences of the amount type sent by the issuer to the acquirer, one in the acquirer’s currency, and one in the issuer’s currency. The Authorization Platform also will provide two occurrences of the DE 54 subfields where DE 54, subfield 2 is 57 and DE 54, subfield 4 is C plus the 12-digit original amount. One occurrence will be in the acquirer’s currency and one occurrence will be in the issuer’s currency.

**Partial Approvals**

The Authorization Request Response/0110 message contains DE 54, subfield 2, value 57 only if the acquirer can process partial approvals and if the issuer is approving part of the total transaction amount. If the issuer approves the entire transaction amount, DE 54 will not be present in the Authorization Request Response/0110.

**Purchase with Cash Back**

Issuers are not required to return DE 54 in Purchase with Cash Back Authorization Request Response/0110 messages. If DE 54 is returned by the issuer, it will be dropped before the response is forwarded to an acquirer. The Authorization Request Response/0110 message contains only DE 54, subfield 2, value 40 in an Authorization Request Response/0110 message when transaction is processed by X-Code or declined by MasterCard with a format error condition (DE 39 = 30).

**Cash Back without Purchase in India**

## Data Element Definitions

### DE 54—Additional Amounts

---

Cash Back without Purchase is supported for India intracountry transactions and is identified in the Authorization Request/0100 messages containing DE 3, subfield 1, value 09 with the presence of DE 54, subfield 2, value 40. For Cash Back without Purchase transactions, DE 54 must be present and equal the same amount in DE 4.

---

#### Real-time Substantiation

---

The Authorization Request/0100 or Authorization Advice/0120 messages contain DE 54, subfield 2, value 10 or 11 to indicate the healthcare and prescription amounts. DE 54, subfield 2, value 10 and 11 are sent only to the issuers that participate in Real-time Substantiation.

---

#### Purchase of Goods or Services with Cash Back

---

Refer to [Programs and Service Requirements, Purchase of Goods or Services with Cash Back, Authorization Platform Edits](#).

---

## Subfield 1—Account Type

DE 54, subfield 1 (Account Type) contains the two-digit code as defined in DE 3 (Processing Code), subfield 2 (Cardholder “From Account” Type Code) or subfield 3 (Cardholder “To Account” Type Code).

---

#### Attributes

---

Data Representation: n-2

---

Data Field: Contents of positions 1–2

---

Justification: N/A

---

#### Values

---

The valid values for this field are the same values as defined for DE 3 (Processing Code), subfield 2 (Cardholder “From Account” Type Code).

---

## Subfield 2—Amount Type

DE 54, subfield 2 (Amount Type) indicates the type of amount applied.

---

#### Attributes

---

Data Representation: n-2

---

Data Field: Contents of positions 3–4

---

Justification: N/A

---

#### Values

---

01 = Ledger Balance

---

02 = Available Balance

---

03	=	Amount Owing
04	=	Amount Due
10	=	Healthcare Eligibility Amount
11	=	Prescription Eligibility Amount
12	=	Reserved for future use
13	=	Reserved for future use
14	=	Reserved for future use
17	=	MasterCard Prepaid Online Bill Pay Transaction Fee Amount
40	=	Amount Cash Back
57	=	Original Amount

### Subfield 3—Currency Code

DE 54, subfield 3 (Currency Code) is a three-digit code that must contain a valid numeric code.

---

#### Attributes

---

Data Representation: n-3

---

Data Field: Contents of positions 5–7

---

Justification: Right

---

#### Values

---

Please refer to the *Quick Reference Booklet*.

---

### Subfield 4—Amount

DE 54, subfield 4 (Amount) indicates the amount is a credit or debit amount.

---

#### Attributes

---

Data Representation: an-13

---

Data Field: Contents of positions 8–20

---

Justification: Right

---

#### Values

---

C = (credit amount) plus 12 digits

---

D = (debit amount) plus 12 digits

---

## Data Element Definitions

### DE 55—Integrated Circuit Card (ICC) System-Related Data

---

## DE 55—Integrated Circuit Card (ICC) System-Related Data

DE 55 (Integrated Circuit Card [ICC] System-Related Data) contains binary data that only the issuer or the issuer agent processes; it is used locally by the payment application on the chip at a chip-capable terminal. This data element is present in chip full-grade transactions.

---

### Attributes

---

Length of Length Field:	3
Data Representation:	b...255; LLLVAR The “LLL” length field of LLLVAR
Data Field:	Contents of subelements
Subelements:	Number of subelements depend on message type
Justification:	N/A

---

### Usage

---

Following is the usage of DE 55 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	O
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•

---

### Values

---

See “Subelements”.

---

### Application Notes

---

For ICC information, refer to *M/Chip Requirements*

See DE 55, Authorization Platform Edits, that describe the edits performed on this data element.

**For UK Domestic Maestro:** DE 55 must be present for all Chip Full Grade transactions where DE 22 (POS Entry Mode) contains value 05x or 07x.

---

## DE 55—Subelement Encoding Scheme

DE 55 contains chip data formatted in accordance with EMV specifications. EMV uses Basic Encoding Rules (BER). Reference the EMV specification for details regarding coding of BER-ID, length, value (TLV) data objects. The chip data in DE 55 consists of a series of subelements in a “ID-length-data” format.

<b>Position(s)</b>	<b>Description</b>
1–3	DE 55 Total Length
4 or 4–5	First subelement ID, in binary representation; the length is either one or two positions depending on the definition of the subelement ID in the EMV specification.
5 or 5–6	First subelement length; the value of the “length” subelement is always one; position depends on the subelement ID length.
6–xxx or 7–xxx	First subelement variable length data; the starting position depends on the subelement ID length.
	Positions of the subelement length and variable length data depend on the subelements used. Subelement ID, Length, and Variable Length Data may be repeated as needed until all chip data has been presented.

## DE 55—Subelements

The following table lists the required and optional subelements in Authorization Request/0100 and Authorization Request Response/0110 messages that contain chip data.

<b>Subelement Description</b>	<b>Tag Value</b>	<b>Component<sup>10</sup></b>	<b>Each Component Length<sup>11</sup></b>	<b>Total Subelement Length<sup>12</sup></b>
<b>Required Subelements in Authorization Request/0100</b>				
Application Cryptogram (AC)	9F26	ID	2	11
		length	1	
		data	8	
Cryptogram Information Data	9F27	ID	2	4
		length	1	
		data	1	
Issuer Application Data (IAD)	9F10	ID	2	4–35

- 10. The hexadecimal representation is given here. Every two positions of hexadecimal data is one byte of binary data.
- 11. Lengths are in binary format.
- 12. The “Total Subelement Length” is the sum of the subelement’s ID, length, and data subfields.

**Data Element Definitions****DE 55—Integrated Circuit Card (ICC) System-Related Data**

<b>Subelement Description</b>	<b>Tag Value</b>		<b>Each Component<sup>10</sup></b>	<b>Total Subelement Length<sup>12</sup></b>
(Mandatory if the corresponding data object [EMV tag 9F10] is provided by the card to the terminal)			length	1
			data	1–32
Unpredictable Number	9F37		ID	2
			length	1
			data	4
Application Transaction Counter	9F36		ID	2
			length	1
			data	2
Terminal Verification Result (TVR)	95		ID	1
			length	1
			data	5
Transaction Date	9A		ID	1
			length	1
			data	3
Transaction Type	9C		ID	1
			length	1
			data	1
Amount Authorized	9F02		ID	2
			length	1
			data	6
Transaction Currency Code	5F2A		ID	2
			length	1
			data	2
Application Interchange Profile	82		ID	1
			length	1
			data	2
Terminal Country Code	9F1A		ID	2
			length	1

**Data Element Definitions**  
**DE 55—Integrated Circuit Card (ICC) System-Related Data**

---

<b>Subelement Description</b>	<b>Tag Value</b>	<b>Component<sup>10</sup></b>	<b>Each Component Length<sup>11</sup></b>	<b>Total Subelement Length<sup>12</sup></b>
		data	2	

**Optional Subelements in Authorization Request/0100**

---

When DE 55 is present in the Authorization Request/0100 message, the following subelements are optional in DE 55:

Cardholder Verification Method (CVM) Results	9F34	ID	2	6
		length	1	
		data	3	

The presence of 9F34 is mandatory for all authorization messages containing DE 55 that are transmitted from acquirer chip systems certified by MasterCard on or after 13 April 2012. The presence of 9F34 is mandatory for all authorization messages containing DE 55 effective 1 April 2017.

Terminal Capabilities	9F33	ID	2	6
		length	1	
		data	3	
Terminal Type	9F35	ID	2	4
		length	1	
		data	1	
Interface Device (IFD) Serial Number	9F1E	ID	2	11
		length	1	
		data	8	
Transaction Category Code	9F53	ID	2	4
		length	1	
		data	1	
Dedicated File Name	84	ID	1	7–18
		length	1	
		data	5–16	
Application Version Number	9F09	ID	2	5
		length	1	
		data	2	
Transaction Sequence Counter	9F41	ID	2	5–7
		length	1	

## Data Element Definitions

### DE 55—Integrated Circuit Card (ICC) System-Related Data

Subelement Description	Tag Value	Component <sup>10</sup>	Each Component Length <sup>11</sup>	Total Subelement Length <sup>12</sup>
		data	2–4	
Amount Other	9F03	ID	2	9
		length	1	
		data	6	

When cash back is not permitted by product rules, 9F03 may be absent, or present with a zero value.

When cash back is permitted by product rules:

- and there is a cash back amount, 9F03 carries the amount and presence is mandatory
- and there is no cash back amount, the value of 9F03 is zero. 9F03 may be absent, or present with a zero value.

#### Optional Subelements in Authorization Request Response/0110

For Authorization Request Response/0110 messages related to chip full-grade transactions and response messages related to e-commerce transactions with EMV-compliant ICC data, issuers may provide DE 55, including the following subelements: if any of these subfields are present in the Authorization Request Response/0110 message, the acquirer must pass the subelements, unaltered, to the IC card.

Issuer Authentication Data (Provides data to be transmitted to the card for issuer authentication.)	91	ID	1	10–18
		length	1	
		data	8–16	
Issuer Script Template 1 and 2 (Allows the issuer to provide a post-issuance command for transmission to the card. Present if issuer sends commands to ICC; acquirer network must support a minimum of 25 bytes and a maximum of 129 bytes.)	71 and 72	ID	1	3–129
		length	1	
		data	1–127	
Issuers may send more than one instance (maximum of 10 instances or maximum length of DE 55) of subelement 71 and subelement 72 in the Authorization Request Response/0110.				

## DE 55—Authorization Platform Edits

The Authorization Platform performs the following edits.

If MasterCard determines through its Internal Chip Monitoring process that improperly formatted chip transactions are being submitted from acquirers not certified to send chip transactions, MasterCard will notify each acquirer before

activating an edit. The Authorization Platform will perform the following edits on the Authorization Request/0100 message.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 22, subfield 1 contains value 05 or 07 and DE 55 is present and Acquirer Chip Testing Level associated with the acquirer indicates the acquirer is approved for partial grade chip transactions	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 055</li> </ul>
DE 22, subfield 1 contains value 05 and DE 55 is not present and Acquirer Chip Testing Level associated with the acquirer indicates the acquirer is approved to send full grade chip transactions	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 055</li> </ul>
DE 22, subfield 1 contains value 07 and DE 55 is not present and Acquirer Chip Testing Level associated with the acquirer indicates the acquirer is approved to send full grade chip transactions	Sends the acquirer an Authorization Request Response/0110 where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 055</li> </ul>
<b>IF...</b>	<b>THEN...</b>
DE 55 is present in the Authorization Request/0100 message or the Authorization Advice/0120 message,	DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 must be 05, 07, or 81 or the Authorization Platform rejects the Authorization Request/0100 message or Authorization Advice/0120 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 055</li> </ul>
DE 55 is not present in the Authorization Request/0100 message for a Chip PIN Management transaction	The Authorization Platform sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 055</li> </ul>

## Data Element Definitions

### DE 56—Reserved for ISO Use

---

The Authorization Platform will perform the following edits on an Authorization Request Response/0110 message.

WHEN...	THEN the Authorization Platform...
DE 55 is echoed in the Authorization Request Response/0110 message	Sends the issuer an Authorization Response Negative Acknowledgement/0190 message where: <ul style="list-style-type: none"><li>• DE 39 = 30 (Format error)</li><li>• DE 44 = 055</li></ul>
<b>WHEN the issuer...</b>	<b>THEN the Authorization Platform...</b>
Sends an Authorization Request Response/0110 message where DE 55, subelement 72 is present and exceeds 127 bytes in length	Sends an Authorization Response Negative Acknowledgement/0190 message to the issuer where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 055</li></ul>
Sends an Authorization Request Response/0110 message where DE 55, subelement 71 is present and exceeds 127 bytes in length	Sends an Authorization Response Negative Acknowledgement/0190 message to the issuer where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 055</li></ul>
<b>IF...</b>	<b>THEN the Authorization Platform...</b>
DE 55 is present in the Authorization Request Response/0110 and DE 55 was not present in the original Authorization Request/0100	Sends an Authorization Response Negative Acknowledgement/0190 message to the issuer where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 055</li></ul>

### DE 56—Reserved for ISO Use

DE 56 (Reserved for ISO Use) is reserved for future use.

---

#### Attributes

---

Length of Length Field:	3
Data Representation:	ans...999; LLLVAR
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

**Usage**

The Authorization Platform currently does not use this data element.

**DE 57–DE 59—Reserved for National Use**

DE 57–DE 59 are reserved for future use.

**Attributes**

Length of Length Field:	3
-------------------------	---

Data Representation:	ans...999; LLLVAR
----------------------	-------------------

Data Field:	N/A
-------------	-----

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

**Usage**

The Authorization Platform currently does not use this data element.

**Values**

N/A
-----

**DE 60—Advice Reason Code**

DE 60 (Advice Reason Code) indicates to the receiver of an Advice message the specific reason for the transmission of the Advice message.

**Attributes**

Length of Length Field:	3
-------------------------	---

Data Representation:	ISO: ans...999; LLLVAR MasterCard: ans...060; LLLVAR
----------------------	---

Data Field:	Contents of subfields
-------------	-----------------------

Subfields:	3
------------	---

Justification:	See “Subfields”
----------------	-----------------

**Usage**

Following is the usage of DE 60 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Org	Sys	Dst
-----	-----	-----

Authorization Advice/0120—Acquirer-generated	M	•	M
--	---	---	---

## Data Element Definitions

### DE 60—Advice Reason Code

Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Reversal Advice/0420	•	M	M
Administrative Request/0600	M	•	M
Administrative Request Response/0610	ME	•	ME
Administrative Advice/0620	•	M	M
<b>Values</b>			
See “Subfields”			
<b>Application Notes</b>			
Not all Advice Reason Codes may be used within all programs and services.			

### Subfield 1—Advice Reason Code

Subfield 1 (Advice Reason Code) is mandatory for all Advice messages and indicates the general category of (or “reason” for) the Advice message. Advice reason code values are listed by message type identifier (MTI) and by program or service.

#### Attributes

Data Representation:	n-3
Data Field:	Contents of positions 1–3
Justification:	N/A

#### Values

See Advice Reason Codes listed by MTI.

### DE 60, Subfield 1 Values, in Authorization Advice/0120

The following values are valid in Authorization Advice/0120 messages.

Code	Description	MC	NP	VI	TE	MS	CI
100	Alternate Issuer Route: Issuer selected option <sup>13</sup>	✓	✓	✓		✓	✓
101	Alternate Issuer Route: IPS signed out	✓	✓	✓		✓	✓
102	Alternate Issuer Route: IPS timed out	✓	✓	✓		✓	✓

13. This secondary route is to either the Stand-In System or the optional alternate route.

**Data Element Definitions**
**DE 60—Advice Reason Code**

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
103	Alternate Issuer Route: IPS unavailable <sup>11</sup>	✓	✓	✓		✓	✓
104	Transaction processed via Limit-1	✓	✓	✓		✓	✓
105	Transaction processed via X-Code	✓	✓	✓			
106	Transaction processed via Limit-1 at the MIP	✓	✓	✓		✓	✓
107	PIN processing error	✓				✓	✓
108	Alternate Issuer Route: MIP Error <sup>11</sup>	✓	✓	✓		✓	✓
109	Alternate Issuer Route: Issuer Edit Response Error <sup>11</sup>	✓	✓	✓		✓	✓
111	Alternate Issuer Route: Issuer Host System Error <sup>11</sup>	✓	✓	✓		✓	✓
112	Alternate Route: Network Not Dispatched Error <sup>11</sup>	✓	✓	✓		✓	✓
113	Alternate Route: Issuer Undelivered <sup>11</sup>	✓	✓	✓		✓	✓
114	Alternate Route: Direct Down Option	✓	✓	✓		✓	✓
115	Transaction Processed via On-behalf Service Decision	✓				✓	✓
116	Invalid Merchant		✓				
120	Reserved for Future Use						
121	Account Lookup Service	✓	✓			✓	
126	Pay with Rewards Processing Advice to Issuer	✓					
140	Unable to convert <i>PayPass</i> or virtual account number	✓				✓	
190	Acquirer Processing System (APS) Approved	✓	✓	✓		✓	✓
191	Acquirer Processing System (APS) Completed Authorization Transaction	✓	✓		✓	✓	
200	inControl Processing Advice to Issuer		✓				
650	Administrative textual message transmittal (reference applicable user manual for Administrative message delivery capabilities within each program and service)	✓	✓	✓		✓	✓

**DE 60, Authorization Advice/0120 Edits**

The Authorization Platform performs the following edit on Authorization Advice/0120—Acquirer-generated messages.

**Data Element Definitions**  
**DE 60—Advice Reason Code**

---

<b>IF..</b>	<b>THEN the Authorization Platform...</b>
DE 60 is not 190 (Acquirer Processing System (APS) Approved) or 191 (Acquirer Processing System (APS) Completed Authorization Transaction)	Sends the issuer an Authorization Advice Response/0130 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 060</li> </ul>

**DE 60, Subfield 1 Values, in Reversal Advice/0420**

The following values are valid in Reversal Advice/0420 messages.

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
400	Banknet advice: APS error; unable to deliver response	√	√	√	√	√	√
401	Banknet advice: APS error; no APS Authorization Acknowledgement/0180 or Financial Transaction Acknowledgement/0280	√	√	√		√	√
402	Issuer Time-out	√	√	√		√	√
403	Issuer Signed-out	√	√	√		√	√
409	Issuer Response Error	√	√	√		√	√
410	Reversal message provided by a system other than Banknet	√				√	√
413	Issuer Undelivered	√	√	√		√	√

**DE 60, Subfield 1 Values, in Administrative Request/0600**

Following are the valid values in Administrative Request/0600 messages.

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
650	Administrative message containing customer application and account data	√		√			

**DE 60, Subfield 1 Values, in Administrative Request Response/0610**

Following are valid values in Administrative Request Response/0610 messages.

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
650	Administrative message containing customer application and account data	√		√			

**DE 60, Subfield 1 Values, in Administrative Advice/0620**

Following are valid values in Administrative Advice/0620 messages.

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
600	Message unreadable or indecipherable or contains invalid data. Subfield 2 (Advice Detail Code) may contain the bit map number of the data element where message scanning was aborted)	✓	✓	✓	✓	✓	✓
650	Administrative textual message transmittal (reference applicable user manual for Administrative message delivery capabilities within each program and service)	✓	✓	✓		✓	✓

**Subfield 2—Advice Detail Code**

DE 60, subfield 2 (Advice Detail Code) is optional, depending on the primary Advice Reason Code; if used, it provides additional (specific) information as to the exact nature of the Advice message. Advice Detail Codes are determined individually for each program and service. The Advice Detail Codes for MasterCard activity appear below. Refer to the appropriate documentation for information on codes for non-MasterCard activity.

**Attributes**

Data Representation: n-4

Data Field: Contents of positions 4-7

Justification: N/A

**Values**

0000 Accept

0001 Reject: negative file

0002 Reject: capture card

0003 Reject: issuer not participating

0004 Reject: invalid PIN

0005 Reject: ATM

0006 Reject: transaction limit test

0041 Reject: Recurring Payment Cancellation Service

## Data Element Definitions

### DE 60—Advice Reason Code

---

#### DE 60, Subfield 2 Values, in Authorization Advice/0120—Issuer-generated

The following values are valid in Authorization Advice/0120-Issuer-generated messages.

Code	Description
0030	Accept: Member-generated Authorization Advice/0120 sent to the RiskFinder scoring server. (Used with Advice Reason Code 650.)

#### DE 60, Subfield 2 Values, in Authorization Advice/0120—System-generated

The following values are valid in Authorization Advice/0120—System-generated messages.

Values
Reason codes 0007–1611 apply only to the Authorization Advice/0120—System-generated message.
0007        Reject: Premium listing cumulative limit test
0008        Reject: merchant suspicious indicator test
0009        Reserved
0010        Reserved
0011        Reject: day number 1/number of transactions
0012        Reject: day number 2/number of transactions
0013        Reject: day number 3/number of transactions
0014        Reject: day number 4/number of transactions
0015        Reject: day number 1/amount
0016        Reject: day number 2/amount
0017        Reject: day number 3/amount
0018        Reject: day number 4/amount
0019        Reject: extended Cash Advance cumulative amount
0020        Reject: card number in blocked range
0021        Reject: Premium Listing transaction limit test
0028        Reject: invalid CVC 1
0029        Reject: expired card

**Values**

0031	Reject: unable to decrypt/encrypt PIN data. (Used with Advice Reason Code 107)
0036	Reject: CVC 1 Unable to process

**DE 60, Subfield 2 Values, in Administrative Advice/0620**

Following are the valid values in Administrative Advice/0620 messages.

**Code      Description**

0029	MIP-generated RiskFinder Advice transactions
0030	Member-generated RiskFinder Advice transactions

**DE 60, Subfield 2 Values, in Customer Service Messages**

Following are the valid values in Customer Service messages.

**Code      Description**

0080	Consumer application request
0081	Consumer application status inquiry
0082	Consumer user lookup inquiry
0083	Consumer account lookup inquiry
0084	Consumer account maintenance request
0085	Consumer counteroffer reply
0086	Consumer preapproved offer inquiry
0090	Business application request
0091	Business application status inquiry
0092	Business user lookup inquiry
0093	Business account lookup inquiry
0094	Business account maintenance request
0095	Business counteroffer reply
0096	Business pre-approved offer inquiry

**DE 60, Subfield 2 Values, in CVC 3 Validation**

Following are valid values in CVC 3 Validation transactions.

## Data Element Definitions

### DE 60—Advice Reason Code

---

Code	Description
0042	Reject: CVC 3 Unable to process
0043	Reject: CVC 3 ATC outside allowed range
0044	Reject: CVC 3 Invalid
0045	Reject: CVC 3 Unpredictable number mismatch
0046	Reject: CVC 3 ATC Replay

### DE 60, Subfield 2 Values, in MasterCard inControl Service

Following are valid values in MasterCard inControl Service transactions.

Code	Description
0060	Reject: Virtual Card Number (expiration date does not match)
0061	Reject: Virtual Card Number (expiration date expired)
0062	Reject: Virtual CVC 2 does not match
0063	Reject: Validity Period Limit: inControl
0064	Reject: Transaction Amount Limit Check
0065	Reject: Cumulative Amount Limit Check
0066	Reject: Transaction Number Usage
0067	Reject: Merchant ID Limit
0068	Reject: Invalid Virtual Card Number–Real Card Number Mapping Relationship
0069	Reject: MCC Limit
0070	Reject: Database Status Bad
0071	Reject: Decline Other
0072	Reject: Geographic Restriction
0073	Reject: Transaction Type Restriction
0075	Reject: Transaction Time/Date Restriction

### DE 60, Subfield 2 Values, in M/Chip On-Behalf Services

Following are valid values in M/Chip On-Behalf Services transactions.

<b>Code</b>	<b>Description</b>
0032	Reject: Chip technical failure
0033	Reject: Incorrect chip data
0034	Reject: Chip validation failed
0035	Reject: TVR/CVR validation failed
0039	Reject: Cryptogram not ARQC

**DE 60, Subfield 2 Values, in Pay with Rewards**

Following are valid values in MasterCard Pay with Rewards service.

<b>Code</b>	<b>Description</b>
0120	Reject: Pay with Rewards—Insufficient points balance
0121	Reject: Pay with Rewards—Redemption rule(s) failed
0122	Reject: Pay with Rewards service was not performed successfully
0123	Reject: Pay with Rewards—Account not registered
0124	Reject: Pay with Rewards System error

**DE 60, Subfield 2 Values, in PIN Validation**

Following are the valid values in PIN Validation transactions.

<b>Code</b>	<b>Description</b>
0050	Reject: Unable to Process
0051	Reject: Invalid PIN
0052	Reject: Mandatory PVV not on file
0052	Reject: PIN Retry Exceeded (invalid PIN)

**DE 60, Subfield 2 Values, in Private Label Processing**

Following are valid values in Private Label Processing transactions.

<b>Code</b>	<b>Description</b>
0116	Reject: Merchant not allowed for Private Label transaction

## Data Element Definitions

### DE 60—Advice Reason Code

---

#### **DE 60, Subfield 2 Values, in TCC, CAT Level, and Promotion Code in Failed Parameter Combinations (country-specific)**

Following are valid values in TCC, CAT Level, and Promotion Code in Failed Parameter Combinations (country-specific) transactions.

<b>Code</b>	<b>Description</b>
0300	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
0301	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
0310	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
0311	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

#### **DE 60, Subfield 2 Values, in TCC, CAT Level, and Promotion Code in Failed Parameter Combinations (global)**

Following are valid values in TCC, CAT Level, and Promotion Code in Failed Parameter Combinations (global) transactions.

<b>Code</b>	<b>Description</b>
0400	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
0401	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
0410	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
0411	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

## **DE 60, Subfield 2 Values, in MCC, CAT Level, and Promotion Code in Failed Parameter Combinations (country-specific)**

Following are valid values for MCC, CAT Level, and Promotion Code in Failed Parameter Combinations (country-specific) transactions.

<b>Code</b>	<b>Description</b>
0100	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
0101	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
0110	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
0111	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

## **DE 60, Subfield 2 Values, in MCC and Promotion Code in Failed Parameter Combinations (country-specific)**

Following are valid values in MCC and Promotion Code in Failed Parameter Combinations (country-specific) transactions.

<b>Code</b>	<b>Description</b>
0500	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
0501	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
0510	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
0511	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

**DE 60, Subfield 2 Values, in MCC and Promotion Code in Failed Parameter Combinations (global)**

Following are valid values in MCC and Promotion Code in Failed Parameter Combinations (global) transactions.

<b>Code</b>	<b>Description</b>
0600	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
0601	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
0610	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
0611	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

**DE 60, Subfield 2 Values, in TCC and Promotion Code in Failed Parameter Combinations (country-specific)**

Following are valid values in TCC and Promotion Code in Failed Parameter Combinations (country-specific) transactions.

<b>Code</b>	<b>Description</b>
0700	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
0701	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
0710	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
0711	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

## **DE 60, Subfield 2 Values, in TCC and Promotion Code in Failed Parameter Combinations (global)**

Following are valid values in TCC and Promotion Code in Failed Parameter Combinations (global) transactions.

<b>Code</b>	<b>Description</b>
0800	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
0801	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
0810	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
0811	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

## **DE 60, Subfield 2 Values, in MCC and CAT Level in Failed Parameter Combinations (country-specific)**

Following are valid values in MCC and CAT Level in Failed Parameter Combinations (country-specific) transactions.

<b>Code</b>	<b>Description</b>
0900	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
0901	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
0910	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
0911	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

## Data Element Definitions

### DE 60—Advice Reason Code

---

#### **DE 60, Subfield 2 Values, in MCC and CAT Level in Failed Parameter Combinations (global)**

Following are valid values in MCC and CAT Level in Failed Parameter Combinations (global) transactions.

<b>Code</b>	<b>Description</b>
1000	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
1001	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
1010	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
1011	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

#### **DE 60, Subfield 2 Values, in TCC and CAT Level in Failed Parameter Combinations (country-specific)**

Following are valid values in TCC and CAT Level in Failed Parameter Combinations (country-specific) transactions.

<b>Code</b>	<b>Description</b>
1100	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
1101	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
1110	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
1111	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

## DE 60, Subfield 2 Values, in TCC and CAT Level in Failed Parameter Combinations (global)

Following are valid values in TCC and CAT Level in Failed Parameter Combinations (global) transactions.

<b>Code</b>	<b>Description</b>
1200	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
1201	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
1210	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
1211	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

## DE 60, Subfield 2 Values, in MCC in Failed Parameter Combinations (country-specific)

Following are valid values in MCC in Failed Parameter Combinations (country-specific) transactions.

<b>Code</b>	<b>Description</b>
1300	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
1301	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
1310	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
1311	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

**DE 60, Subfield 2 Values, in MCC in Failed Parameter Combinations (global)**

Following are valid values in MCC in Failed Parameter Combinations (global) transactions.

<b>Code</b>	<b>Description</b>
1400	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
1401	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
1410	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
1411	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

**DE 60, Subfield 2 Values, in TCC in Failed Parameter Combinations (country-specific)**

Following are valid values in TCC in Failed Parameter Combinations (country-specific) transactions.

<b>Code</b>	<b>Description</b>
1500	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
1501	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
1510	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
1511	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

## DE 60, Subfield 2 Values, in TCC in Failed Parameter Combinations (global)

Following are valid values in TCC in Failed Parameter Combinations (global) transactions.

<b>Code</b>	<b>Description</b>
1600	Reject: transaction limit test MasterCard default limits caused transaction to fail; card present at point of interaction
1601	Reject: transaction limit test MasterCard default limits caused transaction to fail; card not present at point of interaction
1610	Reject: transaction limit test Member-defined limits caused transaction to fail; card present at point of interaction
1611	Reject: transaction limit test Member-defined limits caused transaction to fail; card not present at point of interaction

## DE 60, Subfield 2 Values, in Miscellaneous Processing

Following are valid values in miscellaneous processing transactions.

<b>Code</b>	<b>Description</b>
1700	Accept: via X-Code processing
1701	Reject: via X-Code processing
1702	Reject: capture card via X-Code processing
1900	Accept: via Limit-1 at the MIP
1901	Reject: via Limit-1 at the MIP
1902	Reject: capture card via Limit-1 at the MIP
2000	Reject: PIN data present in Authorization Request/0100 message (used in conjunction with Reversal Advice/0420 message)
9999	Reject: failed validation test because transaction type or authorization method was invalid

### **Subfield 3—Advice Detail Text**

Subfield 3 (Advice Detail Text) is optional and may be used to contain textual information supplementary to the Advice Detail Code. Advice Detail Text data is determined individually for each program and service. Refer to the appropriate user manual for information on Advice message text.

---

#### **Attributes**

---

Data Representation: ans...53

---

Data Field: Contents of positions 8–60

---

Justification: Left

---

#### **Values**

---

Advice message text

---

## **DE 61—Point-of-Service (POS) Data**

DE 61 (Point-of-Service [POS] Data) supersedes and replaces the ISO-specified DE 25 (Point-of-Service [POS] Condition Code) that customers must not use in the Authorization Request/0100. DE 61 indicates the conditions that exist at the point of service at the time of the transaction.

---

#### **Attributes**

---

Length of Length Field: 3

---

Data Representation: ISO: ans...999; LLLVAR  
MasterCard: ans...026; LLLVAR

---

Data Field: Contents of subfields

---

Subfields: 14

---

Justification: See “Subfields”

---

#### **Usage**

---

Following is the usage of DE 61 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	M	•	M
Authorization Advice/0120—Acquirer-generated	M	•	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Reversal Request/0400	M	•	M

---

**Values**

---

See “Subfields”.

Three basic categories of data include:

- POS Condition Code: Indicating POS terminal data (mandatory) in subfields 1–11
  - POS Authorization Life Cycle: Indicating the transaction is a pre-authorization request and the specific amount of days for which the pre-authorization will remain valid (the number of days the issuer or its agent will guarantee or hold funds) in subfield 12
  - POS geographic reference: Indicating the specific merchant location of the transaction in subfields 13–14
- 

**Application Notes**

---

This data element will be edited as described in the [Authorization Platform Edits](#).

---

## **Subfield 1—POS Terminal Attendance**

DE 61, subfield 1 (POS Terminal Attendance) indicates if the card acceptor is attending the terminal.

---

**Attributes**

---

Data Representation: n-1

---

Data Field: Contents of position 1

---

Justification: N/A

---

**Values**

---

0 = Attended Terminal

---

1 = Unattended terminal (cardholder-activated terminal [CAT], home PC, mobile phone, PDA)

---

2 = No terminal used (voice/audio response unit [ARU] authorization)

---

## **Subfield 2—Reserved for Future Use**

DE 61, subfield 2 (Reserved) is reserved.

---

**Attributes**

---

Data Representation: n-1

---

Data Field: Contents of position 2

---

Justification: N/A

---

**Data Element Definitions**  
**DE 61—Point-of-Service (POS) Data**

---

---

**Values**

---

Zero-filled

---

### **Subfield 3—POS Terminal Location**

DE 61, subfield 3 (POS Terminal Location) indicates the terminal location.

---

**Attributes**

---

Data Representation: n-1

---

Data Field: Contents of position 3

---

Justification: N/A

---

**Values**

---

0 = On premises of card acceptor facility

---

1 = Off premises of card acceptor facility (merchant terminal—remote location)

---

2 = Off premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA)

---

3 = No terminal used (voice/ARU authorization)

---

### **Subfield 4—POS Cardholder Presence**

DE 61, subfield 4 (POS Cardholder Presence) indicates whether the cardholder is present at the point of service and explains the condition if the cardholder is not present.

---

**Attributes**

---

Data Representation: an-1

---

Data Field: Contents of position 4

---

Justification: N/A

---

**Values**

---

0 = Cardholder present

---

1 = Cardholder not present, unspecified

---

2 = Mail/facsimile order

---

3 = Phone/ARU order

---

4	=	Standing order/recurring transactions
5	=	Electronic order (home PC, Internet, mobile phone, PDA)

## **Subfield 5—POS Card Presence**

DE 61, subfield 5 (POS Card Presence) indicates if the card is present at the point of service.

---

### **Attributes**

---

Data Representation: n-1

---

Data Field: Contents of position 5

---

Justification: N/A

---

### **Values**

---

0 = Card present

---

1 = Card not present

---

## **Subfield 6—POS Card Capture Capabilities**

DE 61, subfield 6 (POS Card Capture Capabilities) indicates whether the terminal has card capture capabilities.

---

### **Attributes**

---

Data Representation: n-1

---

Data Field: Contents of position 6

---

Justification: N/A

---

### **Values**

---

0 = Terminal/operator has no card capture capability

---

1 = Terminal/operator has card capture capability

---

## **Subfield 7—POS Transaction Status**

DE 61, Subfield 7 (POS Transaction Status) indicates the purpose or status of the request.

---

### **Attributes**

---

Data Representation: n-1

---

**Data Element Definitions**  
**DE 61—Point-of-Service (POS) Data**

---

Data Field:	Contents of position 7
Justification:	N/A
<b>Values</b>	
0 =	Normal request (original presentment)
2 =	SecureCode Phone Order
3 =	ATM Installment Inquiry
4 =	Preauthorized request
6 =	ATC Update
8 =	Account Status Inquiry Service

### **Subfield 8—POS Transaction Security**

DE 61, subfield 8 (POS Transaction Security) indicates the card acceptor's security level.

<b>Attributes</b>	
Data Representation:	n-1
Data Field:	Contents of position 8
Justification:	N/A
<b>Values</b>	
0 =	No security concern
1 =	Suspected fraud (merchant suspicious—code 10)
2 =	ID verified

### **Subfield 9—Reserved for Future Use**

DE 61, Subfield 9 (Reserved) is reserved.

<b>Attributes</b>	
Data Representation:	n-1
Data Field:	Contents of position 9
Justification:	N/A
<b>Values</b>	
Zero-filled.	

## **Subfield 10—Cardholder-Activated Terminal Level**

DE 61, subfield 10 (Cardholder-Activated Terminal Level) indicates whether the cardholder activated the terminal with the use of the card and the CAT security level.

---

### **Attributes**

---

Data Representation: n-1

---

Data Field: Contents of position 10

---

Justification: N/A

---

### **Values**

---

0 = Not a CAT transaction

---

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

---

4 = Authorized Level 4 CAT: In-flight commerce

---

5 = Reserved

---

6 = Authorized Level 6 CAT: Electronic commerce

---

7 = Authorized Level 7 CAT: Transponder transaction

---

8 = Reserved for future use

---

## **Subfield 11—POS Card Data Terminal Input Capability Indicator**

DE 61, subfield 11 indicates the terminal capabilities for transferring the data on the card into the terminal.

---

### **Attributes**

---

Data Representation: n-1

---

Data Field: Contents of position 11

---

Justification: N/A

---

### **Values**

---

0 = Unknown or unspecified

---

1 = No terminal used (voice/ARU authorization); server

---

2 = Magnetic stripe reader only

---

**Data Element Definitions**  
**DE 61—Point-of-Service (POS) Data**

---

3	=	Contactless M/Chip (Proximity Chip) Terminal supports <i>PayPass</i> M/Chip and <i>PayPass</i> magstripe transactions. The terminal also may support other card input types, including contact transactions
4	=	Contactless Magnetic Stripe (Proximity Chip) only The terminal supports <i>PayPass</i> magstripe transactions. The terminal also may support other card input types, including contact transactions
5	=	EMV specification (compatible chip reader) and magnetic stripe reader. The terminal also may support contactless transactions; however contactless transactions should always be submitted with value 3 or 4.
6	=	Key entry only
7	=	Magnetic stripe reader and key entry
8	=	EMV specification (compatible chip reader), magnetic stripe reader and key entry. The terminal also may support contactless transactions; however contactless transactions should always be submitted with value 3 or 4.
9	=	EMV specification (compatible chip reader) only The terminal also may support contactless transactions; however contactless transactions should always be submitted with value 3 or 4.

---

**Application Notes**

DE 61, subfield 11 values 3, 4, 5, 8, and 9 can only be used if the terminal is chip certified by MasterCard.

This subfield 11 indicates the terminal data input capability and not how the terminal captured the card data. For example, values 5 and 8 may be submitted for a magnetic stripe transaction when the EMV capable terminal was not used to capture chip data. Acquirers should submit, and issuers should accept, value 3 when the terminal has *PayPass* contactless M/Chip capability.

Acquirers should submit, and issuers should accept, value 4 when the terminal has *PayPass* contactless magnetic stripe capability.

The PAN entry mode (DE 22 [Point-of-Service Entry Model], subfield 1 [POS Terminal PAN Entry Model]) may be any mode supported by the terminal.

Acquirers may also continue to pass the POS Card Data Terminal Capability indicator in DE 61, subfield 11 as they do today.

---

## Subfield 12—POS Authorization Life Cycle

DE 61, subfield 12 (POS Authorization Life Cycle) indicates the number of days pre-authorization will stay in effect; used for Visa Custom Payment Service automobile rentals and hotel reservations—otherwise it must contain zeros. When the Authorization Life Cycle subfield is not applicable to a message, it must be zero filled if POS Geographic Reference Data is required.

---

**Attributes**

---

Data Representation: n-2

---

Data Field: Contents of positions 12 and 13

---

Justification: Zero filled, right justified

---

**Values**

---

Zero fill or number of days.

---

## **Subfield 13—POS Country Code**

DE 61, subfield 13 (POS Country Code) indicates the country of the POS location (not the acquirer location) using ISO-specified codes.

---

**Attributes**

---

Data Representation: n-3

---

Data Field: Contents of positions 14–16

---

Justification: N/A

---

**Values**

---

Please refer to the *Quick Reference Booklet* for valid country codes.

---

## **Subfield 14—POS Postal Code**

DE 61, subfield 14 (POS Postal Code) indicates the geographic code of the POS (merchant) location (not the acquirer's location).

---

**Attributes**

---

Data Representation: ans...10

---

Data Field: Contents of positions 17–26

---

Justification: Left

---

**Values**

---

Postal code of merchant location. Must not be blank filled.

---

**Data Element Definitions**  
**DE 61—Point-of-Service (POS) Data**

---

---

**Application Notes**

---

This data is required for all MasterCard and Visa transactions.  
Subfield 14 must be present if postal codes are available in the acquiring country. However, subfield 14 may be omitted if the postal code does not exist in the acquiring country.  
Postal code data must be valid and accurate. Effective 12 October 2012, the content, format and presentation of postal code data must match in all authorization and clearing messages associated with a transaction.

---

## Authorization Platform Edits

The Authorization Platform performs the following edits on data element 61 (Point-of-Service [POS] Data).

### Authorization Request/0100 Character Edit

<b>WHEN the Acquirer...</b>	<b>THEN the Authorization Platform...</b>
Sends an Authorization Request/0100 message containing less than nine characters	Sends an Authorization Request Response/0110 message to the acquirer where: DE 39 = 30 DE 44 = 061
Sends an Authorization Request/0100 message where DE 61, subfields 1–9 contain a non-numeric character	Sends an Authorization Request Response/0110 message to the acquirer where: DE 39 = 30 DE 44 = 061

### Non-ATM CAT Level 1 Transactions

<b>WHEN the Authorization Request/0100 message contains...</b>	<b>THEN the Authorization Platform...</b>
DE 61, subfield 10, value 1 (Authorized Level 1 CAT: Automated dispensing machine with a PIN) and DE 52 (PIN Data) is not present and DE 55 (Integrated Circuit Card [ICC] System-related Data) is present	Forwards the Authorization Request/0100 message to the issuer.
DE 61, subfield 10, value 1 and DE 52 is present and DE 55 is present	Forwards the Authorization Request/0100 message to the issuer.

<b>WHEN the Authorization Request/0100 message contains...</b>	<b>THEN the Authorization Platform...</b>
DE 61, subfield 10, value 1 and DE 52 is present and DE 55 is not present	Forwards the Authorization Request/0100 message to the issuer.
DE 61, subfield 10, value 1 and DE 55 is not present and DE 52 is not present <b>MoneySend transactions with a CAT 1 are excluded from this edit.</b>	Sends an Authorization Request Response/0110 message to the acquirer where: DE 39 = 30 DE 44 = 052

### **Electronic Commerce Transactions**

<b>IF...</b>	<b>THEN...</b>	<b>Otherwise, the Authorization Platform...</b>
DE 48, subelement 42, position 3 is value 1, 2, or 3 and DE 61, subfield 4 is value 4 (Standing order/recurring transactions) or 5 (Electronic Order)	DE 61, subfield 7 must not contain value 2 (SecureCode Phone Order) and Subfield 10 must contain value 6 (Electronic commerce)	Rejects the authorization transaction with a format error indicated by: DE 39 = 30 DE 44 = 061

### **Phone Order Transactions**

<b>IF...</b>	<b>THEN...</b>	<b>Otherwise, the Authorization Platform...</b>
DE 48, subelement 42, position 3 is value 1 or 2	DE 61, subfield 4 must contain value 3 or 4 and Subfield 7 must contain value 2 (SecureCode phone order) and Subfield 10 must not contain value 6	Rejects the authorization transaction with a format error indicated by: DE 39 = 30 DE 44 = 061

## Data Element Definitions

### DE 62—Intermediate Network Facility (INF) Data

#### Account Status Inquiry Service

WHEN...	THEN the Authorization Platform...
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains value 8 (Account Status Inquiry Service) and DE 4 (Amount, Transaction) contains a value other than zero	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 004</li></ul>
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains value 8 (Account Status Inquiry Service) and DE 4 (Amount, Transaction) contains a value equal to zero and DE 3 (Processing Code) contains a value other than 00 (Purchase)	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 003</li></ul>

## DE 62—Intermediate Network Facility (INF) Data

DE 62 (Intermediate Network Facility [INF] Data), contains “acquiring network trace information” that INFs may require to quickly and accurately route Administrative Advice/0620 messages back to the original acquiring institution. DE 62 assists acquiring INF facilities that connect directly to the Authorization Platform. It allows these INFs to maintain sufficient information within a message to permit immediate online routing of chargebacks and retrieval requests without the requirement of maintaining large online reference databases containing the original transactions.

#### Attributes

Length of Length Field:	3
Data Representation:	ISO: ans...999; LLLVAR
	MasterCard: ans...100; LLLVAR
Data Field:	Contents of positions 1-100
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of DE 62 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	O	•	O

**Data Element Definitions**  
**DE 62—Intermediate Network Facility (INF) Data**

---

Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Acquirer-generated	O	•	O
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice Response/0130—Issuer-generated	CE	CE	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	•	CE
Authorization Advice Response/0130—System-generated	•	CE	CE
Reversal Request/0400	O	•	O
Reversal Request Response/0410	CE	•	CE
Reversal Advice/0420	•	C	C
Reversal Advice Response/0430	CE	CE	•
Administrative Request/0600	O	•	O
Administrative Request Response/0610	CE	•	CE
Administrative Advice/0620	•	C	C
Administrative Advice Response/0630	CE	CE	•

#### **Values**

---

DE 62 is a free-format, variable-length alphanumeric data element that may be used to store unique acquiring network ID codes, acquiring network chaining data, or other information useful to INFs in routing online chargebacks and retrieval requests.

#### **Application Notes**

---

DE 62 is an optional data element that customers may place in any originating Authorization Request/0100 or Authorization Advice/0120. Subsequently, this data element (if present in an original transaction) is required to be returned without alteration in any Administrative Advice (Retrieval)/0620 pertaining to the original transaction. It contains INF network trace information that allows acquiring INFs to directly route the chargeback or retrieval request to the original acquirer.

When the RiskFinder scoring server generates an Authorization Advice Response/0130 or an Administrative Advice/0620, it places a value of “RISK” in DE 62. When a customer generates a corresponding Administrative Advice Response/0630, DE 62 must contain the same value of “RISK.”

When the Authorization Platform generates an Administrative Advice/0620, it places the value MCBN620060000xxx, where xxx is the MIP ID. When a customer generates a corresponding Administrative Advice Response/0630, DE 62 must contain the same value.

**For UK Domestic Maestro:** This data element is not applicable in UK Domestic Maestro transactions.

## Data Element Definitions

### DE 63—Network Data

---

## DE 63—Network Data

DE 63 (Network Data) is generated by the Authorization Platform for each originating message routed through the network. The receiver must retain the data element and use it in any response or acknowledgement message associated with the originating message.

---

### Attributes

---

Length of Length Field:	3
Data Representation:	ISO: ans...999; LLLVAR
	MasterCard: an...050; LLLVAR
Data Field:	Contents of subfields
Subfields:	2
Justification:	See “Subfields”

---

### Usage

---

Following is the usage of DE 63 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	M
Authorization Request Response/0110	ME	•	M
Authorization Advice/0120—Acquirer-generated	•	X	M
Authorization Advice/0120—Issuer-generated	M	M	•
Authorization Advice/0120—System-generated	•	M	M
Authorization Advice Response/0130—Issuer-generated	ME	ME	•
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	ME	•	ME
Authorization Advice Response/0130—System-generated	•	X	M
Authorization Acknowledgement/0180	ME	ME	•
Authorization Negative Acknowledgement/0190	•	ME	ME
Issuer File Update Request/0302	•	M	•
Issuer File Update Request Response/0312	•	ME	ME
Reversal Request/0400	•	X	M
Reversal Request Response/0410	ME	•	M
Reversal Advice/0420	•	M	M

Reversal Advice Response/0430	ME	ME	•
Administrative Request/0600	•	X	M
Administrative Request Response/0610	ME	•	ME
Administrative Advice/0620	•	M	M
Administrative Advice Response/0630	ME	ME	•
Network Management Request/0800—Sign-On/Sign-Off	•	X	•
Network Management Request/0800—Network Connection Status, Member-generated	•	X	•
Network Management Request/0800—Network Connection Status, System-generated	•	X	•
Network Management Request Response/0810—Network Connection Status, Member-generated	ME	ME	•
Network Management Request Response/0810—Network Connection Status, System-generated	•	ME	ME
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request/0800—PEK Exchange—On Demand	•	M	•
Network Management Request Response/0810	•	ME	ME
Network Management Request Response/0810—PEK Exchange	ME	M	•
Network Management Request Response/0810—PEK Exchange—On Demand	•	ME	ME
Network Management Advice/0820	•	•	M
Network Management Advice/0820—PEK Exchange	•	M	M

**Values**

See “Subfields”

**Application Notes**

This data element contains blanks if the transaction fails edit checking and is rejected before determining the appropriate Financial Network Code.

## Subfield 1—Financial Network Code

DE 63, subfield 1 (Financial Network Code) identifies the specific program or service (for example, the financial network, financial program, or card program) with which the transaction is associated. DE 63 will contain the graduated product when the issuer's cardholder account participates in the Product Graduation Account Level Management service.

## Data Element Definitions

### DE 63—Network Data

---

#### Attributes

Data Representation:	an-3
Data Field:	Contents of positions 1–3
Justification:	Left

#### Values

Code	Description	MC	NP	VI	TE	MS	CI
AMX	American Express <sup>14</sup>				✓		
CBL	Carte Blanche <sup>13</sup>				✓		
CIR	Cirrus					✓	
DAG	Gold Debit MasterCard® Salary		✓				
DAP	Platinum Debit MasterCard® Salary		✓				
DAS	Standard Debit MasterCard® Salary		✓				
DOS	Standard Debit MasterCard® Social		✓				
DCC	Diners Club <sup>13</sup>				✓		
DLG	Debit MasterCard Gold—Delayed Debit		✓				
DLH	Debit MasterCard World Embossed—Delayed Debit		✓				
DLI	Debit MasterCard Standard ISIC Student Card—Delayed Debit		✓				
DLP	Debit MasterCard Platinum—Delayed Debit		✓				
DLS	Debit MasterCard Card—Delayed Debit		✓				
DLU	Debit MasterCard Unembossed—Delayed Debit		✓				
EXC	ADP/Exchange <sup>13</sup>		✓				
HNR	Honor <sup>13</sup>		✓				
ITT	Instant Teller <sup>13</sup>		✓				
JCB	Japanese Credit Bureau <sup>13</sup>		✓				

---

14. This product code is not a valid value in DE 120, MCC103 or MCC104, field 3, Card Program.

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
LNC	LINC New York <sup>13</sup>			✓			
MAB	World Elite™ MasterCard® Business		✓				
MAC	MasterCard® Corporate World Elite®		✓				
MBD	MasterCard Professional Debit Business Card		✓				
MBE	MasterCard® Electronic Business Card	✓					
MBK	MasterCard Black		✓				
MBP	MasterCard Corporate Prepaid		✓				
MBT	MasterCard Corporate Prepaid Travel		✓				
MCA	MasterCard Electronic Basic Card		✓				
MCB	MasterCard BusinessCard® Card MasterCard Corporate Card®		✓				
MCC	MasterCard® Card	✓					
MCE	MasterCard® Electronic™ Card		✓				
MCF	MasterCard Corporate Fleet Card®		✓				
MCG	Gold MasterCard® Card		✓				
MCH	MasterCard Premium Charge		✓				
MCM	MasterCard Corporate Meeting Card <sup>13</sup>		✓				
MCO	MasterCard Corporate		✓				
MCP	MasterCard Corporate Purchasing Card®		✓				
MCS	MasterCard® Standard Card		✓				
MCT	Titanium MasterCard		✓				
MCU	MasterCard Unembossed		✓				
MCV	Merchant-Branded Program		✓				
MCW	World MasterCard™ Card		✓				
MDB	Debit MasterCard BusinessCard Card		✓				
MDG	Debit Gold MasterCard®		✓				

## Data Element Definitions

### DE 63—Network Data

Code	Description	MC	NP	VI	TE	MS	CI
MDH	World Debit Embossed	✓					
MDJ	Debit—Debit Other 2 Embossed	✓					
MDL	Business Debit Other Embossed	✓					
MDM	Middle Market Fleet Card	✓					
MDN	Middle Market Purchasing Card	✓					
MDO	Debit MasterCard Other	✓					
MDP	Debit MasterCard Platinum®	✓					
MDQ	Middle Market Corporate Card	✓					
MDR	MasterCard Debit Brokerage Card	✓					
MDS	Debit MasterCard®	✓					
MDT	MasterCard Business Debit	✓					
MDU	Debit MasterCard Unembossed	✓					
MEB	MasterCard Executive BusinessCard Card	✓					
MEC	MasterCard® Electronic Commercial	✓					
MED	Debit MasterCard Electronic	✓					
MEF	MasterCard Electronic Payment Account	✓					
MEO	MasterCard Corporate Executive Card® <sup>13</sup>	✓					
MEP	Premium Debit MasterCard	✓					
MFB	Flex World Elite	✓					
MFD	Flex Platinum	✓					
MFE	Flex Charge World Elite	✓					
MFH	Flex World	✓					
MFL	Flex Charge Platinum	✓					
MFW	Flex Charge World	✓					
MGF	MasterCard® Government Commercial Card	✓					

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
MHA	MasterCard Healthcare Prepaid Non-tax		✓				
MHB	MasterCard HSA Substantiated		✓				
MHC	MasterCard Healthcare Credit Non-substantiated		✓				
MHH	MasterCard HSA Non-substantiated		✓				
MIA	MasterCard Unembossed Prepaid Student Card		✓				
MIB	MasterCard Credit Electronic Student Card		✓				
MIC	MasterCard Credit Standard Student Card		✓				
MID	MasterCard Debit Unembossed Student Card		✓				
MIG	MasterCard Credit Unembossed Student Card		✓				
MIH	MasterCard Electronic Consumer Non U.S. Student Card		✓				
MIJ	MasterCard Debit Unembossed Non U.S. Student Card		✓				
MIK	MasterCard Electronic Consumer Prepaid Non U.S. Student Card		✓				
MIL	MasterCard Unembossed Prepaid Non U.S. Student Card		✓				
MIP	MasterCard Debit Prepaid Student Card		✓				
MIS	MasterCard Debit Standard Student Card		✓				
MIU	Debit MasterCard Unembossed Outside US		✓				
MLA	MasterCard Central Travel Solutions Air		✓				
MLC	MasterCard Micro-Business Card		✓				
MLD	MasterCard Distribution Card		✓				
MLL	MasterCard Central Travel Solutions Land		✓				

## Data Element Definitions

### DE 63—Network Data

Code	Description	MC	NP	VI	TE	MS	CI
MNF	MasterCard® Public Sector Commercial Card			✓			
MNW	World MasterCard Card (Europe)			✓			
MOC	Standard Maestro® Social					✓	
MOG	Maestro® Gold <sup>13</sup>					✓	
MOP	Maestro® Platinum <sup>13</sup>					✓	
MOW	World Maestro					✓	
MPA	Prepaid MasterCard Payroll Card			✓			
MPB	MasterCard Preferred BusinessCard			✓			
MPC	MasterCard Professional Card			✓			
MPF	Prepaid MasterCard Gift Card			✓			
MPG	Prepaid MasterCard Consumer Reloadable Card			✓			
MPJ	Prepaid Debit MasterCard® Card Gold			✓			
MPK	Prepaid MasterCard® Government Commercial Card			✓			
MPL	Platinum MasterCard® Card			✓			
MPM	Prepaid MasterCard Consumer Promotion Card			✓			
MPN	Prepaid MasterCard Insurance Card			✓			
MPO	Prepaid MasterCard Other Card			✓			
MPR	Prepaid MasterCard Travel Card			✓			
MPT	Prepaid MasterCard Teen Card			✓			
MPV	Prepaid MasterCard Government Benefit Card			✓			
MPW	Prepaid MasterCard Corporate Card			✓			
MPX	Prepaid MasterCard Flex Benefit Card			✓			
MPY	Prepaid MasterCard Employee Incentive Card			✓			
MPZ	Prepaid MasterCard Emergency Assistance Card			✓			

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
MRB	Prepaid MasterCard Electronic BusinessCard			√			
MRC	Prepaid MasterCard Electronic Card			√			
MRF	Standard Deferred			√			
MRG	Prepaid MasterCard Card Outside US			√			
MRH	MasterCard Platinum Prepaid Travel Card			√			
MRJ	Prepaid MasterCard Gold Card			√			
MRL	Prepaid MasterCard Electronic Commercial			√			
MRK	Prepaid MasterCard Public Sector Commercial Card			√			
MRO	MasterCard Rewards Only			√			
MRP	Standard Retailer Centric Payments			√			
MRS	Prepaid MasterCard ISIC Student Card			√			
MRW	Prepaid MasterCard BusinessCard Credit Outside US			√			
MSA	Prepaid Maestro Payroll Card					√	
MSB	Maestro Small Business					√	
MSD	Deferred Debit MasterCard			√			
MSF	Prepaid Maestro Gift Card					√	
MSG	Prepaid Maestro Consumer Reloadable Card					√	
MSI	Maestro					√	
MSJ	Prepaid Maestro Gold					√	
MSM	Prepaid Maestro Consumer Promotion Card					√	
MSN	Prepaid Maestro Insurance Card					√	
MSO	Prepaid Maestro Other Card					√	
MSQ	Maestro Prepaid (Reserved for Future Use)					√	

**Data Element Definitions****DE 63—Network Data**

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
MSR	Prepaid Maestro Travel Card					✓	
MSS	Maestro Student Card					✓	
MST	Prepaid Maestro Teen Card					✓	
MSV	Prepaid Maestro Government Benefit Card					✓	
MSW	Prepaid Maestro Corporate Card					✓	
MSX	Prepaid Maestro Flex Benefit Card					✓	
MSY	Prepaid Maestro Employee Incentive Card					✓	
MSZ	Prepaid Maestro Emergency Assistance Card					✓	
MUP	Premium Debit MasterCard Unembossed				✓		
MUS	Prepaid MasterCard Unembossed US				✓		
MUW	MasterCard World Domestic Affluent				✓		
MWB	World MasterCard® for Business				✓		
MWD	World Deferred				✓		
MWE	MasterCard World Elite				✓		
MWO	MasterCard Corporate World				✓		
MWR	World Retailer Centric Payment				✓		
NYC	NYCE Network <sup>13</sup>				✓		
OLB	Maestro Small Business—Delayed Debit					✓	
OLG	Maestro Gold—Delayed Debit					✓	
OLI	ISIC Maestro Student Card—Delayed Debit					✓	
OLP	Maestro Platinum—Delayed Debit					✓	
OLS	Maestro—Delayed Debit					✓	
OLW	World Maestro Delayed Debit					✓	
PLU	PLUS <sup>13</sup>				✓		

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
PRO	Proprietary Card <sup>13</sup>			✓			
PUL	Pulse <sup>13</sup>			✓			
PVA	Private Label 1			✓			
PVB	Private Label 2			✓			
PVC	Private Label 3			✓			
PVD	Private Label 4			✓			
PVE	Private Label 5			✓			
PVF	Private Label 6			✓			
PVG	Private Label 7			✓			
PVH	Private Label 8			✓			
PVI	Private Label 9			✓			
PVJ	Private Label 10			✓			
PVL	Private label—generic <sup>13</sup>			✓			
SAG	Gold MasterCard® Salary-Immediate Debit			✓			
SAL	Standard Maestro® Salary					✓	
SAP	Platinum MasterCard® Salary-Immediate Debit			✓			
SAS	Standard MasterCard® Salary-Immediate Debit			✓			
SOS	Standard MasterCard® Social-Immediate Debit			✓			
STR	Star Network <sup>13</sup>			✓			
SUR	Prepaid MasterCard Unembossed Outside US			✓			
TBE	Business—Immediate Debit			✓			
TCB	MasterCard Business Card—Immediate Debit			✓			
TCC	MasterCard (Mixed BIN)—Immediate Debit			✓			

## Data Element Definitions

### DE 63—Network Data

Code	Description	MC	NP	VI	TE	MS	CI
TCE	MasterCard Electronic—Immediate Debit			✓			
TCF	MasterCard Fleet Card—Immediate Debit			✓			
TCG	Gold MasterCard Card—Immediate Debit			✓			
TCO	MasterCard Corporate—Immediate Debit			✓			
TCP	MasterCard Purchasing Card—Immediate Debit			✓			
TCS	MasterCard Standard Card—Immediate Debit			✓			
TCW	World Signia MasterCard Card—Immediate Debit			✓			
TDN	Middle Market MasterCard Purchasing Card—Immediate Debit			✓			
TEB	MasterCard Executive BusinessCard Card—Immediate Debit			✓			
TEC	MasterCard Electronic Commercial—Immediate Debit			✓			
TEO	MasterCard Corporate Executive Card—Immediate Debit			✓			
TIB	ISIC MasterCard Electronic Student Card—Immediate Debit			✓			
TIC	ISIC MasterCard Standard Student Card—Immediate Debit			✓			
TIU	MasterCard Unembossed—Immediate Debit			✓			
TLA	MasterCard Central Travel Solutions Air—Immediate Debit			✓			
TNF	MasterCard Public Sector Commercial Card—Immediate Debit			✓			
TNW	MasterCard New World—Immediate Debit			✓			
TPB	MasterCard Preferred Business Card—Immediate Debit			✓			
TPC	MasterCard Professional Card—Immediate Debit			✓			

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
TPL	Platinum MasterCard—Immediate Debit			√			
VIS	VisaNet <sup>13</sup>					√	
WBE	World MasterCard® Black Edition			√			

## **Subfield 2—Banknet Reference Number**

DE 63, subfield 2 (Banknet Reference Number) is generated by the Authorization Platform for each originating message it routes. The reference number is guaranteed to be a unique value for any transaction within the specified financial network on any processing day.

---

### **Attributes**

---

Data Representation: an...9

---

Data Field: Contents of positions 4–12

---

Justification: Left

---

### **Values**

---

The Banknet reference number is a minimum of six characters and a maximum of nine characters long.

---

## **DE 64—Message Authentication Code**

DE 64 (Message Authentication Code [MAC]) validates the source and the text of the message between the sender and the receiver.

---

### **Attributes**

---

Length of Length Field: N/A

---

Data Representation: b-8

---

Data Field: N/A

---

Subfields: N/A

---

Justification: N/A

---

### **Usage**

---

May contain message authentication code as defined by ISO standards.

---

**Data Element Definitions**  
**DE 65—Bit Map, Extended**

---

---

**Values**

---

The last bit position within any bit map is reserved for DE 64. If authentication is to be used on a message, the MAC information is indicated by the final bit of the final bit map of that message. The final bit of all preceding bit maps shall contain 0; for example, there shall be only one DE 64 per message and that DE 64 must be the last data element of the message.

---

## **DE 65—Bit Map, Extended**

DE 65 (Bit Map, Extended) is a series of eight bytes (64 bits) used to identify the presence (denoted by 1) or the absence (denoted by 0) of each data element in an extended (third) message segment.

---

**Attributes**

---

Length of Length Field:	N/A
Data Representation:	b-8
Data Field:	Contents of bit positions 1–64 (8 bytes)
Subfields:	N/A
Justification:	N/A

---

**Usage**

---

The Authorization Platform defines only two message segments, the presence or absence of which is indicated by Primary and Secondary Bit Maps. DE 65 would indicate the presence of a “third” message segment, and must never be present in an Authorization Platform message. The corresponding bit (number 65) must always be 0 in the Secondary Bit Map.

---

## **DE 66—Settlement Code**

DE 66 (Settlement Code) indicates the result of a reconciliation request.

---

**Attributes**

---

Length of Length Field:	N/A
Data Representation:	n-1
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

---

**Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 67—Extended Payment Code**

DE 67 (Extended Payment Code) indicates the number of months that the cardholder prefers to pay for an item (the item purchased during the course of this transaction) if permitted by the card issuer.

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-2
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

**Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 68—Receiving Institution Country Code**

DE 68 (Receiving Institution Country Code) is the code of the country where the receiving institution is located.

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-3
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

**Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 69—Settlement Institution Country Code**

DE 69 (Settlement Institution Country Code) is the code of the country where the settlement institution is located.

## Data Element Definitions

### DE 70—Network Management Information Code

---

#### Attributes

Length of Length Field:	N/A
Data Representation:	n-3
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

#### Usage

The Authorization Platform currently does not use this data element.

## DE 70—Network Management Information Code

DE 70 (Network Management Information Code) identifies network status.

#### Attributes

Length of Length Field:	N/A
Data Representation:	n-3
Data Field:	Contents of positions 1–3
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of DE 70 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Network Management Request/0800—Sign-On/Sign-Off	M	M	•
Network Management Request/0800—RiskFinder SAF Request	M	M	•
Network Management Request/0800—Host Session Activation/Deactivation	M	M	•
Network Management Request/0800—Network Connection Status, Member-generated	M	M	•
Network Management Request/0800—Network Connection Status, System-generated	•	M	M
Network Management Request/0800—PEK Exchange—On Demand	M	M	•
Network Management Request/0800—PEK Exchange	•	M	M

**Data Element Definitions**  
**DE 70—Network Management Information Code**

---

Network Management RequestResponse/0810—RiskFinder SAF Request	•	ME	ME	
Network Management Request Response/0810—Sign-On/Sign-Off	•	ME	ME	
Network Management Request Response/0810—Host Session Activation/Deactivation	•	ME	ME	
Network Management Request Response/0810—Network Connection Status, Member-generated	ME	ME	•	
Network Management Request Response/0810—Network Connection Status, System-generated	•	ME	ME	
Network Management Request Response/0810—PEK Exchange	ME	M	•	
Network Management Request Response/0810—PEK Exchange—On Demand	•	ME	ME	
Network Management Advice/0820—RiskFinder SAF End of File	•	M	M	
Network Management Advice/0820—PEK Exchange	•	M	M	

**Values**

See specific Network Management Information Codes and their status functions, control functions, or both.

**Application Notes**

DE 48 (Additional Data—Private Use) may be used in conjunction with DE 70 to provide complete network status or control information. The Authorization Platform uses this data element in Network Management/08xx messages to convey network control commands and network status information to and from customer information processing systems that interface directly to the Authorization Platform.

This data element is defined and used identically within all MasterCard programs and services.

## Network Management Request/0800—Sign-On/Sign-Off

The following values apply to this message.

<b>Code</b>	<b>Financial Network</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
001 =	Sign-on (by prefix)	✓	✓	✓	✓	✓	✓
002 =	Sign-off (by prefix)	✓	✓	✓	✓	✓	✓
061 =	Group sign-on (by MasterCard group sign-on)	✓	✓	✓	✓	✓	✓
062 =	Group sign-off (by MasterCard group sign-on)	✓	✓	✓	✓	✓	✓

## Data Element Definitions

### DE 70—Network Management Information Code

<b>Code</b>	<b>Financial Network</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
063 =	Group sign-on alternate issuer route	✓	✓			✓	✓
064 =	Group sign-off alternate issuer route	✓	✓			✓	✓
065 =	Prefix sign-on (by Group Sign-on ID for primary route)	✓	✓			✓	✓
066 =	Prefix sign-off (by Group Sign-on ID for primary route)	✓	✓			✓	✓
067 =	Prefix sign-on (by Group Sign-on ID for alternate issuer route) <sup>14</sup>	✓	✓			✓	✓
068 =	Prefix sign-off (by Group Sign-on ID for alternate issuer route) <sup>14</sup>	✓	✓			✓	✓
070 =	Sign-on to RiskFinder by Prefix (member requests RiskFinder-scored Administrative Advice/0620 messages)	✓	✓	✓	✓	✓	✓
071 =	Sign-off to RiskFinder by Prefix (does not request RiskFinder-scored Administrative Advice/0620 messages)	✓	✓	✓	✓	✓	✓
072 =	Member wants to receive, by Prefix, RiskFinder-scored Administrative Advice/0620 messages from SAF or End of file encountered for RiskFinder SAF traffic	✓	✓	✓	✓	✓	✓

### Network Management Request/0800—RiskFinder SAF Request

The following values apply to this message.

<b>Code</b>	<b>Financial Network</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
060 =	SAF session request. The request is acknowledged; however, it will not affect SAF processing.	✓	✓	✓	✓	✓	✓
072 =	Member wants to receive, by Prefix, RiskFinder-scored Administrative Advice/0620 messages from SAF or End of file encountered for RiskFinder SAF traffic.	✓	✓	✓	✓	✓	✓

## **Network Management Advice/0820—RiskFinder SAF End of File**

The following values apply to this message.

<b>Code</b>	<b>Financial Network</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
072 =	Member wants to receive, by Prefix, RiskFinder-scored Administrative Advice/0620 messages from SAF or End of file encountered for RiskFinder SAF traffic.	✓	✓	✓	✓	✓	✓

## **Network Management Request/0800—Network Connection Status, Member-generated**

The following values apply to this message.

<b>Code</b>	<b>Financial Network</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
270 =	Network connection status—echo test	✓				✓	✓

## **Network Management Request/0800—Network Connection Status, System-generated**

The following values apply to this message.

<b>Code</b>	<b>Financial Network</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
270 =	Network connection status—echo test	✓				✓	✓

## **Network Management Request/0800—Host Session Activation/Deactivation**

The following values apply to this message.

<b>Code</b>	<b>Financial Network</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
081 =	Host session activation	✓	✓	✓	✓	✓	✓
082 =	Host session deactivation	✓	✓	✓	✓	✓	✓

## Data Element Definitions

### DE 71—Message Number

---

#### Network Management Request/0800—PEK Exchange

The following values apply to this message.

Code	Financial Network	MC	NP	VI	TE	MS	CI
161 =	Encryption key exchange request	✓	✓			✓	✓

#### Network Management Request/0800—PEK Exchange-On Demand

The following values apply to this message.

Code	Financial Network	MC	NP	VI	TE	MS	CI
162 =	Solicitation for key exchange request	✓	✓			✓	✓

### DE 71—Message Number

DE 71 (Message Number) is a sequential, cyclic number the message initiator assigns to a message. Message Number is used to monitor the integrity of interchange.

---

#### Attributes

Length of Length Field:	N/A
Data Representation:	n-4
Data Field:	N/A
Subfields:	N/A
Justification:	Right

---

#### Usage

The Authorization Platform currently does not use this data element.

---

### DE 72—Message Number Last

DE 72 (Message Number Last) is a sequential, cyclic number the message initiator assigns to a message, used to monitor the integrity of interchange.

---

#### Attributes

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	n-4
Data Field:	N/A
Subfields:	N/A
Justification:	Right

**Usage**

The Authorization Platform currently does not use this data element.

## DE 73—Date, Action

DE 73 (Date, Action) specifies the date (year, month, and day) of a future action. In addition, a message originator may use it as a static time such as a birthdate.

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-6
Data Field:	Contents of positions 1–6
Subfields:	N/A
Justification:	N/A

**Usage**

The Authorization Platform currently does not use this data element.

## DE 74—Credits, Number

DE 74 (Credits, Number) is the numeric sum of credit transactions processed.

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-10
Data Field:	N/A
Subfields:	N/A
Justification:	Right

**Usage**

The Authorization Platform currently does not use this data element.

## **DE 75—Credits, Reversal Number**

DE 75 (Credits, Reversal Number) is the sum number of reversal credit transactions.

---

### **Attributes**

---

Length of Length Field:	N/A
Data Representation:	n-10
Data Field:	N/A
Subfields:	N/A
Justification:	Right

---

### **Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 76—Debits, Number**

DE 76 (Debits, Number) is the sum number of debit transactions processed.

---

### **Attributes**

---

Length of Length Field:	N/A
Data Representation:	n-10
Data Field:	Contents of positions 1–10
Subfields:	N/A
Justification:	Right

---

### **Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 77—Debits, Reversal Number**

DE 77 (Debits, Reversal Number) is the sum number of reversal debit transactions.

---

### **Attributes**

---

Length of Length Field:	N/A
Data Representation:	n-10

---

Data Field:	N/A
-------------	-----

Subfields:	N/A
------------	-----

Justification:	Right
----------------	-------

---

**Usage**

---

The Authorization Platform currently does not use this data element.

---

## DE 78—Transfers, Number

DE 78 (Transfers, Number) is the sum number of all transfer transactions processed.

---

**Attributes**

---

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	n-10
----------------------	------

Data Field:	N/A
-------------	-----

Subfields:	N/A
------------	-----

Justification:	Right
----------------	-------

---

**Usage**

---

The Authorization Platform currently does not use this data element.

---

## DE 79—Transfers, Reversal Number

DE 79 (Transfers, Reversal Number) is the sum number of all transfer reversal transactions processed.

---

**Attributes**

---

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	n-10
----------------------	------

Data Field:	N/A
-------------	-----

Subfields:	N/A
------------	-----

Justification:	Right
----------------	-------

---

**Usage**

---

The Authorization Platform currently does not use this data element.

---

## Data Element Definitions

### DE 80—Inquiries, Number

---

## DE 80—Inquiries, Number

DE 80 (Inquiries, Number) is the sum number of inquiry transaction requests processed.

---

### Attributes

---

Length of Length Field: N/A

---

Data Representation: n-10

---

Data Field: N/A

---

Subfields: N/A

---

Justification: Right

---

### Usage

---

The Authorization Platform currently does not use this data element.

---

## DE 81—Authorizations, Number

DE 81 (Authorizations, Number) is the sum number of Authorization Request/0100 and Authorization Advice/0120 messages processed.

---

### Attributes

---

Length of Length Field: N/A

---

Data Representation: n-10

---

Data Field: N/A

---

Subfields: N/A

---

Justification: Right

---

### Usage

---

The Authorization Platform currently does not use this data element.

---

## DE 82—Credits, Processing Fee Amount

DE 82 (Credits, Processing Fee Amount) is the sum of all processing fees due to an institution or customer for services associated with handling and routing transactions. This MasterCard definition replaces the ISO standard definition.

---

### Attributes

---

Length of Length Field: N/A

---

---

Data Representation:	n-12
----------------------	------

Data Field:	N/A
-------------	-----

Subfields:	N/A
------------	-----

Justification:	Right
----------------	-------

---

**Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 83—Credits, Transaction Fee Amount**

DE 83 (Credits, Transaction Fee Amount) is the sum of all transaction fees due to an institution or customer for processing interchange transactions. This MasterCard definition replaces the ISO standard definition.

---

**Attributes**

---

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	n-12
----------------------	------

Data Field:	N/A
-------------	-----

Subfields:	N/A
------------	-----

Justification:	Right
----------------	-------

---

**Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 84—Debits, Processing Fee Amount**

DE 84 (Debits, Processing Fee Amount) is the sum of all processing fees due from an institution or customer for services associated with handling and routing transactions. This MasterCard definition replaces the ISO standard definition.

---

**Attributes**

---

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	n-12
----------------------	------

Data Field:	N/A
-------------	-----

Subfields:	N/A
------------	-----

Justification:	Right
----------------	-------

## Data Element Definitions

### DE 85—Debits, Transaction Fee Amount

---

#### Usage

---

The Authorization Platform currently does not use this data element.

---

## DE 85—Debits, Transaction Fee Amount

DE 85 (Debits, Transaction Fee Amount) is the sum of all transaction fees due from an institution or customer for processing interchange transactions. This MasterCard definition replaces the ISO standard definition.

---

#### Attributes

---

Length of Length Field:	N/A
Data Representation:	n-12
Data Field:	N/A
Subfields:	N/A
Justification:	Right

---

#### Usage

---

The Authorization Platform currently does not use this data element.

---

## DE 86—Credits, Amount

DE 86 (Credits, Amount) is the sum amount of all credit transactions processed exclusive of any fees.

---

#### Attributes

---

Length of Length Field:	N/A
Data Representation:	n-16
Data Field:	N/A
Subfields:	N/A
Justification:	Right

---

#### Usage

---

The Authorization Platform currently does not use this data element.

---

## DE 87—Credits, Reversal Amount

DE 87 (Credits, Reversal Amount) is the sum amount of reversal credits processed exclusive of any fees.

---

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-16
Data Field:	N/A
Subfields:	N/A
Justification:	Right

**Usage**

---

The Authorization Platform currently does not use this data element.

## DE 88—Debits, Amount

DE 88 (Debits, Amount) is the sum amount of all debit transactions processed exclusive of any fees.

---

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-16
Data Field:	N/A
Subfields:	N/A
Justification:	Right

**Usage**

---

The Authorization Platform currently does not use this data element.

## DE 89—Debits, Reversal Amount

DE 89 (Debits, Reversal Amount) is the sum amount of reversal debits processed exclusive of any fees.

---

**Attributes**

Length of Length Field:	N/A
Data Representation:	n-16
Data Field:	N/A
Subfields:	N/A
Justification:	Right

**Data Element Definitions**  
**DE 90—Original Data Elements**

---

---

**Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 90—Original Data Elements**

DE 90 (Original Data Elements) is the data elements in the original message, intended to identify a transaction for correction or reversal.

---

**Attributes**

---

Length of Length Field: N/A

---

Data Representation: n-42

---

Data Field: Contents of subfields 1–5

---

Subfields: 5

---

Justification: see “Subfields”

---

**Usage**

---

Following is the usage of DE 90 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Reversal Request/0400	M	•	M
Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	M	M
Reversal Advice Response/0430	ME	ME	•

---

**Values**

---

See “Subfields.”

---

**Application Notes**

---

DE 90 is mandatory in the Reversal Advice/0420 message. DE 90 is always present in the Reversal Advice/0420 message whether the Reversal Advice/0420 message is reversing an Authorization Request/0100 message or advising the issuer that MasterCard processed a Reversal Request/0400 message on behalf of the issuer.

---

## **Subfield 1—Original Message Type Identifier**

DE 90, subfield 1 (Original Message Type Identifier) indicates the Message Type Identifier (MTI) of the original message.

---

**Attributes**

---

Data Representation: n-4

---

Data Field: Contents of positions 1–4

---

Justification: N/A

---

**Values**

---

MTI of original message.

---

## **Subfield 2—Original DE 11 (Systems Trace Audit Number)**

DE 90, subfield 2 (Original DE 11 [Systems Trace Audit Number]) indicates the Systems Trace Audit Number (STAN) that was in DE 11 of the original message.

---

**Attributes**

---

Data Representation: n-6

---

Data Field: Contents of positions 5–10

---

Justification: N/A

---

**Values**

---

STAN of original message.

---

## **Subfield 3—Original DE 7 (Transmission Date and Time)**

DE 90, subfield 3 (Original DE 7 [Transmission Date and Time]) indicates the Transmission Date and Time that was in DE 7 of the original message.

---

**Attributes**

---

Data Representation: n-10

---

Data Field: Contents of positions 11-20 (in MMDDhhmmss format)

---

Justification: N/A

---

**Values**

---

Transmission date and time of original message. This subfield must contain a valid date expressed as month (MM) and day (DD) and a valid time expressed as hours (hh), minutes (mm), and seconds (ss).

---

### **Subfield 4—Original DE 32 (Acquiring Institution ID Code)**

DE 90, subfield 4 (Original DE 32 [Acquiring Institution ID Code]) indicates the Acquiring Institution ID Code that was in DE 32 of the original message.

---

#### **Attributes**

---

Data Representation:	n-11
Data Field:	Contents of positions 21–31
Justification:	Right with leading zeros

---

#### **Values**

---

Acquiring Institution ID code of original message.

---

### **Subfield 5—Original DE 33 (Forwarding Institution ID Code)**

DE 90, subfield 5 (Original DE 33 [Forwarding Institution ID Code]) indicates the Forwarding Institution ID Code that was in DE 33 of the original message.

---

#### **Attributes**

---

Data Representation:	n-11
Data Field:	Contents of positions 32–42
Justification:	Right with leading zeros

---

#### **Values**

---

Forwarding Institution ID code of original message.

---

## **DE 91—Issuer File Update Code**

DE 91 (Issuer File Update Code) indicates to the system maintaining a file which procedure to follow.

---

#### **Attributes**

---

Length of Length Field:	N/A
Data Representation:	an-1
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	Right

---

#### **Usage**

---

Following is the usage of DE 91 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Issuer File Update Request/0302	M	M	•
Issuer File Update Request Response/0312	•	ME	ME
<b>Values</b>			
1 = Add			
2 = Update			
3 = Delete			
5 = Inquiry			

#### Application Notes

This data element is defined and used identically within all MasterCard programs and services.

## DE 92—File Security Code

DE 92 (File Security Code) is an Issuer File Update security code used to indicate that a message originator is authorized to update a file.

#### Attributes

Length of Length Field:	N/A
Data Representation:	an-2
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

#### Usage

The Authorization Platform currently does not use this data element.

## DE 93—Response Indicator

DE 93 (Response Indicator) indicates the update action a POS system takes.

#### Attributes

Length of Length Field:	N/A
Data Representation:	n-5

## Data Element Definitions

### DE 94—Service Indicator

---

Data Field:	N/A
-------------	-----

Subfields:	N/A
------------	-----

Justification:	Right
----------------	-------

#### Usage

The Authorization Platform currently does not use this data element.

## DE 94—Service Indicator

DE 94 (Service Indicator) indicates the service a message recipient requires.

---

#### Attributes

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	ans-7
----------------------	-------

Data Field:	Contents of positions 1–7. Positions 4–7 must contain spaces or zeros.
-------------	--

Subfields:	3
------------	---

Justification:	See “Subfields”
----------------	-----------------

---

#### Usage

Following is the usage of DE 94 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Network Management Request/0800	M	M	•

---

#### Values

This data element is used in Network Management Request/0800 Sign-on/off messages to indicate that a CPS is signing on or off for debit card traffic, credit card traffic, or both. It is also used to indicate if the sign-on or sign-off applies to acquirer traffic, issuer traffic, or both.

The Authorization Platform allows credit card transactions and debit card transactions from a single institution to be routed to different processing systems.

---

#### Application Notes

See “Subfields”

## Subfield 1—Reserved for Future Use

DE 94, subfield 1 (Reserved for Future Use) is reserved for future use.

**Attributes**

Data Representation: an-1

Data Field: Contents of position 1

Justification: N/A

**Values**

0 = Reserved for Future Use

**Subfield 2—Acquirer/Issuer Indicator**

DE 94, subfield 2 (Acquirer/Issuer Indicator) indicates if the sign-on or sign-off message applies to acquirer traffic, issuer traffic, or both.

**Attributes**

Data Representation: a-1

Data Field: Contents of position 2

Justification: N/A

**Values**

A = Acquirer only

I = Issuer only

B = Both acquirer and issuer

**Subfield 3—Address Data Indicator**

DE 94, subfield 3 (Address Data Indicator) indicates how the address data is provided.

**Attributes**

Data Representation: n-1

Data Field: Contents of position 3

Justification: N/A

**Values**

0 = AVS not currently supported

1 = Issuer receives complete address data

**Data Element Definitions**  
**DE 95—Replacement Amounts**

---

2	=	Issuer receives condensed address data. (This supports the algorithm that uses the first five numeric digits in an address [when scanning the address from left to right].)
3	=	Issuer receives condensed address data. (This supports the algorithm that uses up to the first five numeric digits in an address. This algorithm stops searching for a numeric after it encounters an alphabetic character or space [when scanning the address from left to right].)
4	=	Issuer receives condensed numeric postal code and condensed numeric address data only. (This supports the algorithm that uses the first five numeric digits in an address [when scanning the address from left to right].)

## **DE 95—Replacement Amounts**

DE 95 (Replacement Amounts) contains the “actual amount” subfields necessary to perform a partial or full reversal of a financial transaction.

---

### **Attributes**

---

Length of Length Field:	N/A
Data Representation:	n-42
Data Field:	Contents of subfields 1–4
Subfields:	4
Justification:	See “Subfields”

---

### **Usage**

---

Following is the usage of DE 95 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Reversal Request/0400	C	X	C
Reversal Request Response/0410	CE	X	C
Reversal Advice/0420	•	C	C
Reversal Advice Response/0430	CE	CE	•

---

### **Values**

---

See “Subfields.”

Subfield 1 (Actual Amount, Transaction) must contain valid numeric data. All other subfields must be zero-filled; if required, the Authorization Platform performs currency conversion.

DE 95 is necessary to perform a partial reversal of an authorization transaction. However, the Authorization Platform will support full reversals via usage of a Reversal Request/0400 message. Therefore, acquirers are not required to include DE 95 in the Reversal Request/0400 message. If DE 95 is included in a Reversal Request/0400 message for full reversals, DE 95 must contain a value of all zeros.

The Authorization Platform requires a message initiator to generate only subfield 1 (Actual Amount, Transaction). The Authorization Platform automatically calculates and inserts subfield 2 (Actual Amount, Settlement) and subfield 3 (Actual Amount, Cardholder Billing).

**The subfield definitions the Authorization Platform employs differ slightly from the ISO subfield definitions for this data element. This difference accommodates the Authorization Platform automatic currency conversion service.**

---

#### **Application Notes**

This data element is defined and used identically within all MasterCard programs and services. MasterCard does not provide currency conversion services for all programs and services.

MasterCard supports DE 95 in Reversal Request/0400 and Reversal Advice/0420 messages. DE 95 must be less than DE 4. If DE 95 contains all zeros, MasterCard will remove DE 95 before forwarding the message to the issuer.

**For UK Domestic Maestro:** This data element is not applicable in UK Domestic Maestro transactions.

---

## **Subfield 1—Actual Amount, Transaction**

DE 95, subfield 1 (Actual Amount, Transaction) indicates the actual transaction amount.

---

#### **Attributes**

---

Data Representation: n-12

---

Data Field: Contents of positions 1–12

---

Justification: Right with leading zeros

---

#### **Values**

---

**Full Reversal:** If present, and the reversal is a full reversal, DE 95, subfield 1 must contain a value of all zeros.

**Partial Reversal:** If the reversal is a partial reversal, DE 95, subfield 1 must contain a value less than the amount in DE 4 (Amount Transaction).

---

## **Subfield 2—Actual Amount, Settlement**

DE 95, subfield 2 (Actual Amount, Settlement) indicates the actual settlement amount in the settlement currency.

---

### **Attributes**

---

Data Representation:	n-12
Data Field:	Contents of positions 13–24
Justification:	Right with leading zeros

---

### **Values**

---

Must contain valid numeric data. Absence of data must be indicated with zeros.

---

### **Application Notes**

---

All settlement amounts are specified in U.S. dollars. The Authorization Platform will provide this subfield in the settlement currency (U.S. dollars) if subfield 1 is not all zeros and if the customer chooses to receive settlement amount-related data elements; otherwise, subfield 2 is zero-filled.

---

## **Subfield 3—Actual Amount, Cardholder Billing**

DE 95, subfield 3 (Actual Amount, Cardholder Billing) the actual amount in the issuer currency.

---

### **Attributes**

---

Data Representation:	n-12
Data Field:	Contents of positions 25–36
Justification:	Right with leading zeros

---

### **Values**

---

Must contain valid numeric data. Absence of data must be indicated with zeros. The Authorization Platform will provide this subfield in the issuer's cardholder billing currency if subfield 1 is not all zeros.

---

## **Subfield 4—Zero Fill**

DE 95, subfield 4 (Zero Fill) indicates zeros.

---

### **Attributes**

---

Data Representation:	n-6
Data Field:	Contents of positions 37–42

---

---

Justification:	N/A
----------------	-----

**Values**

---

Must contain zeros.
---------------------

## **DE 96—Message Security Code**

DE 96 (Message Security Code) is a verification between a card acceptor and a card issuer that a message is authorized to update or modify a special file.

---

**Attributes**

---

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	ISO: b-8 MasterCard: n-8
----------------------	-----------------------------

Data Field:	ISO: Contents of bit positions 1–64 (8 bytes) MasterCard: Contents of positions 1–8 (EBCDIC hexadecimal format)
-------------	--

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

---

**Usage**

---

Following is the usage of DE 96 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Issuer File Update Request/0302	M	M	•
Network Management Request/0800	M	M	•

---

**Values**

---

If an issuer has been assigned a Security Authorization Code that represents the MasterCard customer “password”, allowing access in the Authorization Platform network by the CPS or INF processor, this data element must contain valid security control data when used in Issuer File Update/0302, and Network Management Request/0800—Sign-On/Sign-Off, and Network Management Request/0800—RiskFinder SAF Request messages.

## **DE 97—Amount, Net Settlement**

DE 97 (Amount, Net Settlement) is the net value of all gross amounts.

---

**Attributes**

---

Length of Length Field:	N/A
-------------------------	-----

## Data Element Definitions

### DE 98—Payee

---

Data Representation:	an-17
Data Field:	Contents of subfields 1–2
Subfields:	2
Justification:	See “Subfields”
<b>Usage</b>	
The Authorization Platform currently does not use this data element.	

### Subfield 1—Debit/Credit Indicator

DE 97, subfield 1 (Debit/Credit Indicator) indicates whether the transaction was credit or debit.

---

#### Attributes

---

Data Representation:	a-1
Data Field:	Contents of position 1
Justification:	N/A

---

#### Values

---

N/A
-----

### Subfield 2—Amount

DE 97, subfield 2 (Amount) indicates the transaction amount.

---

#### Attributes

---

Data Representation:	n-16
Data Field:	Contents of positions 2–17
Justification:	Right

---

#### Values

---

N/A
-----

## DE 98—Payee

DE 98 (Payee), is the third-party beneficiary in a payment transaction.

**Attributes**

Length of Length Field:	N/A
Data Representation:	ans-25
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

The Authorization Platform currently does not use this data element.

---

## DE 99—Settlement Institution ID Code

DE 99 (Settlement Institution ID Code) identifies the settlement institution or its agent.

**Attributes**

Length of Length Field:	2
Data Representation:	n...11; LLVAR
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

**Usage**

The Authorization Platform currently does not use this data element.

---

## DE 100—Receiving Institution ID Code

DE 100 (Receiving Institution ID Code) is the identity of the institution receiving a Request or Advice message in an interchange system if not the same as identified in DE 2 (Primary Account Number [PAN]) or DE 34 (Primary Account Number [PAN], Extended). The Authorization Platform uses DE 100 to determine the destination routing of Administrative/06xx messages. For these messages, DE 33 (Forwarding Institution ID Code) identifies the “sender” of the message; DE 100 identifies the “receiver” of the message.

**Attributes**

Length of Length Field:	2
Data Representation:	n...11; LLVAR
Data Field:	Contents of positions 1-11

## Data Element Definitions

### DE 101—File Name

---

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

#### Usage

---

Following is the usage of DE 100 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Administrative Advice/0620	•	M	M
Administrative Advice Response/0630	ME	ME	•

#### Values

---

Must contain a valid five-digit MasterCard customer ID number. It identifies the destination CPS or INF to receive the message.

#### Application Notes

---

This data element is defined and used identically within all MasterCard programs and services.

Processing systems responding to originating Administrative Advice/06xx and Network Management/08xx messages must not swap the contents of DE 33 and DE 100 in the Response message to achieve proper routing of the Response to the originator.

## DE 101—File Name

DE 101 (File Name) is the actual or abbreviated name of the file that the issuer accesses. DE 101 is used in Issuer File Update/03xx messages to identify the specific name of an Authorization Platform data file or program parameter table that is being updated by a customer's Issuer File Update Request/0302.

---

#### Attributes

Length of Length Field:	2
-------------------------	---

Data Representation:	ans...17; LLVAR
----------------------	-----------------

Data Field:	Contents of positions 1–17
-------------	----------------------------

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

#### Usage

---

Following is the usage of DE 101 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Issuer File Update Request/0302	M	M	•

Issuer File Update Request Response/0312	•	ME	ME
<b>Values</b>			
MCC102	=	Stand-In Account File	
MCC103	=	Electronic Warning Bulletin File	
MCC104	=	Local Stoplist File	
MCC105	=	Recurring Payment Cancellation Service File	
MCC106	=	PAN Mapping File	
MCC107	=	Enhanced Value File	
MCC108	=	Product Graduation File	
MCC109	=	<i>PayPass Application Transaction Counter (ATC) File</i>	

**Example****NOTE**

**For UK Domestic Maestro: This data element is not applicable in Authorization Request/0100 messages.**

**DE 102—Account ID 1**

DE 102 (Account ID-1) is a series of digits that identify a customer account or relationship. Members primarily use it for the “from account” in a transfer transaction. DE 102 may be used in Authorization Request Response/0110 messages to identify the specific “from account” that the transaction affected. DE 102 may be used for printing on cardholder transaction receipts.

**Attributes**

Length of Length Field:	2
Data Representation:	ans...28; LIVAR
Data Field:	Contents of positions 1–28
Subfields:	N/A
Justification:	N/A

**Usage**

Following is the usage of DE 102 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C

## Data Element Definitions

### DE 103—Account ID 2

Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C

#### Values

The “from” account is the account specified in digits three and four of DE 3 (Processing Code).

#### Application Notes

This data element is defined and used identically within all MasterCard programs and services.

## DE 103—Account ID 2

DE 103 (Account ID-2) is a series of digits that identify a customer account or relationship. Members primarily use it for the “to account” in a transfer transaction.

#### Attributes

Length of Length Field:	2
Data Representation:	ans...28; LLVAR
Data Field:	Contents of positions 1–28
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of DE 103 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C

#### Values

The “To Account” is specified in digits five and six of DE 3 (Processing Code).

#### Application Notes

This data element is defined and used identically within all MasterCard programs and services.

## **DE 104—Transaction Description**

DE 104 (Transaction Description) describes additional characteristics of the transaction for billing purposes

---

### **Attributes**

---

Length of Length Field:	3
Data Representation:	ans...100; LLLVAR
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

---

### **Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 105–DE 111—Reserved for Future Use**

DE 105–DE 111 (Reserved for ISO Use) are reserved for future use

---

### **Attributes**

---

Length of Length Field:	3
Data Representation:	ans...999; LLLVAR
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

---

### **Usage**

---

The Authorization Platform currently does not use this data element.

---

## **DE 112—Additional Data, National Use**

DE 112 (Additional Data—National Use) is reserved for national organizations to define data unique to specific networks or specific programs and services. DE 112 provides other supplemental data in a message when a specific ISO-designated data element is not available. It is a free-format, variable-length, alphanumeric data element used for information on transactions between customers.

## Data Element Definitions

### DE 112—Additional Data, National Use

---

#### Attributes

Length of Length Field:	3
Data Representation:	ans...100; LLLVAR (The operational length is limited to 100 bytes by system constraints)
Data Field:	Contents of subelements
Subelements:	5
Justification:	N/A

#### Usage

Following is the usage of DE 112 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Issuer-generated	C	•	C
Reversal Request/0400	C	•	C
Reversal Request Response/0410	C	•	C

#### Values

See “Subfields”

#### Application Notes

##### **MasterCard does not perform currency conversion on any amounts in DE 112.**

This data element is defined and used identically within all MasterCard programs and services.

**For UK Domestic Maestro:** UK Domestic Maestro acquirers must populate subelement 001 (Reason Online Code) and subelement 002 (Retailer Classification Code) when used in UK Domestic Maestro transactions.

## DE 112—Encoding Scheme

MasterCard organizes DE 112 into a group of encoded subelements. The overall length of DE 112 is restricted to 103 bytes to accommodate operational limitations. The following table illustrates the structure of DE 112.

LLL	“VAR”—100 maximum					
3 bytes	3 bytes	3 bytes	1–94 bytes	3 bytes	3 bytes	1–94 bytes

Total Length	First Subelement (SE) Data			Second Subelement (SE) Data		
	SE ID	SE Length	SE Variable Length Data	SE ID	SE Length	SE Variable Length Data
<b>103 maximum bytes</b>						

<b>Number of Bytes</b>	<b>Attribute</b>	<b>Description</b>	
3	Total Data Element Length	The “LLL” portion of the data element up to 100	
3	Subelement ID	In the range 000–099	
		000–069	Defined universally for all programs and services
		070–099	Defined for individual programs and services
3	Subelement Length	In the range of 001–094	
1...94	Subelement Variable Length Data	Contains valid values.	

## Cuotas—Payment Transactions

Following are the technical specification for Authorization/01xx message for Cuotas payment transactions within Argentina, Paraguay, and Uruguay.

### Subelement 001—Installment Payment Data

DE 112, Cuotas, subelement 001 (Installment Payment Data) is used in the Authorization Platform for Cuotas payment transactions. Subelement 001 must be present if DE 48, subelement 95 (MasterCard Promotion Code) contains the value ARGCTA, PRYCTA, or URYCTA.

---

#### Attributes

---

Subelement ID:	001
Length of Length Field:	3
Data Representation:	ans...4
Data Field:	Contents of positions 1–4 where:
	XX = positions 1–2

**Data Element Definitions****DE 112—Additional Data, National Use**

---

YY	=	positions 3–4
----	---	---------------

---

Subfields:	N/A
------------	-----

---

Justification:	N/A
----------------	-----

---

**Values****Cuotas Payment Transactions in the Authorization Request/0100**

---

Used for various Cuotas transactions: From acquirer to issuer in the following format:

---

XX	Cuotas plan type:
----	-------------------

---

20	= Issuer-financed
21	= Merchant-financed
22	= Acquirer-financed
23	= Average payment financing
24	= Consumer financing (Purchase)
25	= Consumer financing (Manual Cash Advance)
80	= ATM Installment Inquiry
81	= ATM Installment Withdrawal

---

YY	The total number of Cuotas
----	----------------------------

---

**Cuotas Payment Transactions in the Authorization Request Response/0110**

---

Used for various Cuotas transactions: From issuer to acquirer in the following format:

---

XX	Cuotas plan type:
----	-------------------

---

20	= Issuer-financed
21	= Merchant-financed
22	= Acquirer-financed
23	= Average payment financing
24	= Consumer financing (Purchase)
25	= Consumer financing (Manual Cash Advance)
80	= ATM Installment Inquiry
81	= ATM Installment Withdrawal

---

YY	The total number of Cuotas.
----	-----------------------------

---

### **Subelement 003—Installment Payment Response Data**

DE 112, Cuotas, subelement 003 (Installment Payment Response Data) is used in the Authorization Platform and Cuotas payment transactions to provide issuer response data only for consumer financing plan types 24 and 25.

---

#### **Attributes**

---

Subelement ID:	003
Length of Length Field:	3
Data Representation:	ans...55
Data Field:	Contents of positions 1–55
Subfields:	N/A
Justification:	N/A

---

#### **Values**

---

Consumer Financing Cuotas transactions in the Authorization Request Response/0110:

---

From issuer to acquirer, upon transaction approval; all amounts in transaction currency; use the following format:

---

Positions	Length	Description
1–12	12	Installment amount including any issuer-calculated interest, insurance, or other charges; two decimal places.
13–17	5	Annual nominal interest percentage rate or all zeros if nominal rate not applicable; two decimal places.
18–22	5	Annual actual interest percentage rate or all zeros if actual rate not applicable; two decimal places.
23–27	5	Insurance percentage rate or all zeros if insurance not applicable; two decimal places.
28–39	12	Insurance amount or all zeros if insurance not applicable; two decimal places.
40–51	12	Issuing charge amount or all zeros if issuing charge not applicable; two decimal places.
52–53	2	Total number of installments, or all zeros if total number of installments not applicable.
54–55	2	Reserved for future use; insert all zeros.

## Data Element Definitions

### DE 112—Additional Data, National Use

---

#### **Subelement 027—ATM Credit Card Cash Advance Installments**

DE 112, Cuotas—Payment Transactions, subelement 027 (ATM Credit Card Cash Advance Installments) is used in the Authorization System for credit card cash advance installment transactions performed at the ATM. Subelement 027 contains details of the cash advance installment transaction.

---

##### **Attributes**

---

Subelement ID:	027
Length of Length Field:	3
Data Representation:	an-4 (Authorization Request/0100) an-137 (Authorization Request Response/0110)
Data Field:	Contents of subfields Subfields 1–2 (Authorization Request/0100) Subfields 3–11 (Authorization Request Response/0110)
Subfields:	11
Justification:	See “Subfields”

---

##### **Usage**

---

Following is the usage of subelement 027 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	C	•	C

---

##### **Values**

---

See “Subfields”

---

#### **Subfield 1—Transaction Type**

DE 112, Cuotas—Payment Transactions, subelement 027, subfield 1 (Transaction Type) contains the type of ATM credit card cash advance installment transaction.

---

##### **Attributes**

---

Subfield ID:	1
Data Representation:	an-2
Data Field:	Contents of positions 7–8
Justification:	N/A

---

##### **Values**

---

80	=	ATM Installment Inquiry
81	=	ATM Installment Withdrawal

### **Subfield 2—Requested Number of Installments**

DE 112, Cuotas—Payment Transactions, subelement 027, subfield 2 (Requested Number of Installments) contains the requested number of payments required to payoff the credit card cash advance.

---

#### **Attributes**

---

Subfield ID:	2
Data Representation:	n-2
Data Field:	Contents of positions 9–10
Justification:	N/A

---

#### **Values**

---

Valid values 01-99

---

### **Subfield 3—Approved Number of Installments**

DE 112, Cuotas—Payment Transactions, subelement 027, subfield 3 (Approved Number of Installments) contains the number of installment payments approved by the issuer.

---

#### **Attributes**

---

Subfield ID:	3
Data Representation:	n-2
Data Field:	Contents of positions 11–12
Justification:	Left

---

#### **Values**

---

Valid values 01–99

---

### **Subfield 4—Installment Amount**

DE 112, Cuotas—Payment Transactions, subelement 027, subfield 4 (Installment Amount) contains the monthly payment amount.

---

#### **Attributes**

---

Subfield ID:	4
--------------	---

## Data Element Definitions

### DE 112—Additional Data, National Use

---

Data Representation:	n-12
Data Field:	Contents of positions 13–24
Justification:	Right with leading zeros

#### **Subfield 5—Total Transaction Amount**

DE 112, Cuotas—Payment Transactions, subelement 027, subfield 5 (Total Transaction Amount) contains the total amount of the credit card cash advance and the interest charged by the issuer.

---

#### **Attributes**

Subfield ID:	5
Data Representation:	n-12
Data Field:	Contents of positions 25–36
Justification:	Right with leading zeros

#### **Subfield 6—Yearly Interest Rate**

DE 112, Cuotas—Payment Transactions, subelement 027, subfield 6 (Yearly Interest Rate) contains the yearly interest rate that the issuer charges the cardholder for the installment payment.

---

#### **Attributes**

Subfield ID:	6
Data Representation:	n-4
Data Field:	Contents of positions 37–40
Justification:	Right with leading zeros

#### **Subfield 7—Currency Code**

DE 112, Cuotas—Payment Transactions, subelement 027, subfield 7 (Currency Code) contains the currency code the issuer will be charging the cardholder for repayment.

---

#### **Attributes**

Subfield ID:	7
Data Representation:	n-3
Data Field:	Contents of positions 41–43
Justification:	N/A

### **Subfield 8—Member-defined Data**

DE 112, Cuotas—Payment Transactions, subelement 027, subfield 8 (Member-defined data) contains member data.

---

#### **Attributes**

---

Subfield ID:	8
Data Representation:	an-25
Data Field:	Contents of positions 44–68
Justification:	N/A

---

### **Subfield 9—Member-defined Data**

DE 112, Cuotas—Payment Transactions, subelement 027, subfield 9 (Member-defined data) contains member data.

---

#### **Attributes**

---

Subfield ID:	9
Data Representation:	an-25
Data Field:	Contents of positions 69–93
Justification:	N/A

---

## **Mexcta—PaymentTransactions**

Following are the technical specifications for Authorization/01xx messages for Mexcta payment transactions within Mexico.

### **Subelement 004—Credit Line Usage Fee (CLUF)**

DE 112, Mexta, subelement 004 (Credit Line Usage Fee [CLUF]) contains the currency code and fee amount associated with the CLUF for domestic credit card cash advance (CCCA) ATM transactions in Authorization Request Response/0110 and Authorization Reversal Request/0400 Messages.

---

#### **Attributes**

---

Subelement ID:	004
Length of Length Field:	3
Data Representation:	n-11
Data Field:	Contents of positions 1–11

---

## Data Element Definitions

### DE 112—Additional Data, National Use

---

Subfields:	N/A
Justification:	Right-justified
<b>Values</b>	
Numeric currency code (positions 1–3)	
Fee amount (positions 4–11)	

### Subelement 005—Issuing Bank Name (AKA Doing Business As [DBA])

DE 112, Mexta, subelement 005 (Issuing Bank Name [AKA Doing Business As (DBA)]) contains the issuing bank name (DBA) for ATM transactions where the Credit Line Usage Fee (CLUF) applies in Authorization Request Response/0110 and Authorization Reversal Request/0400 Messages.

---

#### Attributes

---

Subelement ID:	005
Length of Length Field:	3
Data Representation:	ans-20
Data Field:	Contents of positions 1–20
Subfields:	N/A
Justification:	Left-justified, trailing spaces

### Subelement 006—Financial Institution ID (FIID)

DE 112, Mexcta, subelement 006 (Financial Institution ID [FIID]) is used in Credit Line Usage Fee (CLUF) transactions on domestic ATM credit card cash advance transactions in the Authorization platform in Authorization Request Response/0110 and Authorization Reversal Request/0400 Messages.

---

#### Attributes

---

Subelement ID:	006
Length of Length Field:	3
Data Representation:	ans-4
Data Field:	Contents of positions 1–4
Subfields:	N/A
Justification:	N/A

---

**Values**

---

Valid FIID

---

### **Subelement 007—Installment Payment Data**

DE 112, Mexcta, subelement 007 (Installment Payment Data) is used in the Authorization Platform for Mexcta payment transactions.

---

**Attributes**

---

Subelement ID:	007
Length of Length Field:	3
Data Representation:	ans-9
Data Field:	Contents of positions 1–9
Subfields:	N/A
Justification:	N/A

---

**Values**

---

#### **Mexcta Payment Transactions in the Authorization Request/0100**

XX	Installment pay plan types (positions 1–2). Valid values include:
	<ul style="list-style-type: none"><li>• 00 (No promotion)</li><li>• 03 (Without interest for the cardholder)</li><li>• 05 (With interest for the cardholder)</li><li>• 07 (Buy today, pay later)</li></ul>
YY	The total number of installments (positions 3–4). Valid value is 01–99.
ZZ	Grace period before first payment (positions 5–6). Valid values is 00–99.
NNN	Transaction Currency Code (positions 7–9). Same value as DE 49 (Currency Code, Transaction) This is the local currency of the acquirer or source location of the transaction. It specifies the currency used in DE 4 (Amount, Transaction). 484 = Mexican Peso

---

#### **Mexcta Payment Transactions in the Authorization Request Response/0110**

XX	Installment pay plan types (positions 1–2). Valid values include:
	<ul style="list-style-type: none"><li>• 00 (No promotion)</li><li>• 03 (Without interest for the cardholder)</li><li>• 05 (With interest for the cardholder)</li><li>• 07 (Buy today, pay later)</li></ul>

---

## Data Element Definitions

### DE 112—Additional Data, National Use

---

YY	The total number of installments (positions 3–4). Valid value is 01–99.
ZZ	Grace period before first payment (positions 5–6). Valid value is 00–99.
NNN	Transaction Currency Code (positions 7–9). Same value as DE 49 (Currency Code, Transaction) This is the local currency of the acquirer or source location of the transaction. It specifies the currency used in DE 4 (Amount, Transaction). 484 = Mexican Peso

### Subelement 008—Installment Payment Response Data

DE 112, Mexcta, subelement 008 (Installment Payment Response Data) is used in the Authorization Platform and Mexcta payment transactions in the Authorization Request Response/0110.

---

#### Attributes

---

Subelement ID:	008
Length of Length Field:	023
Data Representation:	ans-23
Data Field:	Contents of positions 1–23
Subfields:	N/A
Justification:	N/A

---

#### Values

---

Installment amount (positions 1–12)	Installment amount (with two decimal places) including any issuer-calculated interest, insurance, or other charges.
Due Date of First Installment (positions 13–18)	Due Date of First Installment (in binary format: ddmmyyyy)
Finance currency code (positions 19–21)	This is the currency in which the issuer will finance the transaction. This specifies the currency used in installment amount, above 484 (Mexican Peso)
Payment Plan (positions 22–23)	Reserved for future use. Insert all zeros.

### Parcelas—Payment Transactions

Following are the technical specifications for Authorization/01xx messages for Parcelas payment transactions within Brazil.

## **Subelement 001—Installment Payment Data**

DE 112, Parcelas, subelement 001 (Installment Payment Data) is used in the Authorization Platform for Parcelas payment transactions.

---

### **Attributes**

---

Subelement ID:	001
Length of Length Field:	3
Data Representation:	ans-4
Data Field:	Contents of positions 1–4
Subfields:	N/A
Justification:	N/A

---

### **Values**

---

#### **Parcelas Payment Transactions in the Authorization Request/0100**

---

Used for both issuer- or merchant-financed Parcelas transactions: From acquirer to issuer requiring approval; use the following format:

XX    Parcelas plan type:

---

20    =    Issuer-financed

---

21    =    Merchant-financed

YY    The total number of Parcelas

---

#### **Parcelas Payment Transactions in the Authorization Request Response/0110**

---

Used for both issuer- or merchant-financed Parcelas transactions: From acquirer to issuer requiring approval. Echoing this subelement in the Authorization Request Response is unique to Brazil processing. Use the following format:

XX    Parcelas plan type:

---

20    =    Issuer-financed

---

21    =    Merchant-financed

YY    The total number of Parcelas

---

## **Subelement 002—Installment Payment Response Data**

DE 112, Parcelas, subelement 002 (Installment Payment Response Data) is used in the Authorization Platform and Parcelas payment transactions.

---

### **Attributes**

---

Subelement ID:	002
----------------	-----

---

## Data Element Definitions

### DE 112—Additional Data, National Use

---

Length of Length Field:	3
Data Representation:	ans...32 if format 1 used; ans...4 if format 2 used
Data Field:	Contents of positions 1–32 or 1–4
Subfields:	N/A
Justification:	N/A

#### Values

---

##### **Format 1: Issuer-Financed Parcelas transactions in the Authorization Request Response/0110:**

---

Issuer acknowledgement format 1, from issuer to acquirer, upon transaction approval; all amounts are express in transaction currency; contents are as follows:

Positions 1–4	Parcelas information, same as subelement 001.
Positions 5–16	Parcelas (or installment) amount issuer calculates, including calculated interest; two decimal places.
Positions 17–28	Transaction total amount issuer calculates, including calculated interest; two decimal places.
Positions 29–32	Monthly interest rate issuer calculates; two decimal places.

##### **Format 2: Merchant-Financed Parcelas transactions in the Authorization Request Response/0110**

---

Issuer acknowledgement format 2, from issuer to acquirer, upon transaction approval; Parcelas information copied from subelement 001 as follows:

21	=	Merchant-financed
YY	=	The total number of Parcelas

## Percta—Payment Transactions

Following are the technical specifications for Authorization/01xx messages for Percta payment transactions within Peru.

### Subelement 007—Installment Payment Data

DE 112, Percta, Subelement 007 (Installment Payment Data) is used in the Authorization Platform for Percta payment transactions.

---

#### Attributes

---

Subelement ID:	007
Length of Length Field:	3
Data Representation:	ans-8

Data Field:	Contents of positions 1–8
Subfields:	N/A
Justification:	N/A

**Values**

**Percta Payment Transactions in the Authorization Request/0100**

XX Type of credit (positions 1–2). Valid value is 20 (Issuer-financed) In the case of Peru, issuer finance is the only finance model.

YY The total number of installments (positions 3–4). Valid value is 01–99.

Z Grace period before first payment (position 5). Valid values are:

- 0 = No grace period
- 1 = One month
- 2 = Two months

NNN Transaction Currency Code (positions 6–8). Echo of DE 49 (Currency Code, Transaction)

This is the local currency of the acquirer or source location of the transaction. It specifies the currency used in DE 4 (Amount, Transaction).

604 = Peru Nuevo Sol

840 = United States dollar

**Percta Payment Transactions in the Authorization Request Response/0110**

XX Type of credit (positions 1–2). Valid value is 20 (Issuer-financed) In the case of Peru, issuer finance is the only finance model.

YY The total number of installments (positions 3–4). Valid value is 01–99.

Z Grace period before first payment (position 5). Valid values are:

- 0 = No grace period
- 1 = One month
- 2 = Two months

NNN Transaction Currency Code (positions 6–8). Echo of DE 49 (Currency Code, Transaction)

This is the local currency of the acquirer or source location of the transaction. It specifies the currency used in DE 4 (Amount, Transaction).

604 = Peru Nuevo Sol

840 = United States dollar

**Subelement 008—Installment Payment Response Data**

DE 112, Percta, subelement 008 (Installment Payment Response Data) is used in the Authorization Platform and Percta payment transactions.

**Data Element Definitions****DE 112—Additional Data, National Use**

<b>Attributes</b>	
Subelement ID:	008
Length of Length Field:	023
Data Representation:	ans-23
Data Field:	Contents of positions 1–23
Subfields:	N/A
Justification:	N/A
<b>Values</b>	
Installment amount (positions 1–12)	Installment amount (with two decimal places) including any issuer-calculated interest, insurance, or other charges.
Due Date of First Installment (positions 13–18)	Due Date of First Installment (in binary format: ddmmyyyy)
Finance currency code (positions 19–21)	This is the currency in which the issuer will finance the transaction.  This specifies the currency used in installment amount, above 604 (Peru Nuevo Sol) or 840 (United States dollar)
Payment Plan (positions 22–23)	Reserved for future use. Insert all zeros.

## **Philippines—Payment Transactions**

Following are the technical specifications for Authorization/01xx messages for Philippines payment transactions.

### **Subelement 009—Installment Payment Data**

Subelement 009 (Installment Payment Data) is used in the Authorization System for Philippines payment transactions.

<b>Attributes</b>	
Subelement ID:	009
Length of Length Field:	3
Data Representation:	n-33
Data Field:	Contents of Positions 1–33
Subfields:	N/A
Justification:	Right with leading zeros

#### **Usage**

Following is the usage of subelement 009 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	CE	•	CE
Authorization Advice/0120—Issuer-generated	C	C	•
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE

#### **Values**

Installment type (positions 1–2)	Type of installment contains a type of installment. In the case of Philippines installments, merchant-finance (21) is the only type of installment.
Number of installments (positions 3–4)	Number of installments contains the number of installments selected by the cardholder. In case of Philippines the valid values are 02–24.
Interest rate (positions 5–9)	Interest rate contains the interest rate (2 decimal) that the issuer charges the cardholder for the installment payments. Default rate is 0% ('00000').
First installment amount (positions 10–21)	First installment amount contains the amount of the first installment.
Subsequent installment amount (positions 22–33)	Subsequent installment amount contains the amount of the subsequent installment.

## **UK Domestic Maestro Transactions**

Following are the technical specifications for Authorization/01xx messages for DE 112 for UK Domestic Maestro (UKDM) transactions.

### **Subelement 001—Reason Online Code**

DE 112, UK Domestic Maestro, subelement 001 (Reason Online code) is used in the Authorization Platform for UKDM transactions.

#### **Attributes**

Subelement ID:	001
Length of Length Field:	3

## Data Element Definitions

### DE 112—Additional Data, National Use

---

Data Representation: ns-2

Data Field: Contents of positions 1–2

Subfields: N/A

Justification: N/A

#### **Values**

Additional retailer data provided by the acquirer.

#### **Application Notes**

Mandatory for acquirers to insert in Authorization Request/0100 messages, and must not be included in other message types. It contains additional retailer data provided by the acquirer to identify the reason, provided by the terminal, why a transaction goes online (always present for transactions coming from ICC terminals). Refer to APACS 30/40 standards for the list of reason online codes. If this field is not present in a message from a terminal, the default value is spaces.

---

## **Subelement 002—Retailer Classification Code**

DE 112, UK Domestic Maestro, subelement 002 (Retailer Classification Code) is used in the Authorization Platform for UKDM transactions.

---

#### **Attributes**

Subelement ID: 002

Length of Length Field: 3

Data Representation: n-4

Data Field: Contents of positions 1–4

Subfields: N/A

Justification: N/A

---

#### **Values**

The retailer classification code consists of three-digits and one-digit filler of 0. The “0” filler comes at the end of the RCC. For information about all retailer classification codes (RCCs), see the *Reference Guide for UK Domestic Maestro*.

---

#### **Application Notes**

Mandatory for acquirers to insert in Authorization Request/0100 messages. The retailer classification code consists of three digits and one digit filler of 0. The “0” filler comes at the end of the RCC.

---

The following Authorization System edits will apply only to UK Domestic Maestro transactions.

---

**WHEN...**

**THEN the Authorization System...**

DE 112, subfield 001 and 002 are not present in the Authorization Request/0100 message	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format Error)</li><li>• DE 44 (Additional Response Data) = 112</li></ul>
The issuer does not respond to the Authorization Request/0100 message or does not respond within time limits	Sends the acquirer an Authorization Request Response/0110 message where DE 39 contains value 91 (Authorization System or Issuer Inoperative) and Sends the issuer a Reversal Advice/0420 message where DE 39 contains value 82 (Timeout at issuer).

## DE 113—Reserved for National Use

MasterCard recommends that DE 113 contain Application Generic Data and Application Banking Data. This data element is typically present for consumer and business application requests, counteroffer replies, and pre-approved offer inquiries.

---

### Attributes

---

Data Element ID:	113
Length of Length Field:	3
Data Representation:	ans...999; LLIVAR
Data Field:	Contents of positions 1–999
Subfields:	N/A
Justification:	N/A

---

### Usage

---

Following is the usage of DE 113 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Administrative Request/0600	C	•	C
Administrative Request Response/0610	C	•	C

---

### Application Notes

---

MasterCard edits DE 113 for valid attributes but does not edit or log data contents.  
At least one of DE 113–119 is mandatory within Administrative 0600/0610 messages.

---

### Recommended Format Construction

---

**Data Element Definitions**  
**DE 113—Reserved for National Use**

---

113LLL<field\_name>data<field\_name>data...<field\_name>data

113 is data element number

LLL is total length of all field names, separators and data

< indicates start of field\_name

field\_name is unique name for each field

> indicates end of field\_name

---

## **Generic Data, Administrative Request/0600 Message**

DE 113, Generic Data, may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
client_id	16	Unique identifier of credit client
store_code	16	Unique identifier of each store location
credit_unit	5	Credit unit designation
appl_source_type	3	Origin of application
source_code	19	Application source code
appl_source.empid	11	Employee ID that obtained application request
appl_type	1	<ul style="list-style-type: none"><li>• C = Consumer</li><li>• B = Business</li></ul>
account_type	1	For Business applications use: <ul style="list-style-type: none"><li>• R = Revolving</li><li>• N = Non-revolving</li><li>• I = Installment</li><li>• P = Invoice/Net Pay</li><li>• M = Co-Brand</li></ul> For Consumer applications use: <ul style="list-style-type: none"><li>• 1 = Individual</li><li>• 2 = Joint</li><li>• 3 = Authorized Buyer</li></ul>
language_pref	3	<ul style="list-style-type: none"><li>• ENG = English</li><li>• SPA = Spanish</li><li>• FRE = French</li><li>• and other supported ISO 639 codes</li></ul>

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
sale_pending_amt	12	Amount of initial sale
credit_limit_req_amt	12	Amount of requested credit limit
single_purch_limit	12	Amount limit per purchase
bill_addr1	25	Billing address line 1
bill_addr2	25	Billing address line 2
bill_city	20	Billing city
bill_sub_ctry	2	Billing subnational entity alpha abbreviation; for example U.S. state code abbreviations
bill_post_code	10	Billing postal code
bill_ctry	3	Billing country alpha abbreviation
bill_phone_nbr	15	Billing phone number
bill_email_addr	54	Billing e-mail address
membership_nbr	16	Unique identifier of member or customer
correlation_id	16	Correlation identifier may be assigned when response to application response is status O
reference_nbr	13	Reference number assigned to original application
offer_accept_ind	1	Y or N indicates acceptance of counteroffer
temp_pass_days	2	Number of days requested for a temporary charge pass
pre_approval_nbr	13	Preapproval reference number

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

---

#### **Usage**

Application Generic Data recommended usage when:

- DE 60 = 6500080 (Consumer Application Request)
  - DE 60 = 6500085 (Consumer Counteroffer Reply)
  - DE 60 = 6500090 (Business Application Request)
  - DE 60 = 6500095 (Business Counteroffer Reply)
-

## **Banking Data, Administrative Request/0600 Message**

DE 113, Banking Data, may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
bank_name	35	Name of bank
bank_addr1	25	Bank address line 1
bank_addr2	25	Bank address line 2
bank_city	20	Bank city
bank_sub_ctry	2	Bank subnational entity alpha abbreviation; for example U.S. state code abbreviations
bank_post_code	10	Bank postal code
bank_ctry	3	Bank country alpha abbreviation
bank_phone_nbr	15	Bank phone number
checking_acct_nbr	17	Checking account number
savings_acct_nbr	17	Savings account number

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

---

### **Usage**

Application Banking Data recommended usage when:

- DE 60 = 6500080 (Consumer Application Request)
- DE 60 = 6500090 (Business Application Request)

---

## **DE 114—Reserved for National Use**

MasterCard recommends that DE 114 contain Consumer Application Data or Consumer Maintenance Data. This data element is typically present for consumer application requests, application status inquiries, preapproved offer inquiries, or consumer maintenance requests as well as consumer application or consumer maintenance responses. DE 114 also may be present for business application requests that require a personal guarantee.

---

### **Attributes**

Data Element ID:	114
Length of Length Field:	3
Data Representation:	ans...999; LLLVAR

Data Field:	Contents of positions 1–999
Subfields:	N/A
Justification:	N/A

#### **Usage**

Following is the usage of DE 114 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages.

	Org	Sys	Dst
Administrative Request/0600	C	•	C
Administrative Request Response/0610	C	•	C

#### **Application Notes**

MasterCard edits DE 114 for valid attributes but does not edit or log data contents.  
At least one of DE 113–119 is mandatory within Administrative 0600/0610 messages.

#### **Recommended Format Construction**

114LLL<field\_name>data<field\_name>data...<field\_name>data

114 is data element number

LLL is total length of all field names, separators and data

< indicates start of field\_name

field\_name is unique name for each field

> indicates end of field\_name

## **Consumer Application Request Data Administrative Request/0600 Message**

DE 114, Consumer Application Request Data, may contain the following fields.

Field Name	Max Length	Description
cons_first_name	15	Consumer's first name
cons_middle_initial	1	Consumer's middle initial
cons_last_name	20	Consumer's last name
cons_suffix	6	Consumer's suffix; SR, JR, III, PHD, etc.
birth_date	10	Consumer's date of birth; CCYY/MM/DD
national_id	20	Consumer's national identification number United States—use Social Security number
local_id_type	1	Consumer's local ID type

**Data Element Definitions**  
**DE 114—Reserved for National Use**

---

Field Name	Max Length	Description
	D	= Driver's license
	I	= Identification card
	O	= Other
local_id_location	2	Consumer's local ID location United States—use alpha state codes
local_id_nbr	24	Consumer's local ID number
home_addr1	25	Consumer's home address line 1
home_addr2	25	Consumer's home address line 2
home_city	20	Consumer's home city
home_sub_ctry	2	Consumer's home subnational entity alpha abbreviation; for example U.S. state code abbreviations
home_post_code	10	Consumer's home postal code
home_ctry	3	Consumer's home country alpha abbreviation
home_phone_nbr	15	Consumer's home phone number
rent_own_ind	1	Consumer's home status  B = Board or other  M = Military  O = Own  P = Live with parents or other relatives  R = Rent
residence_time	2	Number of years lived in current residence
prev_residence_time	2	Number of years lived in previous residence
prev home_addr1	25	Consumer's previous home address line 1
prev home_addr2	25	Consumer's previous home address line 2
prev_home_city	20	Consumer's previous home city
prev_home_sub_ctry	2	Consumer's previous home subnational entity alpha abbreviation; for example U.S. state code abbreviations
prev_home_post_code	10	Consumer's previous home postal code

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
prev_home_ctry	3	Consumer's previous home country alpha abbreviation
employment_time	2	Number of years employed by current employer
work_phone_nbr	15	Consumer's work phone number
annual_income_amt	12	Consumer's total annual income amount
credit_ins_ind	1	Y or N—Consumer's acceptance of credit insurance
card_qty	3	Quantity of cards requested
client_employee	1	Y or N—Is applicant an employee of client

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

#### **Usage**

Consumer Application Request Data recommended usage when:

- DE 60 = 6500080 (Consumer Application Request)
- DE 60 = 6500090 (Business Application Request)

## **Consumer Status Inquiry or Preapproved Offer Inquiry Data Administrative Request/0600 Message**

DE 114, Consumer Status Inquiry or Preapproved Offer Inquiry Data may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
client_id	16	Unique identifier of credit client
store_code	16	Unique identifier of each store location
reference_nbr	13	Application reference number provided if available
cons_first_name	15	Consumer's first name
cons_middle_initial	1	Consumer's middle initial
cons_last_name	20	Consumer's last name
cons_suffix	6	Consumer's suffix; SR, JR, III, PHD, etc.
birth_date	10	Consumer's date of birth; CCYY/MM/DD

**Data Element Definitions**  
**DE 114—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
national_id	20	Consumer's national identification number United States—use Social Security number
local_id_nbr	24	Consumer's local ID number United States—use driver's license or other ID
home_phone_nbr	15	Consumer's home phone number
pre_approval_nbr	13	Preapproved reference number
temp_pass_days	2	Number of days requested for a temporary charge pass

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

---

**Usage**

---

Consumer Application Inquiry Data recommended usage when:

- DE 60 = 6500081 (Consumer Application Status Inquiry)
  - DE 60 = 6500086 (Consumer Preapproved Offer Inquiry)
- 

## **Consumer Account Maintenance Data Administrative Request/0600 Message**

DE 114, Consumer Account Maintenance Data may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
client_id	16	Unique identifier of credit client
store_code	16	Unique identifier of each store location
account_nbr	19	Consumer account number
account_status	1	Update account status only to I = Inactive
cons_first_name	15	Update consumer's first name
cons_middle_initial	1	Update consumer's middle initial
cons_last_name	20	Update consumer's last name
cons_suffix	6	Update consumer's suffix; SR, JR, III, PHD, etc.
local_id_type	1	Update consumer's local ID type

**Data Element Definitions**  
**DE 114—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
		D = Driver's license
		I = Identification card
		O = Other
local_id_location	2	Update consumer's local ID location United States—use alpha State codes
local_id_nbr	24	Update consumer's local ID number
home_addr1	25	Update consumer's home address line 1
home_addr2	25	Update consumer's home address line 2
home_city	20	Update consumer's home city
home_sub_ctry	2	Update consumer's home subnational entity alpha abbreviation; for example U.S. state code abbreviations
home_post_code	10	Update consumer's home postal code
home_ctry	3	Update consumer's home country alpha abbreviation
home_phone_nbr	15	Update consumer's home phone number
bill_addr1	25	Update billing address line 1
bill_addr2	25	Update billing address line 2
bill_city	20	Update billing city
bill_sub_ctry	2	Update billing subnational entity alpha abbreviation; for example U.S. state code abbreviations
bill_post_code	10	Update billing postal code
bill_ctry	3	Update billing country alpha abbreviation
bill_phone_nbr	15	Update billing phone number
bill_email_addr	54	Update billing e-mail address
work_phone_nbr	15	Update consumer's work phone number
bank_name	35	Update name of bank
bank_addr1	25	Update bank address line 1
bank_addr2	25	Update bank address line 2
bank_city	20	Update bank city

**Data Element Definitions**  
**DE 114—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
bank_sub_ctry	2	Update bank subnational entity alpha abbreviation; for example U.S. state code abbreviations
bank_post_code	10	Update bank postal code
bank_ctry	3	Update bank country alpha abbreviation
Consumer Account Maintenance Data recommended usage when:  DE 60 = 6500084 (Consumer Account Maintenance Request)	17	Update checking account number
savings_acct_nbr	17	Update savings account number
credit_ins_ind	1	Update Y or N consumer's acceptance of credit insurance
annual_income_amt	12	Update consumer's total annual income amount
language_pref	3	ENG = English, SPA = Spanish, FRE = French, and other supported ISO 639 codes
Repeat following User information as necessary for multiple users.		
user_function	1	A = Add, D = Delete
user_first_name	15	User's first name
user_middle_initial	1	User's middle initial
user_last_name	20	User's last name
user_suffix	6	User's suffix; SR, JR, III, PHD, etc.
The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.		
<b>Usage</b>	15	Update bank phone number
reference_nbr	13	Reference number assigned to each application
appl_source_type	3	Origin of application
cons_first_name	15	Consumer's first name
cons_middle_initial	1	Consumer's middle initial

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
cons_last_name	20	Consumer's last name
cons_suffix	6	Consumer's suffix; SR, JR, III, PHD, etc.
home_addr1	25	Consumer's home address line 1
home_addr2	25	Consumer's home address line 2
home_city	20	Consumer's home city
home_sub_ctry	2	Consumer's home subnational entity alpha abbreviation; for example U.S. state code abbreviations
home_post_code	10	Consumer's home postal code
home_ctry	3	Consumer's home country alpha abbreviation
home_phone_nbr	15	Consumer's home phone number
language_pref	3	ENG = English, SPA = Spanish, FRE = French, and other supported ISO 639 codes
temp_pass_exp_date	10	Expiration date of the temporary charge pass; format CCYY/MM/DD
appl_status	1	A = Approved D = Declined C = Call O = Counteroffer P = Pending M = Mail-based Offer Approved
account_nbr	19	Account number present if status = A
credit_limit_amt	12	Credit limit amount present if status = A or O

## **Consumer Application Response Data Administrative Request Response/0610 Message**

DE 114, Consumer Application Response Data may contain the following fields.

**Data Element Definitions**  
**DE 114—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
reference_nbr	13	Reference number assigned to each application
appl_source_type	3	Origin of application
cons_first_name	15	Consumer's first name
cons_middle_initial	1	Consumer's middle initial
cons_last_name	20	Consumer's last name
cons_suffix	6	Consumer's suffix; SR, JR, III, PHD, etc.
home_addr1	25	Consumer's home address line 1
home_addr2	25	Consumer's home address line 2
home_city	20	Consumer's home city
home_sub_ctry	2	Consumer's home subnational entity alpha abbreviation; for example U.S. state code abbreviations
home_post_code	10	Consumer's home postal code
home_ctry	3	Consumer's home country alpha abbreviation
home_phone_nbr	15	Consumer's home phone number
language_pref	3	ENG = English, SPA = Spanish, FRE = French, and other supported ISO 639 codes
temp_pass_exp_date	10	Expiration date of the temporary charge pass;format CCYY/MM/DD
appl_status	1	A = Approved D = Declined C = Call O = Counteroffer P = Pending M = Mail-based Offer Approved
account_nbr	19	Account number present if status = A
credit_limit_amt	12	Credit limit amount present if status = A or O

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
card_expiry_date	4	Card expiration date may be present if status = A; format YYMM
credit_phone_nbr	15	Phone number may be present for application inquiries by customer or store
credit_terms	256	Credit terms may be present if applicable. Credit terms may include relevant information such as for revolving, non-revolving, or installment credit account.
correlation_id	16	Correlation identifier may be assigned when response to application request is status O
pre_approval_nbr	13	Preapproval reference number
pre_appr_end_date	10	Expiration date of the pre approval offer; format CCYY/MM/DD

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

#### **Usage**

Consumer Application Response Data recommended usage when:

- DE 60 = 6500080 (Consumer Application Request)
- DE 60 = 6500081 (Consumer Application Status Inquiry)
- DE 60 = 6500085 (Consumer Counteroffer Reply)
- DE 60 = 6500086 (Consumer Preapproved Offer Inquiry)

## **Consumer Account Maintenance Data Administrative Request Response/0610 Message**

DE 114, Consumer Account Maintenance Data may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
account_nbr	19	Consumer account number
account_status_maint	1	S = successful, U = unsuccessful
account_status	1	Update account status only to I = Inactive
cons_first_name_maint	1	S = successful, U = unsuccessful
cons_first_name	15	Update consumer's first name

**Data Element Definitions**  
**DE 114—Reserved for National Use**

---

Field Name	Max Length	Description
cons_middle_initial_maint	1	S = successful, U = unsuccessful
cons_middle_initial	1	Update consumer's middle initial
cons_last_name_maint	1	S = successful, U = unsuccessful
cons_last_name	20	Update consumer's last name
cons_suffix_maint	1	S = successful, U = unsuccessful
cons_suffix	6	Update consumer's suffix; SR, JR, III, PHD, etc.
local_id_type_maint	1	S = successful, U = unsuccessful
local_id_type	1	Update consumer's local ID type
local_id_location_maint	1	S = successful, U = unsuccessful
local_id_location	2	Update consumer's local ID location
local_id_nbr_maint	1	S = successful, U = unsuccessful
local_id_nbr	24	Update consumer's local ID number
home_addr1_maint	1	S = successful, U = unsuccessful
home_addr1	25	Update consumer's home address line 1
home_addr2_maint	1	S = successful, U = unsuccessful
home_addr2	25	Update consumer's home address line 2
home_city_maint	1	S = successful, U = unsuccessful
home_city	20	Update consumer's home city
home_sub_ctry_maint	1	S = successful, U = unsuccessful
home_sub_ctry	2	Update home subnational entity alpha abbreviation; for example U.S. state code abbreviations
home_post_code_maint	1	S = successful, U = unsuccessful
home_post_code	10	Update consumer's home postal code
home_ctry_maint	1	S = successful, U = unsuccessful
home_ctry	3	Update consumer's home country alpha abbreviation
home_phone_nbr_maint	1	S = successful, U = unsuccessful
home_phone_nbr	15	Update consumer's home phone number
bill_addr1_maint	1	S = successful, U = unsuccessful

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
bill_addr1	25	Update billing address line 1
bill_addr2_maint	1	S = successful, U = unsuccessful
bill_addr2	25	Update billing address line 2
bill_city_maint	1	S = successful, U = unsuccessful
bill_city	20	Update billing city
bill_sub_ctry_maint	1	S = successful, U = unsuccessful
bill_sub_ctry	2	Update billing subnational entity alpha abbreviation; for example U.S. state code abbreviations
bill_post_code_maint	1	S = successful, U = unsuccessful
bill_post_code	10	Update billing postal code
bill_ctry_maint	1	S = successful, U = unsuccessful
bill_ctry	3	Update billing country alpha abbreviation
bill_phone_nbr_maint	1	S = successful, U = unsuccessful
bill_phone_nbr	15	Update billing phone number
bill_email_addr_maint	1	S = successful, U = unsuccessful
bill_email_addr	54	Update billing e-mail address
work_phone_nbr_maint	1	S = successful, U = unsuccessful
work_phone_nbr	15	Update consumer's work phone number
bank_name_maint	1	S = successful, U = unsuccessful
bank_name	35	Update name of bank
bank_addr1_maint	1	S = successful, U = unsuccessful
bank_addr1	25	Update bank address line 1
bank_addr2_maint	1	S = successful, U = unsuccessful
bank_addr2	25	Update bank address line 2
bank_city_maint	1	S = successful, U = unsuccessful
bank_city	20	Update bank city
bank_sub_ctry_maint	1	S = successful, U = unsuccessful
bank_sub_ctry	2	Update bank subnational entity alpha abbreviation; for example U.S. state code abbreviations

**Data Element Definitions**  
**DE 114—Reserved for National Use**

---

Field Name	Max Length	Description
bank_post_code_maint	1	S = successful, U = unsuccessful
bank_post_code	10	Update bank postal code
bank_ctry_maint	1	S = successful, U = unsuccessful
bank_ctry	3	Update bank country alpha abbreviation
bank_phone_nbr_maint	1	S = successful, U = unsuccessful
bank_phone_nbr	15	Update bank phone number
checking_acct_nbr_maint	1	S = successful, U = unsuccessful
checking_acct_nbr	17	Update checking account number
savings_acct_nbr_maint	1	S = successful, U = unsuccessful
savings_acct_nbr	17	Update savings account number
credit_ins_ind_maint	1	S = successful, U = unsuccessful
credit_ins_ind	1	Update Y or N consumer's acceptance of credit insurance
annual_income_amt_maint	1	S = successful, U = unsuccessful
annual_income_amt	12	Update consumer's total annual income amount
language_pref_maint	1	S = successful, U = unsuccessful
language_pref	3	ENG = English, SPA = Spanish, FRE = French, and other supported ISO 639 codes
Repeat following User information as necessary for multiple users.		
user_function_maint	1	S = successful, U = unsuccessful
user_function	1	A=Add, D=Delete
user_first_name	15	User's first name
user_middle_initial	1	User's middle initial
user_last_name	20	User's last name
user_suffix	6	User's suffix; SR, JR, III, PHD, etc.
The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.		

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
<b>Usage</b>		Consumer Account Maintenance Data recommended usage when: DE 60 = 6500084 (Consumer Account Maintenance Request)

## DE 115—Reserved for National Use

MasterCard recommends that DE 115 contain Business Application Data or Business Maintenance Data. This data element is typically present for business application requests, application status inquiries, preapproved offer inquiries, or business maintenance requests as well as business application or business maintenance responses.

---

### Attributes

---

Data Element ID:	115
Length of Length Field:	3
Data Representation:	ans...999; LLLVAR
Data Field:	Contents of positions 1–999
Subfields:	N/A
Justification:	N/A

---

### Usage

---

Following is the usage of DE 115 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Administrative Request/0600	C	•	C
Administrative Request Response/0610	C	•	C

---

### Application Notes

---

MasterCard edits DE 115 for valid attributes but does not edit or log data contents. At least one DE 113–119 is mandatory within Administrative 0600/0610 messages.

---

### Recommended Format Construction

---

115LLL<field\_name>data<field\_name>data...<field\_name>data

115 is data element number

LLL is total length of all field names, separators and data

< indicates start of field\_name

field\_name is unique name for each field

> indicates end of field\_name

## **Business Application Request Data Administrative Request/0600 Message**

DE 115, Business Application Request Data may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>		
bus_lgl_name	24	Business legal name		
doing_bus_as_name	40	Doing business as name		
bus_addr1	25	Business address line 1		
bus_addr2	25	Business address line 2		
bus_city	20	Business city		
bus_sub_ctry	2	Business subnational entity alpha abbreviation; for example U.S. state code abbreviations		
bus_post_code	10	Business postal code		
bus_ctry	3	Business country alpha abbreviation		
bus_phone_nbr	15	Business phone number		
bill_contact_name	19	Business billing contact name such as Accounts Payable or individual name		
annual_rev_amt	12	Business total annual revenue amount		
employee_qty	6	Number of business employees		
sic	8	Standard Industry Code		
lgl_structure	1	C	=	Corporation
		P	=	Partnership
		S	=	Sole Proprietorship
		L	=	Limited Liability Corp
		D	=	Limited Partnership
		blank	=	Unknown or all other
corp_structure	1	F	=	Fortune 1000
		G	=	Government (national and local)
		P	=	Professional
		N	=	Non-profit
		R	=	Religious

**Data Element Definitions**  
**DE 115—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>			<b>Description</b>
		blank	=	Unknown or all other
bus_structure	1	B	=	Branch of parent organization
		P	=	Parent organization
		I	=	Independent organization
in_business_since	4	Year that business started		
tax_exempt	1	Y if exempt from local taxes; N if not exempt		
tax_id	30	National government tax identifier		
po_req	1	Y if purchase order required; N if not required		
card_qty	3	Quantity of cards requested		
purchase_instructions	40	Contains special instructions applicable to purchases		
signature_first_name	15	First name of person submitting business application		
signature_mid_initial	1	Middle initial of person submitting business application		
signature_last_name	20	Last name of person submitting business application		
signature_title	15	Title of person submitting business application		
signature_present	1	Y or N—Signature of person submitting business application present on physical application		
guar_signature_ind	1	Y or N—Personal guarantor signature present		
guar_signature_date	10	Expiration date of the temporary charge pass; format CCYY/MM/DD		
fax_info_sent	1	Y or N—Additional information sent via fax, such as list of authorized buyers, financial statement, etc.		

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

**Data Element Definitions**  
**DE 115—Reserved for National Use**

---

Field Name	Max Length	Description
<b>Usage</b>		
Business Application Data recommended usage when: DE 60 = 6500090 (Business Application Request)		

## **Business Application Status Inquiry Data or Business Preapproved Offer Inquiry Data Administrative Request/0600 Message**

DE 115, Business Application Status Inquiry Data or Business Preapproved Offer Inquiry Data may contain the following fields.

Field Name	Max Length	Description
client_id	16	Unique identifier of credit client
store_code	16	Unique identifier of each store location
reference_nbr	13	Application reference number if available
bus_lgl_name	24	Business legal name
doing_bus_as_name	40	Doing business as name
tax_id	30	National government tax identifier
bus_phone_nbr	15	Business phone number
pre_approval_nbr	13	Preapproval reference number
temp_pass_days	2	Number of days requested for a temporary charge pass

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

<b>Usage</b>
Business Application Inquiry Data recommended usage when DE 60 = 6500091 (Business Application Status Inquiry) DE 60 = 6500096 (Business Preapproved Offer Inquiry)

## **Business Account Maintenance Data Administrative Request/0600 Message**

DE 115, Business Account Maintenance Data may contain the following fields.

**Data Element Definitions**  
**DE 115—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>		
client_id	16	Unique identifier of credit client		
store_code	16	Unique identifier of each store location		
account_nbr	19	Business account number		
account_status	1	Update account status only to "C" closed or canceled		
bus_lgl_name	24	Update business legal name		
doing_bus_as_name	40	Update doing business as name		
bus_addr1	25	Update business address line 1		
bus_addr2	25	Update business address line 2		
bus_city	20	Update business city		
bus_sub_ctry	2	Update business subnational entity alpha abbreviation; for example U.S. state code abbreviations		
bus_post_code	10	Update business postal code		
bus_ctry	3	Update business country alpha abbreviation		
bus_phone_nbr	15	Update business phone number		
annual_rev_amt	12	Update business total annual revenue amount		
sic	8	Update standard industry code		
lgl_structure	1	C	=	Corporation
		P	=	Partnership
		L	=	Limited Liability Corp
		D	=	Limited Partnership
		S	=	Sole Proprietorship
		blank	=	Unknown or all other
corp_structure	1	F	=	Fortune 1000
		G	=	Government (national and local)
		P	=	Professional

**Data Element Definitions**  
**DE 115—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>	
		N	= Non-profit
		R	= Religious
		blank	= Unknown or all other
bus_structure	1	B	= Branch of parent organization
		P	= Parent organization
		I	= Independent organization
tax_exempt	1	Update—Y if exempt from local taxes; N if not exempt	
tax_id	30	Update national government tax identifier	
po_req	1	Update—Y if purchase order required; N if not required	
card_qty	3	Update quantity of cards requested (additional cards)	
bill_addr1	25	Update billing address line 1	
bill_addr2	25	Update billing address line 2	
bill_city	20	Update billing city	
bill_sub_ctry	2	Update billing subnational entity alpha abbreviation; for example U.S. state code abbreviations	
bill_post_code	10	Update billing postal code	
bill_ctry	3	Update billing country alpha abbreviation	
bill_phone_nbr	15	Update billing phone number	
bill_contact_name	19	Update billing contact name such as Accounts Payable or individual name	
bill_email_addr	54	Update billing e-mail address	
bank_name	35	Update name of bank	
bank_addr1	25	Update bank address line 1	
bank_addr2	25	Update bank address line 2	
bank_city	20	Update bank city	

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
bank_sub_ctry	2	Update bank subnational entity alpha abbreviation; for example U.S. state code abbreviations
bank_post_code	10	Update bank postal code
bank_ctry	3	Update bank country alpha abbreviation
bank_phone_nbr	15	Update bank phone number
checking_acct_nbr	17	Update checking account number
savings_acct_nbr	17	Update savings account number
credit_ins_ind	1	Update Y or N business's acceptance of credit insurance
annual_income_amt	12	Update business's total annual income amount
single_purch_limit	12	Update amount limit per purchase
purchase_instructions	40	Update special instructions applicable to purchases
Repeat following User information as necessary for multiple users.		
user_function	1	A=Add, D=Delete
user_first_name	15	User's first name
user_middle_initial	1	User's middle initial
user_last_name	20	User's last name
user_suffix	6	User's suffix; SR, JR, III, PHD, etc.

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

#### **Usage**

Business Account Maintenance Data recommended usage when:  
DE 60 = 6500094 (Business Account Maintenance Request)

## **Business Application Response Data Administrative Request Response/0610 Message**

DE 115, Business Application Response Data may contain the following fields.

**Data Element Definitions**  
**DE 115—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
reference_nbr	13	Reference number assigned to each application
appl_source_type	3	Origin of application
account_type	1	R = Revolving, N = Non-revolving, I = Installment, P = Invoice/Net Pay, M = Co-Brand
bus_lgl_name	24	Business legal name
doing_bus_as_name	40	Doing business as name
bus_addr1	25	Business address line 1
bus_addr2	25	Business address line 2
bus_city	20	Business city
bus_sub_ctry	2	Business subnational entity alpha abbreviation; for example U.S. state code abbreviations
bus_post_code	10	Business postal code
bus_ctry	3	Business country alpha abbreviation
bus_phone_nbr	15	Business phone number
bill_contact_name	19	Business billing contact name such as Accounts Payable or individual name
po_req	1	Y if purchase order required; N if not required
purchase_instructions	40	Contains special instructions applicable to purchases
language_pref	3	ENG = English, SPA = Spanish, FRE = French, and other supported ISO 639 codes
temp_pass_exp_date	10	Expiration date of the temporary charge pass; format CCYY/MM/DD
fax_info_sent	1	Y or N—Additional information sent via fax, such as list of authorized buyers, financial statement, etc.
fax_info_rcvd	1	Y or N—Additional information received via fax, such as list of authorized buyers, financial statement, etc.
appl_status	1	A = Approved D = Declined C = Call

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
		O = Counteroffer
		P = Pending
account_nbr	19	Account number present if status = A
credit_limit_amt	12	Credit limit amount present if status = A or O
card_expiry_date	4	Card expiration date may be present if status = A; format YYMM
credit_phone_nbr	15	Phone number may be present for application inquiries by customer or store.
credit_terms	256	Credit terms may be present if applicable. Credit terms may include relevant information such as for revolving, non-revolving, or installment credit account.
correlation_id	16	Correlation identifier may be assigned when response to application request is status O
pre_approval_nbr	13	Preapproval reference number
pre_appr_end_date	10	Expiration date of the pre approval offer; format CCYY/MM/DD

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

#### **Usage**

Business Application Response Data recommended usage when:

- DE 60 = 6500090 (Business Application Request)
- DE 60 = 6500091 (Business Application Status Inquiry)
- DE 60 = 6500095 (Business Counteroffer Reply)
- DE 60 = 6500096 (Business Preapproved Offer Inquiry)

## **Business Account Maintenance Data Administrative Request Response/0610 Message**

DE 115, Business Account Maintenance Data may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
account_nbr	19	Consumer account number
account_status_maint	1	S = successful, U = unsuccessful

**Data Element Definitions**  
**DE 115—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
account_status	1	Update account status only to C closed or canceled
bus_lgl_name_maint	1	S = successful, U = unsuccessful
bus_lgl_name	24	Business legal name
doing_bus_as_name_maint	1	S = successful, U = unsuccessful
doing_bus_as_name	40	Doing business as name
bus_addr1_maint	1	S = successful, U = unsuccessful
bus_addr1	25	Business address line 1
bus_addr2_maint	1	S = successful, U = unsuccessful
bus_addr2	25	Business address line 2
bus_city_maint	1	S = successful, U = unsuccessful
bus_city	20	Business city
bus_sub_ctry_maint	1	S = successful, U = unsuccessful
bus_sub_ctry	2	Business subnational entity alpha abbreviation; for example U.S. state code abbreviations
bus_post_code_maint	1	S = successful, U = unsuccessful
bus_post_code	10	Business postal code
bus_ctry_maint	1	S = successful, U = unsuccessful
bus_ctry	3	Business country alpha abbreviation
bus_phone_nbr_maint	1	S = successful, U = unsuccessful
bus_phone_nbr	15	Business phone number
annual_rev_amt_maint	1	S = successful, U = unsuccessful
annual_rev_amt	12	Business total annual revenue amount
sic_maint	1	S = successful, U = unsuccessful
sic	8	Standard Industry Code
lgl_structure_maint	1	S = successful, U = unsuccessful
lgl_structure	1	C = Corporation P = Partnership L = Limited Liability Corp

**Data Element Definitions**  
**DE 115—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>	
		D	= Limited Partnership
		S	= Sole Proprietorship
		blank	= Unknown or all other
corp_structure_maint	1	S = successful, U = unsuccessful	
corp_structure	1	F	= Fortune 1000
		G	= Government (national and local)
		P	= Professional
		N	= Non-profit
		R	= Religious
		blank	= Unknown or all other
bus_structure_maint	1	S = successful, U = unsuccessful	
bus_structure	1	B	= Branch of parent organization
		P	= Parent organization
		I	= Independent organization
tax_exempt_maint	1	S = successful, U = unsuccessful	
tax_exempt	1	Y if exempt from local taxes; N if not exempt	
tax_id_maint	1	S = successful, U = unsuccessful	
tax_id	30	National government tax identifier	
po_req_maint	1	S = successful, U = unsuccessful	
po_req	1	Y if purchase order required; N if not required	
card_qty_maint	1	S = successful, U = unsuccessful	
card_qty	3	Quantity of cards requested (additional cards)	
bill_addr1_maint	1	S = successful, U = unsuccessful	
bill_addr1	25	Update billing address line 1	
bill_addr2_maint	1	S = successful, U = unsuccessful	
bill_addr2	25	Update billing address line 2	
bill_city_maint	1	S = successful, U = unsuccessful	

**Data Element Definitions**  
**DE 115—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
bill_city	20	Update billing city
bill_sub_ctry_maint	1	S = successful, U = unsuccessful
bill_sub_ctry	2	Update billing subnational entity alpha abbreviation; for example U.S. state code abbreviations
bill_post_code_maint	1	S = successful, U = unsuccessful
bill_post_code	10	Update billing postal code
bill_ctry_maint	1	S = successful, U = unsuccessful
bill_ctry	3	Update billing country alpha abbreviation
bill_phone_nbr_maint	1	S = successful, U = unsuccessful
bill_phone_nbr	15	Update billing phone number
bill_contact_name_maint	1	S = successful, U = unsuccessful
bill_contact_name	19	Update billing contact name such as Accounts Payable or individual name
bill_email_addr_maint	1	S = successful, U = unsuccessful
bill_email_addr	54	Update billing e-mail address
bank_name_maint	1	S = successful, U = unsuccessful
bank_name	35	Update name of bank
bank_addr1_maint	1	S = successful, U = unsuccessful
bank_addr1	25	Update bank address line 1
bank_addr2_maint	1	S = successful, U = unsuccessful
bank_addr2	25	Update bank address line 2
bank_city_maint	1	S = successful, U = unsuccessful
bank_city	20	Update bank city
bank_sub_ctry_maint	1	S = successful, U = unsuccessful
bank_sub_ctry	2	Update bank subnational entity alpha abbreviation; for example U.S. state code abbreviations
bank_post_code_maint	1	S = successful, U = unsuccessful
bank_post_code	10	Update bank postal code
bank_ctry_maint	1	S = successful, U = unsuccessful

**Data Element Definitions**  
**DE 115—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
bank_ctry	3	Update bank country alpha abbreviation
bank_phone_nbr_maint	1	S = successful, U = unsuccessful
bank_phone_nbr	15	Update bank phone number
checking_acct_nbr_maint	1	S = successful, U = unsuccessful
checking_acct_nbr	17	Update checking account number
savings_acct_nbr_maint	1	S = successful, U = unsuccessful
savings_acct_nbr	17	Update savings account number
credit_ins_ind_maint	1	S = successful, U = unsuccessful
credit_ins_ind	1	Update Y or N business's acceptance of credit insurance
annual_income_amt_maint	1	S = successful, U = unsuccessful
annual_income_amt	12	Update business's total annual income amount
single_purch_limit_maint	1	S = successful, U = unsuccessful
single_purch_limit	12	Update amount limit per purchase
purchase_instructions_maint	1	S = successful, U = unsuccessful
purchase_instructions	40	Contains special instructions applicable to purchases
Repeat following User information as necessary for multiple users.		
user_function_maint	1	S = successful, U = unsuccessful
user_function	1	A=Add, D=Delete
user_first_name	15	User's first name
user_middle_initial	1	User's middle initial
user_last_name	20	User's last name
user_suffix	6	User's suffix; SR, JR, III, PHD, etc.
The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.		

## Data Element Definitions

### DE 116—Reserved For National Use

---

Field Name	Max Length	Description
<b>Usage</b>		Business Account Maintenance Data recommended usage when: DE 60 = 6500094 (Business Account Maintenance Request)

## DE 116—Reserved For National Use

MasterCard recommends that DE 116 contain Consumer User Lookup Data and Consumer Account Lookup Data. This data element is typically present to request consumer user and account information and provide consumer user account information.

---

### Attributes

---

Data Element ID:	116
Length of Length Field:	3
Data Representation:	ans...999; LLLVAR
Data Field:	Contents of positions 1-999
Subfields:	N/A
Justification:	N/A

---

### Usage

---

Following is the usage of DE 116 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Administrative Request/0600	C	•	C
Administrative Request Response/0610	C	•	C

---

### Application Notes

---

MasterCard edits DE 116 for valid attributes but does not edit or log data contents. At least one of DE 113–119 is mandatory within Administrative 0600/0610 messages.

---

### Recommended Format Construction

---

116LLL<field\_name>data<field\_name>data...<field\_name>data

116 is data element number

LLL is total length of all field names, separators and data

< indicates start of field\_name

field\_name is unique name for each field

> indicates end of field\_name

## **Consumer User Lookup Inquiry Data Administrative Request/0600**

DE 116, Consumer User Lookup Inquiry may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
client_id	16	Unique identifier of credit client
store_code	16	Unique identifier of each store location
account_nbr	19	Account number
national_id	20	Consumer's national identification number United States—use Social Security number
cons_first_name	15	Consumer's first name
cons_middle_initial	1	Consumer's middle initial
cons_last_name	20	Consumer's last name
home_phone_nbr	15	Consumer's home phone number
user_list	1	Y = Request list of consumer account users (The maximum number of users to be provided will depend upon the client system as well as the 0610 maximum message length)

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

---

### **Usage**

Customer User Lookup Inquiry Data recommended usage when:

DE 60 = 6500082 (Consumer User Lookup Inquiry)

Note: DE 118 in 0610 response message contains the Authorized Users.

---

## **Consumer Account Lookup Inquiry Data Administrative Request/0600 Message**

DE 116, Consumer Account Lookup Inquiry Data may contain the following fields.

**Data Element Definitions**  
**DE 116—Reserved For National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
client_id	16	Unique identifier of credit client
store_code	16	Unique identifier of each store location
account_nbr	19	Account number
national_id	20	Consumer's national identification number United States—use Social Security number
cons_first_name	15	Consumer's first name
cons_middle_initial	1	Consumer's middle initial
cons_last_name	20	Consumer's last name
home_phone_nbr	15	Consumer's home phone number
user_first_name	15	User's first name
user_middle_initial	1	User's middle initial
user_last_name	20	User's last name
user_suffix	6	User's suffix; SR, JR, III, PHD, etc.

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

---

**Usage**

---

Customer Account Lookup Inquiry Data recommended usage when:  
DE 60 = 6500083 (Consumer Account Lookup Inquiry)

---

## **Consumer Account Lookup Response Data Administrative Request Response/0610 Message**

DE 116, Consumer Account Lookup Response Data may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
account_nbr	19	Account number
cons_first_name	15	Consumer's first name
cons_middle_initial	1	Consumer's middle initial
cons_last_name	20	Consumer's last name
home_addr1	25	Consumer's home address line 1

**Data Element Definitions**  
**DE 116—Reserved For National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
home_addr2	25	Consumer's home address line 2
home_city	20	Consumer's home city
home_sub_ctry	2	Consumer's home subnational entity alpha abbreviation; for example U.S. state code abbreviations
home_post_code	10	Consumer's home postal code
home_ctry	3	Consumer's home country alpha abbreviation
home_phone_nbr	15	Consumer's home phone number
work_phone_nbr	15	Consumer's work phone number
account_status	1	A = Active B = Blocked I = Inactive
credit_limit_amt	12	Credit limit amount
available_credit_amt	12	Available credit amount
bal_owe_amt	12	Balance owed amount
pay_owe_amt	12	Next payment owed amount
pay_due_date	10	Next payment due date; format CCYY/MM/DD
last_pay_amt	12	Last payment received amount
last_pay_date	10	Last payment received date CCYY/MM/DD
acct_open_date	10	Account open date; format CCYY/MM/DD
custsvc_phone_nbr	15	Customer service phone number may be present for account lookup inquiries by customer or store.
language_pref	3	ENG = English, SPA = Spanish, FRE = French, and other supported ISO 639 codes
credit_terms	256	Credit terms may be present if applicable. Credit terms may include relevant information such as for revolving, non-revolving, or installment credit account.

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

## Data Element Definitions

### DE 117—Reserved for National Use

---

Field Name	Max Length	Description
Usage		Customer Account Lookup Response Data recommended usage when: DE 60 = 65–83 (Consumer Account Lookup Inquiry).

## DE 117—Reserved for National Use

MasterCard recommends that DE 117 contain Business User Lookup Data and Business Account Lookup Data. This data element is typically present to request business user and account information and provide business user account information.

---

### Attributes

---

Data Element ID:	117
Length of Length Field:	3
Data Representation:	ans...999; LLLVAR
Data Field:	Contents of positions 1–999
Subfields:	N/A
Justification:	N/A

---

### Usage

---

Following is the usage of DE 117 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Administrative Request/0600	C	•	C
Administrative Request Response/0610	C	•	C

---

### Application Notes

---

MasterCard edits DE 117 for valid attributes but does not edit or log data contents.  
At least one of DE 113–119 is mandatory within Administrative 0600/0610 messages.

---

### Recommended Format Construction

---

117LLL<field\_name>data<field\_name>data...<field\_name>data

117 is data element number

LLL is total length of all field names, separators and data

< indicates start of field\_name

field\_name is unique name for each field

> indicates end of field\_name

## **Business User Lookup Inquiry Data Administrative Request/0600 Message**

DE 117, Business User Lookup Inquiry Data may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
client_id	16	Unique identifier of credit client
store_code	16	Unique identifier of each store location
account_nbr	19	Account number
tax_id	30	National government tax identifier
bus_lgl_name	24	Business legal name
doing_bus_as_name	40	Doing business as name
bus_phone_nbr	15	Business phone number
auth_user_id	5	ID assigned to authorized user
user_list	1	Y = Request list of consumer account users(the maximum number of users to be provided will depend upon the client system as well as the 0610 maximum message length)

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

---

### **Usage**

---

Business User Lookup Inquiry Data recommended usage when:

DE 60 = 6500092 (Business User Lookup Inquiry)

Note: DE 118 in 0610 response message contains the Authorized Users.

---

## **Business Account Lookup Inquiry Data Administrative Request/0600 Message**

DE 117, Business Account Lookup Inquiry Data may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
client_id	16	Unique identifier of credit client
store_code	16	Unique identifier of each store location
account_nbr	19	Account number
tax_id	30	National government tax identifier
bus_lgl_name	24	Business legal name

**Data Element Definitions**  
**DE 117—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
doing_bus_as_name	40	Doing business as name
bus_phone_nbr	15	Business phone number
auth_user_id	5	ID assigned to authorized user
user_first_name	15	User's first name
user_middle_initial	1	User's middle initial
user_last_name	20	User's last name
user_suffix	6	User's suffix; SR, JR, III, PHD, etc.
user_list	1	Y = Request list of consumer account users (the maximum number of users to be provided will depend upon the client system as well as the 0610 maximum message length)

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

---

**Usage**

---

Business Account Lookup Request Data recommended usage when:  
DE 60 = 6500093 (Business Account Lookup Inquiry)

---

## **Business Account Lookup Response Data Administrative Request Response/0610 Message**

DE 117, Business Account Lookup Response Data may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
account_nbr	19	Account number
tax_id	30	National government tax identifier
bus_lgl_name	24	Business legal name
doing_bus_as_name	40	Doing business as name
bus_addr1	25	Business address line 1
bus_addr2	25	Business address line 2
bus_city	20	Business city

**Data Element Definitions**  
**DE 117—Reserved for National Use**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
bus_sub_ctry	2	Business subnational entity alpha abbreviation; for example U.S. state code abbreviations
bus_post_code	10	Business postal code
bus_ctry	3	Business country alpha abbreviation
bus_phone_nbr	15	Business phone number
account_status	1	A = Active B = Blocked I = Inactive
credit_limit_amt	12	Credit limit amount
available_credit_amt	12	Available credit amount
bal_owe_amt	12	Balance owed amount
pay_owe_amt	12	Next payment owed amount
pay_due_date	10	Next payment due date; format CCYY/MM/DD
last_pay_amt	12	Last payment received amount
last_pay_date	10	Last payment received date CCYY/MM/DD
acct_open_date	10	Account open date; format CCYY/MM/DD
custsvc_phone_nbr	15	Customer service phone number may be present for account lookup inquiries by customer or store.
language_pref	3	ENG = English, SPA = Spanish, FRE = French, and other supported ISO 639 codes
credit_terms	256	Credit terms may be present if applicable. Credit terms may include relevant information such as for revolving, non-revolving, or installment credit account.
po_req	1	Y if purchase order required; N if not required
tax_exempt	1	Y if exempt from local taxes; N if not exempt
single_purch_limit	12	Amount limit per purchase

## Data Element Definitions

### DE 118—Reserved for National Use

---

Field Name	Max Length	Description
purchase_instructions	40	Contains special instructions applicable to purchases

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length.

---

#### Usage

---

Business Account Lookup Response Data recommended usage when:  
DE 60 = 6500093 (Business Account Lookup Inquiry)

---

## DE 118—Reserved for National Use

MasterCard recommends that DE 118 contain Authorized Users. This data element may be present for consumer and business application requests and lookup responses.

---

#### Attributes

---

Data Element ID:	118
Length of Length Field:	3
Data Representation:	ans...999; LLLVAR
Data Field:	Contents of positions 1–999
Subfields:	N/A
Justification:	N/A

---

#### Usage

---

Following is the usage of DE 118 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Administrative Request/0600	C	•	C
Administrative Request Response/0610	C	•	C

---

#### Application Notes

---

MasterCard edits DE 118 for valid attributes but does not edit or log data contents.  
At least one of DE 113–119 is mandatory within Administrative 0600/0610 messages.

---

#### Recommended Format Construction

---

---

118LLL<field\_name>data<field\_name>data...<field\_name>data

---

118 is data element number

LLL is total length of all field names, separators and data

< indicates start of field\_name

field\_name is unique name for each field

> indicates end of field\_name

---

## **Authorized User Data Administrative Request/0600 Message**

DE 118, Authorized User Data may contain the following fields.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
auth_user	0	The first field for each authorized user occurrence
user_first_name	15	User's first name
user_middle_initial	1	User's middle initial
user_last_name	20	User's last name
user_suffix	6	User's suffix; SR, JR, III, PHD, etc.
auth_user_id	5	ID assigned to authorized user

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length. The above fields may be repeated as necessary within this DE 118.

---

### **Usage**

Authorized User Data recommended usage when:

DE 60 = 6500080 (Consumer Application Request)

DE 60 = 6500090 (Business Application Request)

The number of users depends upon the client system as well as the 0610 maximum message length.

---

### **Field Usage Example**

Assume for two authorized users and no assigned auth user id:

<auth\_user> <user\_first\_name>John <user\_middle\_initial> Q <user\_last\_name>  
Public <user\_suffix>Mr <auth\_user> <user\_first\_name> Mary <user\_middle\_initial>J  
<user\_last\_name> Public <user\_suffix> Mrs

---

## **Trade Reference Data Administrative Request/0600 Message**

DE 118, Trade Reference may contain the following fields.

**Data Element Definitions**  
**DE 118—Reserved for National Use**

---

Field Name	Max Length	Description
trade_ref	0	The first field for each trade reference occurrence
trade_ref_name	40	Trade reference name
trade_ref_phone_nbr	15	Trade reference phone number
trade_ref_acct_nbr	28	Applicant's account number with trade reference

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length. The above fields may be repeated as necessary within this DE 118.

---

**Usage**

---

Authorized User Data recommended usage when:

DE 60 = 6500090 (Business Application Request)

The number of users depends upon the client system as well as the 0610 maximum message length.

---

**Field Usage Example**

---

Assume for two trade references:

```
<trade_ref> <trade_ref_name>BigCityHardware <trade_ref_phone_nbr> 18885555555  
<trade_ref_acct_nbr>00000000 <trade_ref> <trade_ref_name> MidCityHardware  
<trade_ref_phone_nbr>18005555555 <trade_ref_acct_nbr> 00000000
```

---

## **Authorized User Response Data Administrative Request/0610 Message**

DE 118, Authorized User Response Data may contain the following fields.

Field Name	Max Length	Description
auth_user	0	The header field for each occurrence
user_first_name	15	User's first name
user_middle_initial	1	User's middle initial
user_last_name	20	User's last name
user_suffix	6	User's suffix; SR, JR, III, PHD, etc.
auth_user_id	5	ID assigned to authorized user

The above fields are not required to be present. Additional fields may be present as needed. Fields need not be in any particular order. Fields may be less than specified maximum length. The above fields may be repeated as necessary within this DE 118.

---

**Usage**

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
Authorized User Data recommended usage when:		
<ul style="list-style-type: none"> <li>• DE 60 = 6500081 (Consumer Application Status Inquiry)</li> <li>• DE 60 = 6500082 (Consumer User Lookup Inquiry)</li> <li>• DE 60 = 6500083 (Consumer Account Lookup Inquiry)</li> <li>• DE 60 = 6500091 (Business Application Status Inquiry)</li> <li>• DE 60 = 6500092 (Business User Lookup Inquiry)</li> <li>• DE 60 = 6500093 (Business Account Lookup Inquiry).</li> <li>• The number of users depends upon the client system, as well as the 0610 maximum message length</li> </ul>		
<b>Field Usage Example</b>		
Assume for two authorized users and no assigned auth user id: <auth_user> <user_first_name>John <user_middle_initial> Q <user_last_name> Public <user_suffix>Mr <auth_user> <user_first_name> Mary <user_middle_initial>J <user_last_name> Public <user_suffix> Mrs		

## DE 119—Reserved for National Use

MasterCard is reserving DE 119 for customer-specific data and is not recommending any particular usage.

---

### Attributes

---

Data Element ID:	119
Length of Length Field:	3
Data Representation:	ans...999; LLLVAR
Data Field:	Contents of positions 1–999
Subfields:	N/A
Justification:	N/A

---

### Usage

---

Following is the usage of DE 119 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Administrative Request/0600	C	•	C
Administrative Request Response/0610	C	•	C

---

### Application Notes

---

## **Data Element Definitions**

### **Using DE 113–119 in Administrative 06xx Messages**

---

MasterCard edits DE 119 for valid attributes but does not edit or log data contents. At least one of DE 113–119 is mandatory within Administrative 0600/0610 messages.

#### **Recommended Format Construction**

119LLL<field\_name>data<field\_name>data...<field\_name>data

119 is data element number

LLL is total length of all field names, separators and data

< indicates start of field\_name

field\_name is unique name for each field

> indicates end of field\_name

---

## **Using DE 113–119 in Administrative 06xx Messages**

The following information explains how to use DE 113–119 in Administrative 0600/0610 messages. MasterCard recommends that the contents of DE 113–119 from 0600 message *not* be returned in the 0610 to avoid maximum message length constraint of 8k.

### **DE 60 = 6500080 Consumer Application Request**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	113	Recommended	Application Generic Data
0600	113	Recommended	Application Banking Data
0600	114	Recommended	Consumer Application Request Data
0600	118	Optional	Authorized User Data
0610	114	Recommended	Consumer Application Response Data

### **DE 60 = 6500081 Consumer Application Status Inquiry**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	114	Recommended	Consumer Application Status Inquiry Data
0610	114	Recommended	Consumer Application Response Data
0610	118	Optional	Authorized User Response Data

### **DE 60 = 6500082 Consumer User Lookup Inquiry**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	116	Recommended	Consumer User Lookup Inquiry Data
0610	118	Recommended	Authorized User Response Data

**DE 60 = 6500083 Consumer Account Lookup Inquiry**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	116	Recommended	Consumer Account Lookup Inquiry Data
0610	116	Recommended	Consumer Account Lookup Response Data
0610	118	Optional	Authorized User Response Data

**DE 60 = 6500084 Consumer Account Maintenance Request**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	114	Recommended	Consumer Account Maintenance Data
0610	114	Recommended	Consumer Account Maintenance Data

**DE 60 = 6500085 Consumer Counteroffer Reply**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	113	Recommended	Application Generic Data
0610	114	Recommended	Consumer Application Response Data

**DE 60 = 6500086 Consumer Preapproved Offer Inquiry**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	114	Recommended	Consumer Application Status Inquiry Data
0610	114	Recommended	Consumer Application Response Data

**DE 60 = 6500090 Business Application Request**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	113	Recommended	Application Generic Data
0600	113	Recommended	Application Banking Data
0600	114	Optional	Consumer Application Request
0600	115	Recommended	Business Application Request Data
0600	118	Optional	Authorized User Data
0600	118	Optional	Trade Reference Data
0610	115	Recommended	Business Application Response Data

**Data Element Definitions**  
**Using DE 113–119 in Administrative 06xx Messages**

---

**DE 60 = 6500091 Business Application Status Inquiry**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	115	Recommended	Business Application Status Inquiry Data
0610	115	Recommended	Business Application Response Data
0610	118	Optional	Authorized User Response Data

**DE 60 = 6500092 Business User Lookup Inquiry**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	117	Recommended	Business User Lookup Inquiry Data
0610	118	Recommended	Authorized User Response Data

**DE 60 = 6500093 Business Account Lookup Inquiry**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	117	Recommended	Business Account Lookup Inquiry Data
0610	117	Recommended	Business Account Lookup Response Data
0610	118	Optional	Authorized User Response Data

**DE 60 = 6500094 Business Account Maintenance Request**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	115	Recommended	Business Account Maintenance Data
0610	115	Recommended	Business Account Maintenance Data

**DE 60 = 6500095 Business Counteroffer Reply**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	113	Recommended	Application Generic Data
0610	115	Recommended	Business Application Response Data

**DE 60 = 6500096 Business Preapproved Offer Inquiry**

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
0600	115	Recommended	Business Application Status Inquiry Data
0610	115	Recommended	Business Application Response Data

## DE 120—Record Data

DE 120 (Record Data) is a variable-length data element used for transmitting file record data or textual character string data in various message types.

### Attributes

Length of Length Field:	3
Data Representation:	ans...999; LLLVAR (supports extended character sets)
Data Field:	Contents of subfields 1, or 2, or 3, or 4
Subfields:	4
Justification:	See “Subfields”

### Usage

Following is the usage of DE 120 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	X	C
Authorization Request Response/0110	C	X	C
Issuer File Update Request/0302	C	C	•
Issuer File Update Request Response/0312	•	C	C
Administrative Advice/0620—System-generated	•	C	C
Administrative Advice/0620—Member-generated	C	•	C

### Values

See “Subfields”

### Application Notes

The following applies to DE 120:

#### Authorization Request/0100—AVS messages

When DE 120 is present in Authorization Request/0100 messages, DE 120 contains Address Verification Service data. Only one of the four possible subfields will be present in a message from an acquirer or to an issuer. In Authorization Request Response/0110—AVS messages, DE 120 contains the AVS data originally provided in the Authorization Request/0100 message.

#### Issuer File Update Request/0302 messages

When DE 120 is present in Issuer File Update Request/0302 messages, DE 120 contains the new, actual file record data used in “add” or “change” file maintenance requests. In Issuer File Update Request Response/0312 messages, DE 120 contains actual record data for file maintenance requests.

## Data Element Definitions

### DE 120—Record Data

---

#### Administrative Advice/0620 messages

---

When DE 120 is present in Administrative Advice/0620 messages, DE 120 contains the following:

- In Administrative Advice/0620—System-generated message where DE 60 is 600, DE 120 contains the first 200 bytes of an indecipherable message.
  - In Administrative Advice/0620—System-generated message where DE 60 is 650, DE 120 contains RiskFinder data.
  - In Administrative Advice/0620—Member-generated message where DE 60 is 650, DE 120 contains member-provided free format textual data.
- 

## Subfield 01—AVS Service Indicator 1

DE 120, subfield 01 (AVS Service Indicator 1) contains AVS data in this format for an issuer whose AVS Service Indicator status is 1.

---

#### Attributes

---

Subfield ID:	01
Length of Length Field:	2
Data Representation:	ans...29
Data Field:	Contents of positions 1–29
Justification:	Left, blank-filled

---

#### Values

---

Positions 1–9: Postal Code

---

Postal Code      Cardholder postal/ZIP code

---

Positions 10–29 Address (MasterCard)

---

Address      Cardholder address

---

Positions 10–29: Address (Visa, American Express)

---

Address      Cardholder address

---

#### Application Notes

---

Some merchants or acquirers are currently limited to supporting only numeric data.

---

## Subfield 02—AVS Service Indicator 2

DE 120, subfield 02 (AVS Service Indicator 2) contains AVS data in this format for an issuer whose AVS Service Indicator status is 2.

---

**Attributes**

Subfield ID:	02
Length of Length Field:	2
Data Representation:	an-14
Data Field:	Contents of positions 1–14
Justification:	Left, blank-filled

---

**Values**

Positions 1–9:	Postal Code
Postal Code	Cardholder postal/ZIP code
Positions 10–14:	Address (MasterCard)
Address	Cardholder address

---

**Application Notes**

Issuer receives condensed address data. (This supports the algorithm that uses the first five numeric digits in an address [when scanning the address from left to right].)

---

## Subfield 03—AVS Service Indicator 3

DE 120, subfield 03 (AVS Service Indicator 3) contains AVS data in this format for an issuer whose AVS Service Indicator status is 3.

---

**Attributes**

Subfield ID:	03
Length of Length Field:	2
Data Representation:	an-14
Data Field:	Contents of positions 1–14
Justification:	Left, blank-filled

---

**Values**

Positions 1–9:	Postal Code
Postal Code	Cardholder postal/ZIP code
Positions 10–14:	Address (MasterCard)
Address	Cardholder address

---

## Data Element Definitions

### DE 120—Record Data

---

#### Application Notes

---

The issuer receives condensed address data. (This subfield supports the algorithm that uses up to the first five numeric digits that appear before the first alphabetic character or space in the address when scanning the address from left to right.)

---

## Subfield 04—AVS Service Indicator 4

DE 120, subfield 04 (AVS Service Indicator 4) contains AVS data in this format for an issuer whose AVS Service Indicator status is 4.

---

#### Attributes

---

Subfield ID:	04
Length of Length Field:	2
Data Representation:	an-14
Data Field:	Contents of positions 1–14
Justification:	Left, blank-filled

---

#### Values

---

##### Positions 1–9: Postal Code

---

Postal Code	Cardholder postal/ZIP code
-------------	----------------------------

---

##### Positions 10–14: Address (MasterCard)

---

Address	Cardholder address
---------	--------------------

---

#### Application Notes

---

Issuer supports AVS, receives condensed numeric postal code and condensed numeric address only. (This supports the algorithm that uses only the numeric digits in a postal code and the first five numeric digits in an address [when scanning the address from left to right].)

---

## Online File Maintenance

DE 120 (Record Data), contains the record detail for the file type identified in DE 101 (File Name). The record detail contained in DE 120 depends on the value provided in DE 91 (Issuer File Update Code). The following table lists the allowed DE 91 values for each DE 101 file type.

<b>DE 101 (File Name)</b>	<b>DE 91 (Issuer File Update Code)</b>			
	<b>1 Add</b>	<b>2 Update</b>	<b>3 Delete</b>	<b>5 Inquiry</b>
MCC102 (Stand-In Account File)	√	√	√	√
MCC103 (Electronic Warning Bulletin File)	√		√	√
MCC104 (Local Stoplist File)	√		√	√
MCC105 (Recurring Payment Cancellation Service File)	√	√	√	√
MCC106 (PAN Mapping File)	√	√	√	
MCC107 (Enhanced Value File)	√	√	√	√
MCC108 (Product Graduation File)	√	√	√	√
MCC109 ( <i>PayPass</i> Application Transaction Counter [ATC] File)	√			√

## **MCC102—Stand-In Account File**

DE 120 (Record Data) contains Stand-In Account file data when DE 101 (File Name) contains MCC102.

Following is the MCC102 data fields that should be completed in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Complete These Fields in DE 120...</b>
1 = Add	Use all appropriate fields
2 = Update	Use all appropriate fields
3 = Delete	Use field 1
5 = Inquiry	Use field 1

Following is the DE 120 Layout for MCC102.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Primary Account Number	an-19	Number that is embossed or encoded or both on the card. Members may only input account numbers for BINs assigned to the associated MasterCard-assigned customer ID. Format: Sixteen digit MasterCard account number, followed by three spaces.
2 Entry Reason	an-1	Reason for listing this card. Valid values: C = Credit

**Data Element Definitions****DE 120—Record Data**

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
		F = Fraud L = Lost O = Other P = Capture Card S = Stolen U = Unauthorized Use V = Premium Listing X = Counterfeit
3 Date-Last-Update Activity	n-6	Inquiry only and is ignored on add, change, and delete. (This field is returned in the 0312 response message only for inquiry requests.) Date of the last maintenance activity occurring on this account.  Format: MMDDYY  MM = month  DD = day  YY = year
4 Time Last Update Activity	n-4	Inquiry only and is ignored on add, change, and delete. (This field returned in the 0312 response message only for inquiry requests.) Time of the last maintenance activity occurring on this account.  Format: hhmm  hh = hour  mm = minute
5 PIN Length	n-2	No longer applicable. Valid values: zeros
6 Premium Listing Accumulative Limit	n-12	Valid only for entry reason V. For other reason codes, use 12 zeros.
7 Premium Listing Limit Currency Code	n-3	Valid only for Entry Reason V. For other reason codes, use three zeros.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
8 Issuer-defined Purge Date	n-8	The issuer-defined purge date must be at least 180 days after the account list date in YYYYMMDD format. This field is optional.
9 Card Sequence Number	n-3	The card sequence number of the listed card. Only required for card-level support.
10 Card Expiration Date	n-6	The expiration date of the listed card in YYYYMM format. Only required for card-level support.

### MCC103—Electronic Warning Bulletin File

DE 120 (Record Data) contains Electronic Warning Bulletin file data when DE 101 (File Name) contains MCC103.

Following is the MCC103 data fields that should be completed in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Complete These Fields in DE 120...</b>
1 = Add or Update	Use all appropriate fields
3 = Delete	Use field 1
5 = Inquiry	Use field 1

Following is the DE 120 Layout for MCC103.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Primary Account Number	an-19	Number that is embossed or encoded on the card. Members can only input account numbers for BINs assigned to the associated MasterCard-assigned customer ID.  Format: Sixteen digit MasterCard account number followed by three spaces.
2 Customer ID	n-6	MasterCard customer ID assigned to the BIN.  Format: right-justified, zero-filled
3 Card Program	a-3	Type of card bearing the account number. Please refer to DE 63 (Network Data), for the list of card program values allowed. Card programs <b>not</b> allowed for MCC103 are footnoted in DE 63, subfield 1.

**Data Element Definitions****DE 120—Record Data**

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
4 Response Code	n-2	Response Code this account listing should prompt for an authorization request. Valid value: 04 capture card
5 Entry Reason	a-1	<p>Reason for listing this card. Valid values:</p> <p>C = Credit F = Fraud O = Other X = Counterfeit</p>
6 Filler	an-25	Reserved for future AMS enhancements.
7 Regional Indicator/ Purge Date	an-7	<p>Issuer-requested region and purge date(s) associated with this account number listing. Field is non-positional (excludes regions and purge dates that do not apply). Field may occur up to six times for that many regions and purge dates. Must be entered in ascending order (1, A,..., E). Format: RYYMMDD</p> <p>R = Region</p> <p>Valid region values:</p> <p>1 = United States A = Canada B = Latin America/Caribbean C = Asia/Pacific D = Europe E = South Asia/Middle East/Africa</p> <p>YY = purge date year MM = purge date month DD = purge date day</p> <p>Note: To purge an account on the card expiration date, enter that date as the purge date. For additional information on purge dates, please refer to the <i>Account Management System User Manual</i>.</p>

**MCC104—Local Stoplist File**

DE 120 (Record Data) contains Local Stoplist file data when DE 101 (File Name) contains MCC104.

Following is the MCC104 data fields that should be completed in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Complete These Fields in DE 120...</b>
1 Add Note: Add will update an existing record if the system finds a match on the master file.	Use all applicable fields.
1 Update	Use all applicable fields that require update.
1 Delete(deletes account from one region)	Use fields one.
1 Delete (deletes account from one country)	Use fields one, seven, eight, and ten.
1 Delete (deletes account from one subcountry)	Use fields one, seven, eight, nine, and ten.
3 Delete (deletes account from <b>all</b> regions, countries, or subcountries)	Use field one.
5 Inquiry	Use field one.

Following is the DE 120 Layout for MCC104.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Primary Account Number	an-19	Number that is embossed, encoded, or both on the card. Members may input only those account numbers that contain their assigned prefixes. Format: Sixteen digit MasterCard account number followed by three spaces.
2 Customer ID	n-6	MasterCard-assigned customer ID, a MasterCard customer may input only an account number with a BIN assigned to it. Format: right-justified, zero-filled

**Data Element Definitions****DE 120—Record Data**

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
3 Card Program	a-3	Type of card bearing the account number. Please refer to DE 63 (Network Data), for the list of card program values allowed. Card programs <b>not</b> allowed for MCC104 are footnoted in DE 63, subfield 1.
4 Response Code	n-2	Response Code this account listing should prompt for an authorization request. Valid value: 04 capture card
5 Entry Reason	a-1	<p>Reason for listing this card.</p> <p>Valid values:</p> <p>C = Credit (Prompts an Authorization response of capture card at regional level) or (Prompts an Authorization response of decline at the country/subcountry level)</p> <p>F = Fraud</p> <p>O = Other</p> <p>X = Counterfeit</p>
6 Filler	an-25	Reserved for future AMS enhancements.
7 Region	an-1	<p>The region associated with this account listing. If a country or subcountry listing is entered, this field must contain the issuer's region as follows:</p> <p>Valid region values:</p> <p>1 = United States</p> <p>A = Canada</p> <p>B = Latin America/Caribbean</p> <p>C = Asia/Pacific</p> <p>D = Europe</p> <p>E = South Asia/Middle East/Africa</p> <p>Region values must be entered in ascending order (1, A, B, C, D, E)</p>

**Data Element Definitions****DE 120—Record Data**

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
8      Country	an-3	If applicable, contains the country associated with this account listing. Must be a participating country within the issuer's region; values are three-digit country code or spaces. Refer to the <i>Quick Reference Booklet</i> for participating countries. Enter spaces if no country is specified.
9      Subcountry	an-2	If applicable, contains the subcountry associated with this account listing. Must be a participating subcountry within the issuer's country; values are two-digit subcountry code or spaces. Refer to the <i>Account Management System User Manual</i> . Enter spaces if no subcountry is specified.
10     Purge Date	n-6	Purge date (format YYMMDD) associated with this account number listing as follows:  YY      =      purge date year MM      =      purge date month DD      =      purge date day
11     Region	an-1	If applicable, second region associated with this account listing. If a second country or subcountry listing is entered, this field must contain the issuer's region. Region values must be entered in ascending order (1, A, B, C, D, E).
12     Country	an-3	If applicable, second country associated with this account listing; must be a participating country within the issuer's region.
13     Subcountry	an-2	If applicable, second subcountry associated with this account listing; must be a participating subcountry within the issuer's country.
14     Purge Date	n-6	If applicable, second purge date associated with this account number listing.

**Data Element Definitions****DE 120—Record Data**

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
15 Region	an-1	If applicable, third region associated with this account listing; if a third country or subcountry listing is entered, this field must contain the issuer's region; region values must be entered in ascending order (1, A, B, C, D, E).
16 Country	an-3	If applicable, third country associated with this account listing; must be a participating country within the issuer's region.
17 Subcountry	an-2	If applicable, third subcountry associated with this account listing; must be a participating subcountry within the issuer's country.
18 Purge Date	n-6	If applicable, third purge date associated with this account number listing.
19 Region	an-1	If applicable, fourth region associated with this account listing; if a fourth country or subcountry listing is entered, this field must contain the issuer's region; region values must be entered in ascending order (1, A, B, C, D, E).
20 Country	an-3	If applicable, fourth country associated with this account listing; must be a participating country within the issuer's region.
21 Subcountry	an-2	If applicable, fourth subcountry associated with this account listing; must be a participating subcountry within the issuer's country.
22 Purge Date	n-6	If applicable, fourth purge date associated with this account number listing.
23 Region	an-1	If applicable, fifth region associated with this account listing; if a fifth country or subcountry listing is entered, this field must contain the issuer's region; region values must be entered in ascending order (1, A, B, C, D, E).
24 Country	an-3	If applicable, fifth country associated with this account listing; must be a participating country within the issuer's region.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
25 Subcountry	an-2	If applicable, fifth subcountry associated with this account listing; must be a participating subcountry within the issuer's country.
26 Purge Date	n-6	If applicable, fifth purge date associated with this account number listing.
27 Region	an-1	If applicable, sixth region associated with this account listing; if a sixth country or subcountry listing is entered, this field must contain the issuer's region; region values must be entered in ascending order (1, A, B, C, D, E).
28 Country	an-3	If applicable, sixth country associated with this account listing; must be a participating country within the issuer's region.
29 Subcountry	an-2	If applicable, sixth subcountry associated with this account listing; must be a participating subcountry within the issuer's country.
30 Purge Date	n-6	If applicable, sixth purge date associated with this account number listing.

### MCC105—Recurring Payment Cancellation Service File

DE 120 (Record Data) contains Recurring Payment Cancellation Service file data when DE 101 (File Name) contains MCC105.

Following is the MCC105 data fields that should be completed in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Complete These Fields in DE 120...</b>
1 = Add	Use all applicable fields; fields 1-5 are mandatory, fields 6-7 are optional
2 = Update	Use all applicable fields; fields 1-5 are mandatory, fields 6-7 are optional
3 = Delete	Use fields 1, 4, and 5; fields 2 and 3 must be filled with spaces
5 = Inquiry	Use fields 1, 4, and 5; fields 2 and 3 must be filled with spaces

Following is the DE 120 Layout for MCC105. Amount fields 6 and 7 must include a minor unit of currency. For example, USD 100.50 entered as 000000010050.

## Data Element Definitions

### DE 120—Record Data

Field ID and Name	Attributes	Comments/Valid Values
1 Primary Account Number	an-19	Number that is embossed, encoded, or both on the card. Members may only input account numbers for BINs assigned to the associated customer ID that MasterCard assigned Format: Left justified, with trailing spaces
2 Entry Reason	an-1	Reason for listing this card. Valid value: A = Recurring payment cancellation service
3 Issuer-defined Purge Date	n-8	The issuer-defined purge date must be no more than 15 months beyond the account list date in YYYYMMDD format.
4 Acquirer ID	n-6	Valid acquirer ICA.
5 Card Acceptor ID Code	ans-15	Must be unique per acquirer ICA. Must be a value other than spaces. Note: This field is case sensitive.
6 Transaction Amount (low)	n-12	Optional field. Right justified with leading zeros. Indicates a single transaction amount or the start of a transaction amount range. Transaction amount must be stated in the transaction currency and not the cardholder billing currency.
7 Transaction Amount (high)	n-12	Optional field. Right justified with leading zeros. Indicates the end of a transaction amount range. Do not use this field if specifying a single amount. If used, must be greater than Transaction Amount (low). Transaction amount must be stated in the transaction currency and not the cardholder billing currency.

### DE 120 When Blocking Recurring Payments

Following are various uses of DE 120 for MCC105:

- Blocking all recurring payment arrangements with all merchants  
A block of all recurring payments arrangements can only be accomplished by setting up blocks for each merchant and acquirer combination.
- Blocking all recurring payment arrangements with one merchant, or blocking a cardholder's only recurring payment with one merchant

- Fields 1–5 are required for Add
- Fields 6–7 should not be provided
- Blocking one of many recurring payment arrangements with one merchant

The one recurring payment arrangement can only be blocked if its transaction amount is different than any of the other recurring payment arrangements with a particular merchant.

The recurring payment arrangement to be blocked has a **fixed** (same amount each billing) transaction amount, such as an insurance premium billing

- Fields 1–5 are required for Add
- Field 6 should be provided to specify the fixed transaction amount
- Field 7 should not be provided

The recurring payment arrangement to be blocked has a **variable** (different amount each billing) transaction amount, such as a long distance telephone billing. For example, if the variable billing previous amounts were between USD 15.00 and USD 50.00, field 6 should contain USD 15.00 and field 7 should contain USD 50.00. This results in transactions being blocked within this specified amount range.

- Fields 1–5 are required for Add
- Field 6 is provided to specify the lowest transaction amount billable
- Field 7 is provided to specify the highest transaction amount billable

Usage of the amount range should only be used if the billing amount of the recurring payment to be blocked is unique and does not overlap with other recurring payments from the same merchant that should not be blocked. If one recurring payment arrangement billing amount was typically between USD 15.00 and USD 50.00 but another recurring payment from the same merchant either had a variable amount that sometimes fell within USD 15.00 to USD 50.00 or had a fixed amount within USD 15.00 to USD 50.00, both recurring payments are blocked.

## MCC106—PAN Mapping File

DE 120 (Record Data) contains PAN Mapping File data when DE 101 (File Name) contains MCC106.

Following is the MCC105 data fields that should be completed in DE 120 depending on the value in DE 91 (Issuer File Update Code).

## Data Element Definitions

### DE 120—Record Data

When DE 91 Contains...	Complete These Fields in DE 120...
1 = Add	Fields 1-2 mandatory, field 3 optional
2 = Update	Fields 1-2 mandatory, fields 3-5 optional Valid combinations of fields 1-5 are: <ul style="list-style-type: none"><li>• Fields 1-3</li><li>• Fields 1-3 and field 5; field 4 must contain spaces</li><li>• Fields 1-2 and field 4; field 3 must contain spaces</li><li>• Fields 1-2 and field 5; fields 3 and 4 must contain spaces</li></ul>
3 = Delete	Use field 1 only. All records associated to <i>PayPass</i> account number will be deleted.

Following is the DE 120 Layout for MCC106 in the Issuer File Update Request/0302 Message.

Field ID and Name	Attributes	Comments/Valid Values
1 <i>PayPass</i> Account Number	an-19	Number that is assigned to the <i>PayPass</i> card or device and transmitted from the card or device to the X terminal. Format: Left justified, with trailing spaces
2 PAN	an-19	Number that is embossed, encoded, or both on the card. Members may only input account numbers for BINs assigned to the associated customer ID that MasterCard assigned. Format: Left justified, with trailing spaces
3 Card Expiration Date (PAN)	n-4	Expiration date that is embossed, encoded, or both on the card that represents the cardholder primary account number. Format: YYMM
4 <i>PayPass</i> account number (replacement)	an-19	Replacement account number that is assigned to the <i>PayPass</i> card or device and transmitted from card or device to the <i>PayPass</i> terminal. Format: Left justified, with trailing spaces
5 PAN (replacement)	an-19	Number that is embossed, encoded, or both on the replacement card. Members may only input account numbers for BINs assigned to the associated customer ID that MasterCard assigned Format: Left justified, with trailing spaces

Following is the DE 120 Layout for MCC106 in the Issuer File Update Request Response/0312 Message.

Field ID and Name	Attributes	Comments/Valid Values
1 <i>PayPass</i> account number	an-19	Number that is assigned to the <i>PayPass</i> card or device and transmitted from the card or device to <i>PayPass</i> terminal. Format: Left justified, with trailing spaces
2 PAN	an-19	Number that is embossed, encoded, or both on the card. Members may only input account numbers for BINs assigned to the associated customer ID that MasterCard assigned. Format: Left justified, with trailing spaces
3 Card Expiration Date (PAN)	n-4	Expiration date that is embossed, encoded, or both on the actual card. Format: YYMM
<i>PayPass</i> account number (replacement)	an-19	Replacement number that is assigned to the <i>PayPass</i> card or device and transmitted from the card or device to <i>PayPass</i> terminal. Format: Left justified, with trailing spaces
5 PAN (replacement)	an-19	Number that is embossed, encoded, or both on the replacement card. Members may only input account numbers for BINs assigned to the associated customer ID that MasterCard assigned. Format: Left justified, with trailing spaces
6 Date-Last-Update Activity	n-6	Format: MMDDYY (Month, Day, Year)
7 Time-Last-Update Activity	n-4	Format: hhmm (hour, minute)

## MCC107—Enhanced Value File

DE 120 (Record Data) contains MasterCard Enhanced Value (Enhanced Value) file data when DE 101 (File Name) contains MCC107.

Following is the MCC107 data fields that should be completed in DE 120 depending on the value in DE 91 (Issuer File Update Code).

When DE 91 Contains...	Complete These Fields in DE 120...
1 = Add	Use fields 1-5, field 2 may contain spaces
2 = Update	Use fields 1-5, field 2 may contain spaces

## Data Element Definitions

### DE 120—Record Data

---

When DE 91 Contains...	Complete These Fields in DE 120...
3 = Delete	Field 1 mandatory, field 2 optional. Fields 3, 4, and 5 not required
5 = Inquiry	Use field 1 only, field 2 optional (but if submitted, must be equal to field 1)

Following is the DE 120 Layout for MCC107 in the Issuer File Update Request/0302 message.

Field ID and Name	Attributes	Comments/Valid Values
1 Primary Account Number (Low PAN)	an-19	This field is mandatory. Field 1 is used to define a single cardholder account the issuer has qualified as eligible for Enhanced Value. This field must be 19 positions, left-justified, filled with spaces. When the issuer is using MCC107 to define subsets of entire account ranges, the field will contain the first account in the range of accounts; field 2 will contain the last account.
2 Primary Account Number (High PAN)	an-19	<p>This field must be 19 positions, left-justified, filled with spaces. This field may be used to complement Field 1 as follows:</p> <ul style="list-style-type: none"><li>• When the issuer's intent is to add, update, or delete a single account, Field 2 must contain either spaces or a value equal to Field 1.</li><li>• When the issuer's intent is to add, update, or delete a range of accounts, Field 2 must contain a value greater than the value found in Field 1. The total number of cardholder accounts defined with this method must not exceed 100,000.</li><li>• When the issuer's intent is to inquire, Field 2 is not required; however if present, Field 2 must contain spaces or a value equal to the value in Field 1. Inquiries on ranges of accounts are not permitted.</li></ul>
3 Account Category	an-1	This field must only contain a value of B (Enhanced Value) or space.
4 Purge Date	n-8	This field must contain a date in CCYYMMDD format. The date must be no greater than 20 years from the date on which the account is listed.
5 Program ID	an-6	This field must contain the Program ID assigned to the issuer when the issuer enrolled in Enhanced Value.

Following is the DE 120 Layout for MCC107 in the Issuer File Update Request Response/0312 message.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Primary Account Number (Low PAN)	an-19	This field is mandatory. Field 1 is used to define a single cardholder account the issuer has qualified as eligible for Enhanced Value. This field must be 19 positions, left-justified, filled with spaces. When the issuer is using MCC107 to define subsets of entire account ranges, the field will contain the first account in the range of accounts; field 2 will contain the last account.
2 Primary Account Number (High PAN)	an-19	<p>This field must be 19 positions, left-justified, filled with spaces. This field may be used to complement Field 1 as follows:</p> <ul style="list-style-type: none"> <li>• When the issuer's intent is to add, update, or delete a single account, Field 2 must contain either spaces or a value equal to Field 1.</li> <li>• When the issuer's intent is to add, update, or delete a range of accounts, Field 2 must contain a value greater than the value found in Field 1. The total number of cardholder accounts defined with this method must not exceed 100,000.</li> <li>• When the issuer's intent is to inquire, Field 2 is not required; however if present, Field 2 must contain spaces or a value equal to the value in Field 1. Inquiries on ranges of accounts are not permitted.</li> </ul>
3 Account Category	an-1	This field must only contain a value of B (Enhanced Value), S (Premium High Spend), or a blank.
4 Purge Date	n-8	This field must contain a date in CCYYMMDD format. The date must be no greater than 20 years from the date on which the account is listed.
5 Program ID	an-6	This field must contain the Program ID assigned to the issuer when the issuer enrolled in Enhanced Value.
6 Customer ID	n-6	The unique customer number that is assigned by MasterCard. Format: right-justified, zero-filled.

## Data Element Definitions

### DE 120—Record Data

---

Field ID and Name	Attributes	Comments/Valid Values
7 Date-Last-Update Activity	n-6	Format: MMDDYY
8 Time-Last-Update Activity	n-4	Format: HHMM

### MCC108—Product Graduation File

DE 120 (Record Data) contains MasterCard Product Graduation (Product Graduation) file data when DE 101 (File Name) contains MCC108.

Following is the MCC108 data fields that should be completed in DE 120 depending on the value in DE 91 (Issuer File Update Code).

When DE 91 Contains...	Complete These Fields in DE 120...
1 = Add	Use fields 1-7
2 = Update	Use fields 1-7
3 = Delete	Use field 1 only
5 = Inquiry	Use field 1 only

Following is the DE 120 Layout for MCC108 in the Issuer File Update Request/0302 message.

Field ID and Name	Attributes	Comments/Valid Values
1 Primary Account Number	an-19	Mandatory. This field must be used to define a single account. The field must be 19 positions, left-justified, filled with spaces.
2 Account Category	an-1	Conditional. Valid values: B = Enhanced Value Space = Cards registered as Product Graduation only or Product Graduation and Enhanced Value
3 Graduated Product Code	a-3	Mandatory. This field must contain the product code to which the issuer wants to migrate the account found in Field 1.
4 Purge Date	n-8	Mandatory. This field must contain a date in CCYYMMDD format. The date must be no greater than 20 years from the date on which the account is listed.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
5 Previous Product Code	an-3	<p>Optional. The field will contain the product code from which the account is migrating.</p> <p>This field must contain spaces if a product code is not provided.</p>
6 Program ID	an-6	<p>Conditional. This field is required if the issuer is registering the account for Enhanced Value.</p> <p>This field must contain spaces if a program ID is not provided.</p>
7 Customer Specific Index (CSI)	an-7	<p>Optional. This field will contain the issuer-defined number associated with the CSI to which the issuer is assigning the account found in Field 1.</p> <p>This field must contain spaces if a CSI number is not provided.</p>

Following is the DE 120 Layout for MCC108 in the Issuer File Update Request Response/0312 message.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>															
1 Primary Account Number	an-19	This field must be used to define a single account. The field must be 19 positions, left-justified, filled with spaces.															
2 Account Category	an-1	Mandatory. Valid values: <table style="margin-left: 20px;"> <tr> <td>B</td> <td>=</td> <td>Enhanced Value</td> </tr> <tr> <td>M</td> <td>=</td> <td>Enhanced Value and Product Graduation</td> </tr> <tr> <td>P</td> <td>=</td> <td>Product Graduation</td> </tr> <tr> <td>S</td> <td>=</td> <td>High Value</td> </tr> <tr> <td>T</td> <td>=</td> <td>High Value and Product Graduation</td> </tr> </table>	B	=	Enhanced Value	M	=	Enhanced Value and Product Graduation	P	=	Product Graduation	S	=	High Value	T	=	High Value and Product Graduation
B	=	Enhanced Value															
M	=	Enhanced Value and Product Graduation															
P	=	Product Graduation															
S	=	High Value															
T	=	High Value and Product Graduation															
3 Graduated Product Code	an-3	Mandatory. This field must contain the product code to which the issuer wants to migrate the account found in Field 1.															
4 Purge Date	n-8	Mandatory. This field must contain a date in CCYYMMDD format. The date must be no greater than 20 years from the date on which the account is listed.															

**Data Element Definitions****DE 120—Record Data**

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
5 Previous Product Code	an-3	This field will contain the previous product code on file for the account regardless of whether the issuer provided a product code value in the Previous Product Code field of the Issuer File Update Request/0302 message.
6 Program ID	an-6	Conditional. This field will contain spaces if a program ID is not provided.
7 Customer Specific Index (CSI)	an-7	Optional. This field will contain spaces if a CSI number is not provided.
8 Customer ID	n-6	Mandatory. The unique custom number that is assigned by MasterCard. Format: right-justified, zero-filled.
9 Date-Last Update Activity	n-6	Format: MMDDYY
10 Time-Last-Update Activity	n-4	Format: HHMM

**MCC109—PayPass Application Transaction Counter File**

DE 120 (Record Data) contains *PayPass Application Transaction Counter* file data when DE 101 (File Name) contains MCC109.

Following is the MCC109 data fields that should be completed in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Complete These Fields in DE 120...</b>
1 = Add	Fields 1-4 mandatory
3 = Delete (Note: applicable only when submitting a R311 bulk file deletion request.)	Fields 1-4 mandatory
5 = Inquiry	Fields 1-3 mandatory

Following is the DE 120 Layout for MCC109 in the Issuer File Update Request/0302 message. Fields 1 through 3 must be considered contiguous to identify if an entry exists when trying to delete a record.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 <i>PayPass Account Number</i>	an-19	Number that is assigned to the <i>PayPass</i> card or device and transmitted from the card or device to the <i>PayPass</i> terminal Format: Left justified, with trailing spaces
2 Card Sequence Number	n-1	May be zero
3 <i>PayPass Account Expiration Date</i>	n-4	Expiration dateFormat: YYMM
4 <i>PayPass Application Transaction Counter (ATC) Value</i>	n-5	Right-justified, leading zeros

Following is the DE 120 Layout for MCC109 in the Issuer File Update Request Response/0312 message.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 <i>PayPass Account Number</i>	an-19	Number that is assigned to the <i>PayPass</i> card or device and transmitted from the card or device to <i>PayPass</i> terminal. Format: Left justified, with trailing spaces
2 Card Sequence Number	n-1	May be zero
3 <i>PayPass Account Expiration Date</i>	n-4	Expiration date Format: YYMM
4 <i>PayPass Application Transaction Counter (ATC) Value</i>	n-5	Right-justified, leading zeros
5 Filler	an-1	
6 Issuer Customer ID	n-6	
7 Date/Time-Last-Update Activity	n-12	Format: MMDDYYHHMMSS
8 Entry Change Indicator	an-1	Indicates how the ATC Value was last changed B = batch entry O = online entry T = transaction

## Data Element Definitions

### DE 120—Record Data

---

Field ID and Name	Attributes	Comments/Valid Values
9 Creation Date/Time Stamp	n-14	Format: MMDDCCYYHHMMSS
10 Last Transaction Time	n-4	Last transaction time for valid ATC. Format: hhmm

### DE 120 Error Codes

Following are the DE 120 Error Codes.

#### MCC102 Error Codes

The Authorization System returns a Issuer File Update Request Response/0312 message where DE 39 contains the value 27 and DE 44 contains the value 120xxx (xxx indicates the field in MCC102 where the error occurred).

Error Code	Error Message
120001	Primary Account Number (PAN), extended not numeric -Or- BIN in Primary Account Number (PAN), extended not on FIM -Or- Origin of message invalid for BIN in Primary Account Number (PAN), extended -Or- Check digit in Primary Account Number (PAN), extended not correct -Or- Primary Account Number (PAN), extended not on Account File (for delete or inquiry).
120002	Entry Reason not one of the following: (C, F, G, L, O, P, S, U, V, X).
120005	PIN length not numeric or spaces.
120006	Entry-Reason = V and Premium Listing Accumulative Limit Amount not numeric.
120007	Invalid Currency Code
120008	Invalid Issuer-defined Purge Date
120009	Invalid Card Sequence Number
120010	Invalid Card Expiration Date

#### MCC103 Error Codes

The Authorization System returns a Issuer File Update Request Response/0312 message where DE 39 contains the value 25 or 27 and DE 44 contains the value 120xxx (xxx indicates the field in MCC103 where the error occurred).

---

**Error Code    Error Message**


---

When DE 39 contains the value 25 (Unable to locate record on file [no action taken]), DE 44 contains the following error code:

---

120001 Primary account number not on file.

---

When DE 39 contains the value 27, DE 44 contains one of the following error codes:

---

120001 Primary account number not on file  
-Or-  
Primary Account Number (PAN), extended is not numeric  
-Or-  
BIN in Primary Account Number (PAN), extended is invalid  
-Or-  
Check digit in cardholder number is not correct and product code is not equal to MNS (Non-standard)  
-Or-  
Origin of message invalid for BIN in Primary Account Number (PAN), Extended.

---

120002 Issuing ICA (customer ID) is not associated with Primary Account Number (PAN), Extended BIN.

---

120003 Product code is not equal to a valid card program value.

---

120004 Response code not equal to 04 (capture card).

---

120005 Entry reason is not C, F, O, or X.

---

120006 Regional indicator is not 1, A, B, C, D, or E.  
-Or-  
Regional indicator is not in ascending order.

---

120007 Region-requested purge date invalid.  
-Or-

Region-requested purge date not equal to current or future date.

-Or-

Requested purge date must be at least one day beyond current date if account is not already listed.

---

### MCC104 Error Codes

The Authorization System returns a Issuer File Update Request Response/0312 message where DE 39 contains the value 25, 27, or 30 and DE 44 contains the value 120xxx (xxx indicates the field in MCC104 where the error occurred.)

---

**Error Code    Error Message**


---

When DE 39 contains the value 25, DE 44 contains the following error code:

---

120001 Account not on file.

---

## Data Element Definitions

### DE 120—Record Data

---

Error Code	Error Message
When DE 39 contains the value 27, DE 44 contains one of the following error codes:	
120001	Primary Account Number (PAN), Extended is not numeric -Or- BIN in Primary Account Number (PAN), Extended is invalid -Or- Check digit in cardholder number is not correct and product code is not equal to PNS (Non-standard) -Or- Origin of message invalid for BIN in Primary Account Number (PAN), Extended.
120002	Issuing ICA (customer ID) is not associated with Primary Account Number (PAN)
120003	Card Program is not equal to a valid value -Or- BIN is not set up for proprietary card program, and card program in the request equals PRO or PNS.
120004	Response code is not 04.
120005	Entry reason is not C, F, O, or X.
120006	Regional indicator is not equal to 1, A, B, C, D, or E -Or- Regional indicator is not in ascending order.
120007	Country invalid or outside issuer region.
120008	Subcountry invalid or outside issuer country.
120009	Purge date invalid -Or- Purge date not equal to current or future date -Or- Requested purge date must be at least one day beyond current date if account is not already listed.

### MCC105 Error Codes

If the Authorization System detects an error in the Issuer File Update Request/0302 message, it returns an Issuer File Update Request Response/0312 message containing error codes specific to each file name. DE 39 (Response Code) contains value 27 (Issuer File Update field edit error) and DE 44 (Additional Response Data) contains the value 120xxx (where xxx indicates the field in MCC105 where the error occurred).

Error Code	Error Message
120001	<p>Primary Account Number (PAN) not within account range that is an RPCS participant</p> <p>-Or-</p> <p>Primary Account Number (PAN) not numeric</p> <p>-Or-</p> <p>BIN in Primary Account Number (PAN) not valid</p> <p>-Or-</p> <p>Check digit in Primary Account Number (PAN) not correct</p> <p>-Or-</p> <p>Primary Account Number (PAN) not on RPCS File (for update, delete, or inquiry).</p>
120002	Entry Reason is not (A).
120003	<p>Invalid Issuer-defined Purge Date format</p> <p>-Or-</p> <p>Issuer-defined Purge Date not equal to or greater than system date</p> <p>-Or-</p> <p>Issuer-defined Purge Date not greater than system date by 15 months</p>
120004	Acquirer ICA not numeric
120005	Card Acceptor ID code not present.
120006	Transaction Amount (low limit) not numeric
120007	<p>Transaction Amount (high limit) not numeric</p> <p>-Or-</p> <p>Transaction Amount (high limit) not greater than Transaction Amount (low limit)</p> <p>-Or-</p> <p>Transaction Amount (high limit) is present but Transaction Amount (low limit) is not present.</p>

### MCC106 Error Codes

DE 39 contains the appropriate value and DE 44 contains value 120xxx (where xxx indicates the field in MCC106 where the error occurred).

Error Code	Error Message
	When DE 39 contains value 25 (Unable to locate record on file), DE 44 contains the following error code:
120001	<i>PayPass</i> account number not on MCC106 (PAN Mapping File) (for update or delete)
120002	PAN not on MCC106 (PAN Mapping File) (for update)

## Data Element Definitions

### DE 120—Record Data

---

Error Code	Error Message
When DE 39 contains value 27 (Issuer File Update Field Edit Error), DE 44 contains one of the following error codes:	
120001	<p><i>PayPass</i> account number not numeric</p> <p>-Or-</p> <p>Prefix in <i>PayPass</i> account number not valid</p> <p>-Or-</p> <p>Check digit in <i>PayPass</i> account number not correct</p> <p>-Or-</p> <p><i>PayPass</i> account number not within account range that is a <i>PayPass</i> Mapping Service participant</p>
120002	<p>PAN not numeric</p> <p>-Or-</p> <p>Prefix in PAN not valid</p> <p>-Or-</p> <p>Check digit in PAN not correct</p> <p>-Or-</p> <p>PAN and <i>PayPass</i> account number prefixes do not have same country and product</p> <p>-Or-</p> <p>PAN prefix should not be participating in the <i>PayPass</i> Mapping Service</p>
120003	Invalid PAN card expiration date
120004	<p>Replacement <i>PayPass</i> account number not numeric</p> <p>-Or-</p> <p>Prefix in Replacement <i>PayPass</i> account number not valid</p> <p>-Or-</p> <p>Check digit in Replacement <i>PayPass</i> account number not correct</p> <p>-Or-</p> <p>Replacement <i>PayPass</i> account number not within account range that is a <i>PayPass</i> Mapping Service participant</p>
120005	<p>Replacement PAN not numeric</p> <p>-Or-</p> <p>Prefix in Replacement PAN not valid</p> <p>-Or-</p> <p>Check digit in Replacement PAN not correct</p> <p>-Or-</p> <p>Replacement PAN and <i>PayPass</i> account number prefixes do not have same country and product</p> <p>-Or-</p> <p>Replacement PAN prefix should not be participating in the <i>PayPass</i> Mapping Service</p>

Error Code	Error Message
When DE 39 contains value 80 (Duplicate add, action not performed), DE 44 contains the following error code:	
120001	<i>PayPass</i> account number is a duplicate
120004	Replacement <i>PayPass</i> account number is a duplicate

### MCC107 Error Codes

DE 39 contains the appropriate value and DE 44 contains value 120xxx (where xxx indicates the field in MCC107 where the error occurred).

Error Code	Error Message	
When DE 39 contains value 27 (Issuer File Update Field Edit Error), DE 44 contains the following error code:		
120001	<p>Primary Account Number (PAN) is not numeric          -Or-          Primary Account Number (PAN) is not valid          -Or-          PAN does not begin with 51-55, 36, or 38          -Or-          PAN for an account range that is a non-U.S. range (the country code associated with the range is not 840)          -Or-          DE 91 contains a value of 1 (Add) and Field 1 contains a PAN that is already listed on MCC107 with Account Category value B          -Or-          DE 91 contains a value of 1 (Add) and Field 1 contains a PAN that is already listed on MCC107 with Account Category value M          -Or-          DE 91 contains a value of 1 (Add) and Field 1 contains a PAN that is already listed on MCC108 with Account Category value P and is graduated to a product that would result in transactions qualifying for a premium interchange rate (for example, World)          -Or-          DE 91 contains a value of 1 (Add) and Field 1 contains a PAN that is already listed on MCC107 with Account Category value S          -Or-          DE 91 contains a value of 2 (Update), Field 1 contains a PAN that is already listed on MCC107 with Account Category value B, M, or S and the other fields in DE 120 have not changed          -Or-          DE 91 contains a value of 2 (Update) and the account is not listed on MCC107          -Or-</p>	

## Data Element Definitions

### DE 120—Record Data

---

Error Code	Error Message
	<p>The issuer submits a delete request for MCC107 but the Account Category value is P (MasterCard Product Graduation)</p> <p>-Or-</p> <p>The country associated with the PAN is not valid for Account Level Management</p>
120002	<p>Primary Account Number (PAN) is not numeric</p> <p>-Or-</p> <p>Primary Account Number (PAN) is not valid</p> <p>-Or-</p> <p>PAN does not begin with 51-56, 36, or 38</p>
120003	<p>Account Category is not valid</p> <p>-Or-</p> <p>Account Category is not valid for the product associated with the account range</p>
120004	<p>Purge Date is not equal to or less than 20 years from the current date</p> <p>-Or-</p> <p>Purge Date is not formatted in CCYYMMDD format</p>
120005	<p>Program ID is not 6 alphanumeric positions</p> <p>-Or-</p> <p>Program ID is not a valid value, as assigned to the issuer by MasterCard</p>
120999	Number of accounts generated by the combination of Low PAN (Field 1) and High PAN (Field 2) exceeds a total of 100,000 accounts.

### MCC108 Error Codes

DE 39 contains the appropriate value and DE 44 contains value 120xxx (where xxx indicates the field in MCC108 where the error occurred).

Error Code	Error Message
	<p>When DE 39 contains value 27 (Issuer File Update Field Edit Error), DE 44 contains the following error code:</p>
120001	<p>Primary Account Number (PAN) is not numeric</p> <p>-Or-</p> <p>Primary Account Number (PAN) is not valid</p> <p>-Or-</p> <p>PAN does not begin with 51-55, 36, or 38</p> <p>-Or-</p> <p>PAN for an account range that is a non-U.S. range (the country code associated with the range is not 840).</p> <p>-Or-</p>

Error Code	Error Message
	<p>DE 91 contains a value of 1 (Add) and Field 1 contains a PAN that is already listed on both MCC107 and MCC108 with Account Category value M</p> <p>-Or-</p> <p>DE 91 contains value 1 (Add) and Field 1 contains a PAN that is already listed on MCC108 with Account Category value P</p> <p>-Or-</p> <p>DE 91 contains value 1 (Add) and Field 1 contains a PAN that is already listed on both MCC107 and MCC108 with Account Category value P</p> <p>-Or-</p> <p>The country associated with the PAN is not valid for Account Level Management</p>
120002	<p>Account Category is not valid</p> <p>-Or-</p> <p>Account Category is not valid for the product associated with the account range.</p> <p>-Or-</p> <p>Field 2 does not contain a valid Account Category value. Valid values are: B or space.</p> <p>-Or-</p> <p>Field 2 contains an Account Category not valid for the product code to which the issuer is graduating the account. Valid values are: B or space.</p>
120003	<p>Product Code is not valid</p> <p>-Or-</p> <p>Product Code override is not valid for the product currently maintained at the issuer account range.</p> <p>-Or-</p> <p>Field 3 does not contain a valid graduated product code</p>
120004	<p>Purge Date is not equal to or less than 20 years from the current date.</p> <p>-Or-</p> <p>Purge Date is not formatted in CCYYMMDD format</p>
120005	The product code is not a valid product code

## Data Element Definitions

### DE 120—Record Data

---

Error Code	Error Message
120006	<p>Invalid program ID -Or- The Program ID is not an-6 -Or- The Program ID is not provided for an account being registered for MasterCard Enhanced Value Platform (Field 2 Account Category value B) -Or- The Program ID contains all zeroes or all spaces for an account being registered for MasterCard Enhanced Value Platform (Field 2 Account Category value B) -Or- The Program ID is not a valid Program ID for the ICA associated with the PAN -Or- The Program ID is provided for an account being graduated to a premium product</p>
120007	<p>Invalid CSI value -Or- The Customer Specific Index (CSI) value provided is not an-7 -Or- The CSI value is not valid for the ICA associated with the PAN</p>

### MCC109 Error Codes

DE 39 contains the appropriate value and DE 44 contains value 120xxx (where xxx indicates the field in MCC109 where the error occurred).

Error Code	Error Message
	<p>When DE 39 contains value 25 (Unable to locate record on file), DE 44 contains the following error code:</p>
120001	<p><i>PayPass</i> Account Number/Card Sequence Number/<i>PayPass</i> Account Expiration Date not on <i>PayPass</i> Application Transaction Counter (ATC) File (MCC109) (for add or inquiry)</p>
	<p>When DE 39 contains value 27 (Issuer File Update Field Edit Error), DE 44 contains one of the following error codes:</p>
120001	<p><i>PayPass</i> Account Number not numeric -Or- Prefix in <i>PayPass</i> account not valid -Or- Check digit in <i>PayPass</i> Account Number not correct</p>
120002	<p>Card Sequence Number not numeric</p>

<b>Error Code</b>	<b>Error Message</b>
120003	<i>PayPass</i> Account Expiration Date invalid
120004	ATC not numeric
When DE 39 contains value 80 (Duplicate add, action not performed), DE 44 contains the following error code:	
120001	<i>PayPass</i> Account Number/Card Sequence Number/ <i>PayPass</i> Account Expiration Date already exists on file (applies to Add)

## DE 121—Authorizing Agent ID Code

DE 121 (Authorizing Agent ID Code), when used, must contain the appropriate MasterCard-assigned customer ID number that uniquely identifies the Authorization Platform Stand-In processing facility or alternate routing CPS responsible for performing Stand-In processing on-behalf of the issuer.

---

### Attributes

---

Length of Length Field:	3
Data Representation:	ISO: n..999; LLIVAR
	MasterCard: n...6; LLIVAR
Data Field:	Contents of positions 1–6
Subfields:	N/A
Justification:	N/A

---

### Usage

---

Following is the usage of DE 121 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Reversal Request Response/0410	C	•	C
Reversal Advice/0420	•	C	C

---

### Values

---

## Data Element Definitions

### DE 122—Additional Record Data

---

Must contain a valid MasterCard customer ID number. MasterCard reserves values 000000–000999 for MasterCard use.

The following values may be present in DE 121:

- If the 0110 message was responded to by the issuer, the value may contain the issuer's MasterCard ID.
- If the 0110 message was responded to by the MIP X-Code System, the value will be 000000.
- If the 0110 message was responded to by the Stand-In System, the value will be 000001.
- If the 0110 message was responded to by an alternate issuer host route, the value will be 000002.
- If a decline occurred due to an on-behalf service, the value will be 000003.
- If the 0110 message was responded to by the MasterCard Rewards System, the value will be 000004 (MasterCard Rewards System).

---

#### Application Notes

---

This data element is defined and used identically within all MasterCard programs and services.

When Stand-In processing or “alternate authorizer” performs an Authorization Request/0100 on behalf of an issuer, it must insert this data element into the appropriate response message (for example, Authorization Request Response/0110) and into the appropriate Authorization Advice/0120—System-generated message so that the entire transaction audit trail clearly identifies the specific authorizing agent that actually approved the transaction.

The acquirer must insert this value in the Authorization Advice/0120 message when DE 121 is present in the Authorization Request Response/0110 message.

DE 121 is not required in Authorization Request/0100 or Authorization Advice/0120 messages the original issuer or its designated “primary” authorizing agent initiates.

DE 121, value 000002 is applicable only to issuers that use an alternate issuer host route instead of the Stand-In System. The issuer will provide in the Authorization Request Response/0110 message DE 121, value 000002 when an alternate issuer processed the original request.

DE 121 will have the value 000003 when a decline occurred due to an on-behalf service.

DE 121, value 000004 is applicable only to issuers participating in the MasterCard Pay with Rewards service and will only be present in the Authorization Advice/0120—System-generated messages notifying issuers of a declined request. The specific reason for the decline will be specified in DE 60 (Advice Reason Code).

**For UK Domestic Maestro:** This data element is not applicable for UKDM transactions.

---

## DE 122—Additional Record Data

DE 122 is a “free-format” variable length data element used for transmitting file record data in various message types. When used in Issuer File Update Request Response/0312 messages, this data element contains additional record data for file “inquiry” requests.

---

#### **Attributes**

Length of Length Field:	3
Data Representation:	ans...999; LLLVAR
Data Field:	Contents of positions 1–999
Subfields:	N/A
Justification:	N/A

---

#### **Usage**

Following is the usage of DE 122 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Issuer File Update Request Response/0312	•	C	C

---

#### **Values**

The length field must be in the range 001–999.

DE 122 is a “free-format” variable length data element used for transmitting file record data in various message types.

---

#### **Application Notes**

This data element is defined and used identically within all MasterCard programs and services.

When used in Issuer File Update Request Response/0312 messages, this data element contains additional record data for file “inquiry” requests.

---

## **DE 123—Receipt Free Text**

DE 123 (Receipt Free Text) is only applicable to Swedish Domestic Authorization Switching Service (SASS). DE 123 contains information to be printed on a receipt (not displayed on the terminal screen) for balance inquiry and ATM transactions (where DE 3 [Processing Code] is value 01 [Withdrawal] or value 30 [Balance Inquiry]).

---

#### **Attributes**

Length of Length Field:	3
Data Representation:	ISO: ans...999; LLLVAR MasterCard: ans...512; LLLVAR
Subfields:	N/A
Justification:	N/A

---

#### **Usage**

## Data Element Definitions

### DE 124—Member-defined Data

---

Following is the usage of DE 123 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	O	X	C

#### Values

---

Proprietary receipt free data up to 512 characters.

#### Application Notes

---

Issuers may provide DE 123 for balance inquiry transactions, combined authorization response and account balance transactions, and ATM withdrawal transactions.

WHEN...	THEN the Authorization Platform
DE 123 is present in an Authorization Request Response/0110 message where DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) does not contain value 01 (Withdrawal) or 30 (Balance Inquiry)	Sends the issuer an Authorization Response Negative Acknowledgement/0190 where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 123</li></ul>

WHEN...	THEN the Authorization Platform
DE 123 contains a length greater than 512 characters	Sends the issuer an Authorization Response Negative Acknowledgement/0190 where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 123</li></ul> The Authorization Platform will not send DE 123 in an Authorization Request Response/0110 message to an acquirer that is not registered to receive this data.

## DE 124—Member-defined Data

DE 124 (Member-defined Data) is described for general use, MasterCard MoneySend only, Brazil Maestro only, and Bill Payment at the ATM only use.

### DE 124—Member-defined Data (General Use)

DE 124 (Member-defined Data-General Use) may be used to submit up to 199 bytes of member-defined data. DE 124 can contain program-specific data as defined by the DE 124 subelements.

---

#### Attributes

---

Length of Length Field:	3
Data Representation:	ans...199; LLLVAR

Data Field:	Contents of positions 1-199
Subelements:	Determined by program
Justification:	N/A

#### **Usage**

Following is the usage of DE 124 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—System-generated	•	C	C
Authorization Advice/0120—Acquirer-generated	O	•	C
Reversal Request/0400	O	•	C
Reversal Request Response/0410	O	•	C

#### **Application Notes**

DE 124 may be required in support of programs to convey information between customers in an Authorization Request/0100 and Authorization Request Response/0110 message.

#### **Acquirers:**

IF DE 124 is...	THEN...
Up to 199 bytes in the Authorization Request/0100 message	The Authorization Platform will not edit the content of DE 124 and will forward the entire length of the data to the issuer.
More than 199 bytes of data in the Authorization Request/0100 message	The Authorization Platform will truncate to 199 bytes the length of the data sent to the issuer.

Absolute positioning of data in DE 124 subfields is required; padding will be necessary. Members must select all State, Province, and Country Codes from the *Quick Reference Booklet*. If a country code is used, it must be the ISO 3-character alphabetic (not numeric) Country Code. If used, a State or Province Code should be right-justified in this subfield with one leading blank space. Members must not use all zeros, all low values, or all high values when formatting DE 124.

**Subfields 1–4:** are used for MasterCard *MoneySend* transactions, DE 124 is mandatory in *MoneySend* Payment Transactions for acquirers to provide sender identification data. DE 124 is optional in *MoneySend* Funding Transactions.

**Subfields 6–13:** are used for Maestro credit usage in Brazil.

#### **Issuers:**

IF DE 124 is...	THEN...
-----------------	---------

## Data Element Definitions

### DE 124—Member-defined Data

---

Up to 199 bytes in the Authorization Request Response/0110 message	The Authorization Platform will not edit the content of DE 124 and will forward the entire length of the data to the acquirer.
More than 199 bytes of data in the Authorization Request Response/0110 message.	The Authorization Platform will truncate to 199 bytes the length of the data sent to the acquirer.
The Authorization Request/0100 and Authorization Request Response/0110 messages will be able to contain DE 124 data independently from one another. Therefore, issuers may:	
<ul style="list-style-type: none"><li>• Send back the same value in DE 124 in the Authorization Request Response/0110 message as was present in DE 124 of the Authorization Request/0100 message.</li><li>• Send a different value in DE 124 in the Authorization Request Response/0110 message as was present in DE 124 of the Authorization Request/0100 message.</li><li>• Not send DE 124 in the Authorization Request Response/0110 message. In this case, the acquirer will not receive DE 124 in the Authorization Request Response/0110 message.</li><li>• Include DE 124 in the Authorization Request Response/0110 message even when the acquirer did not send it in the Authorization Request/0100 message.</li></ul>	

### DE 124—Member-defined Data (*MoneySend Only*)

DE 124 (Member-defined Data-*MoneySend Only*) is used only for MasterCard *MoneySend* transactions.

**Subfields 1–4:** are used for MasterCard *MoneySend* transactions, DE 124 is mandatory in *MoneySend* Payment Transactions for acquirers to provide sender identification data. DE 124 is optional for *MoneySend* Funding Transactions.

### DE 124—Member-defined Data (Brazil Maestro Only)

DE 124 (Member-defined Data-Brazil Maestro Only) is used only for Brazil Maestro transactions.

**Subfields 1–8:** are used for Maestro credit usage in Brazil.

### Subfield 1—Unique Reference Number

DE 124, subfield 1 (Unique Reference Number) contains a unique reference number as it applies to MasterCard *MoneySend* transactions.

---

#### Attributes

---

Data Representation: ans-19

---

Data Field: Contents of positions 1–19

---

Justification:	Left-justified with trailing spaces
----------------	-------------------------------------

---

**Values**

Valid value string will contain a leading zero (0), followed by:  
ICA (n-6)  
Year (n-1)  
Julian Date (n-3)  
Time hhmmss (n-6)  
Transaction Sequence number (01-99) (n-2)  
Example: 055555801215305401

---

## **Subfield 2—Sender/Payer/User ID**

DE 124, subfield 2 (Sender/Payer/User ID) contains sender name, payer name, or user ID data.

---

**Attributes**

Data Representation:	ans-24
----------------------	--------

Data Field:	Contents of positions 20–43
-------------	-----------------------------

Justification:	Left-justified with trailing spaces
----------------	-------------------------------------

---

**Values**

Sender name, payer name, or user ID value up to 24 character spaces.

---

**Application Notes**

Subfield 2 is required for *MoneySend* Payment Transactions and must be properly formatted. Subfield 2 is optional for *MoneySend* Funding Transactions.

---

## **Subfield 3—Sender/Payer Address**

DE 124, subfield 3 (Sender/Payer/Address) contains sender/payer address data.

---

**Attributes**

Data Representation:	ans-91
----------------------	--------

Data Field:	Contents of positions 44–134
-------------	------------------------------

Justification:	Left-justified with trailing spaces
----------------	-------------------------------------

---

**Values**

## Data Element Definitions

### DE 124—Member-defined Data

---

Street address (ans-50)  
City (ans-25)  
State/Province Code (ans-3)  
Country Code (ans-3)  
Postal Code (ans-10)

---

#### Application Notes

---

Subfield 3 is required for *MoneySend* Payment Transactions and must be properly formatted. Subfield 3 is optional for *MoneySend* Funding Transactions

---

## Subfield 4—Reserved For Future Use

DE 124, (Reserved for Future Use) is reserved.

---

#### Attributes

---

Data Representation: ans-65

---

Data Field: Contents of positions 135-199

---

Justification: Left-justified with trailing spaces

---

#### Values

---

Optional Reserved data is formatted as follows:

Telephone number (n-20)

Optional message (ans-45)

---

## Subfield 6—Discretionary Message on Sales Slip Supported

DE 124, subfield 6 (Discretionary Message on Sales Slip Supported), used in association with Maestro credit in Brazil, is sent by the acquirer in the Authorization Request/0100 message, to indicate whether the POS terminal supports the discretionary message on the sales slip.

---

#### Attributes

---

Data Representation: an-1

---

Data Field: Contents of position 1-6

---

Justification: N/A

---

#### Values

---

Valid value will consist of one of the following:

0 = no (Merchant terminal does not support the printing of messages sent by the issuer.)

1 = yes (Merchant terminal supports the printing of messages sent by the issuer.)

---

## **Subfield 7—Discretionary Message on Sales Slip Code**

DE 124, subfield 7 (Discretionary Message on Sales Slip Code) is sent by the issuer in the Authorization Request Response/0110 message, to indicate the number of the message to be printed on the sales slip

---

### **Attributes**

---

Data Representation: an-3

---

Data Field: Contents of positions 7–9

---

Justification: Left

---

### **Values**

---

Valid value will contain the number of the message to be printed on the sales slip.

---

## **Subfield 8—Discretionary Message on Sales Slip Content**

DE 124, subfield 8 (Discretionary Message on Sales Slip Content) contains the variable part of the message to be printed on the sales slip.

---

### **Attributes**

---

Data Representation: an-10

---

Data Field: Contents of positions 10–19

---

Justification: Left

---

### **Values**

---

Valid value will consist of the variable part of the message to be printed on the sales slip.

---

## **Subfield 9—Phoneshop (Phone Company ID)**

DE 124, subfield 9 (Phoneshop [Phone Company ID]) is sent by the acquirer in the Authorization Request/0100 message, to identify the telephone company that provides the service for the Phoneshop product (for example, Telefonica = 01).

---

### **Attributes**

---

Data Representation: an-2

---

Data Field: Contents of positions 20–21

---

Justification: Left

---

### **Values**

---

Valid value will consist of the phone company ID.

---

## Data Element Definitions

### DE 124—Member-defined Data

---

#### Subfield 10—Phoneshop (Cell Phone Number)

DE 124, subfield 10 (Phoneshop [Cell Phone Number]) is sent by the acquirer in the Authorization Request/0100 message, to indicate the cardholder cell phone number for the Phoneshop product.

---

##### Attributes

---

Data Representation: n-10

---

Data Field: Contents of positions 22–31

---

Justification: Right

---

##### Values

---

Valid value will consist of the cell phone number.

---

#### Subfield 11—Phoneshop (Message Security Code)

DE 124, subfield 11 (Phoneshop [Message Security Code]) is sent by the issuer in the Authorization Request Response/0110 message, to indicate the security code that the merchant sent for validation.

---

##### Attributes

---

Data Representation: an-4

---

Data Field: Contents of positions 32–35

---

Justification: Left

---

##### Values

---

Valid value will consist of the message security code.

---

#### Subfield 12—Merchant CNPJ Number

DE 124, subfield 12 (Merchant CNPJ Number) is sent by the acquirer in the Authorization Request/0100 message, to indicate the Merchant CNPJ number.

---

##### Attributes

---

Data Representation: n-14

---

Data Field: Contents of positions 36–49

---

Justification: Right

---

##### Values

---

Valid value will consist of the Merchant CNPJ Number (a registration number provided by the government to all merchants).

---

## Subfield 13—Total Annual Effective Cost

DE 124, subfield 13 (Total Annual Effective Cost) is sent by the issuer in the Authorization Request Response/0110 message, to indicate the total annual effective cost in a financing transaction. A financing transaction includes purchase or cash withdrawal using a credit card.

### Attributes

Data Representation:	n-6
----------------------	-----

Data Field:	Contents of positions 50–55
-------------	-----------------------------

Justification:	Right
----------------	-------

### Values

Note: Optionally, issuers may submit spaces preceding the positional start of subfield 13. Data submitted for this subfield should begin in position 50.

Valid value will consist of the total annual effective cost in a financing transaction (including interest amount, taxes, and fees charged to the cardholder). This amount is mandated by local law number 3517 (implemented to ensure the cardholder is enforced about the total effective cost of the transaction.) This applies to purchase or cash withdrawal at an ATM using a credit card.

## DE 125—New PIN Data

DE 125 (New PIN Data) consists of a binary block containing a derived encrypted value calculated from the new PIN introduced by the cardholder at the ATM offering the PIN change service.

### Attributes

Length of Length Field:	N/A
-------------------------	-----

Data Representation:	b-8
----------------------	-----

Data Field:	Contents of bit positions 1-64 (8 bytes)
-------------	--

Subfields:	N/A
------------	-----

Justification:	N/A
----------------	-----

### Usage

Following is the usage of DE 125 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Authorization Request/0100	C	X	C
----------------------------	---	---	---

## Data Element Definitions

### DE 126—Private Data

---

#### Values

---

DE 125 contains the new PIN, which is formatted into one of the supported PIN block formats and is then encrypted. The PIN block format and encryption method used must be the same as the one used for the existing PIN that is stored in DE 52. DE 125 is only required in Authorization Request/0100—PIN Change messages. Otherwise, it must not be present.

---

## DE 126—Private Data

DE 126 (Private Data) is reserved for future use.

---

#### Attributes

---

Length of Length Field:	3
Data Representation:	ISO: ans...999; LLLVAR
	MasterCard: ans...100; LLLVAR
Data Field:	Contents of positions 1–100
Subfields:	N/A
Justification:	N/A

---

#### Usage

---

By provision of the ISO 8583–1987 specification, MasterCard defined this data element for use as “Private Data” available for MasterCard’s optional use for additional acquirer data.

The Authorization Platform does not pass data placed in this data element through to the message receiver; rather, the Authorization Platform temporarily stores the data. The Authorization Platform does not return this data to the message originator in any subsequent response to an original Request, Advice, Response, or Acknowledgement message.

---

#### Values

---

The length subelement must be in the range 001–100.

---

#### Application Notes

---

This data element is defined and used identically within all MasterCard programs and services.

---

## DE 127—Private Data

DE 127 (Private Data) may contain any private-use data that the customer may want to include in a message. Any Authorization Platform message originator may use DE 127.

<b>Attribute</b>	<b>Description</b>		
Length of Length Field:	3		
Data Representation:	ISO: ans...999; LLLVAR MasterCard: ans...100; LLLVAR		
Data Field:	Contents of positions 1–100		
Subfields:	N/A		
Justification:	N/A		
<b>Usage</b>			
Following is the usage of DE xx (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:			
	Org	Sys	Dst
Authorization Request/0100	O	X	•
Authorization Request Response/0110	O	X	CE
Authorization Advice/0120—Acquirer-generated	O	X	•
Authorization Advice Response/0130—System-generated	•	X	CE
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated 0120)	CE	X	CE
Authorization Acknowledgement/0180	CE	CE	•
Authorization Negative Acknowledgement/0190	•	X	CE
Issuer File Update Request/0302	O	X	•
Issuer File Update Request Response/0312	•	X	CE
Reversal Request Response/0410	O	X	CE
Reversal Advice/0420	•	X	CE
Reversal Advice Response/0430	CE	CE	•
Administrative Request/0600	O	X	•
Administrative Request Response/0610	•	X	CE
Administrative Advice/0620	•	O	O
Administrative Advice Response/0630	•	X	CE
Network Management Request/0800	O	X	•
Network Management Request/0800—PEK Exchange—On Demand	O	X	•
Network Management Request Response/0810	•	X	CE

## Data Element Definitions

### DE 128—Message Authentication Code

---

#### Values

---

The length must be in the range 001–100.

---

#### Application Notes

---

Data placed in DE 127 is not passed through to the message receiver; rather, the Authorization Platform temporarily stores the data and returns it to the message originator in any subsequent response to an original Request, Advice, Response, or Acknowledgement message.

This data element is defined and used identically within all MasterCard programs and services.

Acquirers that provide DE 127 in the Authorization Request/0100 message will receive the first twenty bytes of the value provided in DE 072 (Data Record) of IPM Fee Collection/1740–783 for interregional non-financial ATM transactions.

---

## DE 128—Message Authentication Code

DE 128 (Message Authentication Code [MAC]) validates the source and the text of the message between the sender and the receiver.

---

#### Attributes

---

Length of Length Field:	2
Data Representation:	b-8
Data Field:	Contents of bit positions 1–64 (8 bytes)
Subfields:	N/A
Justification:	N/A

---

#### Usage

---

May contain message authentication code as defined by ISO standards.

---

#### Values

---

Not applicable.

---

#### Application Notes

---

This data element should not be present in any Authorization Platform message.

The last bit position within any bit map is reserved for DE 128. If authentication is to be used on a message, the MAC information is indicated by the final bit of the final bit map of that message. The final bit of all preceding bit maps shall contain zero; for example, there shall be only one DE 128 per message and that DE 128 must be the last data element of the message.

---

---

## **Chapter 5 Program and Service Format Requirements**

*This section provides program specific message information.*

---

Product Value Constraints .....	5-1
Permitted Transactions by Card Program.....	5-1
Value Constraints by Transaction Type .....	5-5
Account Status Inquiry Service .....	5-8
Authorization Request/0100—Account Status Inquiry .....	5-10
Authorization Request Response/0110—Account Status Inquiry .....	5-10
Authorization Platform Edits .....	5-11
Address Verification Service .....	5-11
Authorization Request/0100—AVS and Authorization Request .....	5-12
Authorization Request Response/0110—AVS and Authorization Request .....	5-13
Network Management Request/0800—AVS Sign-on .....	5-14
Alternate Processing .....	5-14
DE 48 and DE 120 Structure in AVS Transactions .....	5-14
Authorization Platform Edits .....	5-15
Automated Fuel Dispenser Completion .....	5-16
AFD Message Scenarios .....	5-16
Authorization Request/0100—Automated Fuel Dispenser Completion.....	5-17
Authorization Advice/0120—Acquirer-generated (Automated Fuel Dispenser Completion).....	5-17
Authorization Advice/0120—Acquirer-generated (Automated Fuel Dispenser Completion).....	5-18
Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated) .....	5-20
Alternate Processing .....	5-20
Account Level Management .....	5-21
Enhanced Value and Product Graduation in Dual Message System Processing.....	5-21
High Value in Dual Message System Processing.....	5-24
ATM Bill Payment Service .....	5-25
Authorization Request/0100—ATM Bill Payment, Europe Acquired.....	5-25
Authorization Request/0100—ATM Bill Payment, Non-Europe Acquired .....	5-26
Authorization Platform Edits .....	5-27
ATM Credit Card Cash Advance in Installments.....	5-27
Authorization Request/0100—ATM Installment Inquiry .....	5-27
Authorization Request Response/0110—ATM Installment Inquiry .....	5-28

## **Program and Service Format Requirements**

---

Authorization Request/0100—ATM Installment Withdrawal .....	5-29
Authorization Request Response/0110—ATM Installment Withdrawal .....	5-30
Balance Inquiry—ATM.....	5-31
Authorization Request/0100—ATM Balance Inquiry .....	5-31
Authorization Request/0100—ATM Balance Inquiry Edits .....	5-32
Authorization Request Response/0110—ATM Balance Inquiry .....	5-32
Authorization Request Response/0110—ATM Balance Inquiry Edits .....	5-33
Authorization Advice/0120—Acquirer-generated—ATM Balance Inquiry Edits .....	5-34
Alternate Processing .....	5-34
Balance Inquiry—Point-of-Sale .....	5-34
Authorization Request/0100—POS Balance Inquiry .....	5-35
Authorization Request Response/0110—POS Balance Inquiry .....	5-36
Authorization Request/0100—POS Balance Inquiry Edits.....	5-36
Authorization Request/0110—POS Balance Inquiry Edits.....	5-37
Authorization Advice/0120—Acquirer-generated—POS Balance Inquiry Edits.....	5-38
Alternate Processing .....	5-39
Balance Inquiry—Short Message Service .....	5-39
Authorization Request/0100—Short Message Service Balance Inquiry .....	5-39
Balance Inquiry—Mobile Remote Payments Program .....	5-40
Authorization Request/0100—Mobile Remote Payments Program Balance Inquiry.....	5-40
Chip-Specific Value Constraints .....	5-40
Chip Partial Grade Value Constraints .....	5-41
Chip Full Grade Value Constraints.....	5-42
Contact and Contactless Chip Specific Value Constraints.....	5-42
Card Validation Code 2 .....	5-44
Authorization Request/0100—CVC 2 Verified .....	5-44
Authorization Request/0100—CVC 2 Unverified.....	5-45
Authorization Request/0100—CVC 2 Processed by Stand-In .....	5-46
Authorization Request/0100—CVC 2 Processed by X-Code .....	5-47
Authorization Request/0100—Processed by Limit-1.....	5-48
CVC 2 DE 48 Structure.....	5-48
Authorization Request/0100—CVC 2 .....	5-49
Authorization Request Response/0110—CVC 2 .....	5-49
Card Validation Code 3 .....	5-50
Authorization Request Response/0110—CVC 3 Result.....	5-50
Currency Conversion .....	5-50
Amount-Related Data Elements in Authorization and Reversal Messages.....	5-51
Dual Message System Processing.....	5-53

Acquirer Send MTIs in Authorization and Reversal Messages.....	5-53
Acquirer Receive MTIs in Authorization and Reversal Messages .....	5-54
Issuer Receive MTIs in Authorization and Reversal Messages .....	5-55
Issuer Send MTIs in Authorization and Reversal Messages.....	5-56
Currency Conversion in RiskFinder Transactions.....	5-57
Alternate Processing .....	5-57
Authorization Platform Edits .....	5-58
Electronic Commerce Processing.....	5-60
No Security Protocol .....	5-61
Channel Encryption .....	5-62
Authorization Request/0100—Electronic Commerce Purchase .....	5-63
Authorization Request Response/0110—Electronic Commerce Purchase .....	5-65
Authorization Platform Edits .....	5-65
MasterCard <i>SecureCode</i> .....	5-66
Static AAV and the Maestro and MasterCard Advance Registration Programs.....	5-68
Forgotten Card at ATM.....	5-69
Reversal Request/0400—Forgotten Card.....	5-69
Fraud Scoring Service .....	5-70
Authorization Request/0100—Fraud Scoring .....	5-70
Alternate Processing .....	5-71
Gaming Payment Transactions.....	5-71
Authorization Request/0100—Gaming Payment .....	5-71
Reversal Request/0400—Gaming Payment .....	5-72
Authorization Platform Edits .....	5-73
Maestro Pre-authorized Transactions .....	5-73
Authorization Request/0100—Maestro Pre-Authorization .....	5-73
Authorization Advice/0120—Maestro Pre-Authorization Completion .....	5-74
Maestro Recurring Payments Program .....	5-74
Authorization Request/0100—Maestro Recurring Payment.....	5-76
Authorization Platform Edits .....	5-76
Magnetic Stripe Compliance .....	5-78
Authorization Request/0100—Magnetic Stripe-read.....	5-79
Authorization Request Response/0110—Magnetic Stripe-read.....	5-80
MasterCard Hosted Mobile Phone Top-up ATM Transactions.....	5-80
Authorization Request/0100—MasterCard Hosted Mobile Phone Top-up .....	5-81
Authorization Platform Edits .....	5-82
MasterCard inControl Service.....	5-83

## **Program and Service Format Requirements**

---

Authorization Request/0100—inControl Purchase Control .....	5-83
Dual Message System Processing.....	5-84
MasterCard inControl Real Card Spend Control.....	5-86
Process of a MasterCard inControl Service Eligible Transaction .....	5-86
Authorization Request/0100—inControl Real Card Spend Control .....	5-88
Authorization Advice/0120—inControl Real Card Spend Control .....	5-88
MasterCard inControl Virtual Card Mapping and Spend Control Service.....	5-89
Authorization Request/0100—inControl Virtual Card Mapping and Spend Control Service .....	5-89
Exception Processing.....	5-89
MasterCard <i>MoneySend</i> .....	5-90
Authorization Request/0100—MasterCard <i>MoneySend</i> Funding Transactions.....	5-92
Reversal Request/0400—MasterCard <i>MoneySend</i> Funding Transaction .....	5-93
Authorization Platform Edits .....	5-94
Authorization Request/0100—MasterCard <i>MoneySend</i> Payment Transactions .....	5-94
Reversal Request/0400—MasterCard <i>MoneySend</i> Payment Transaction.....	5-95
Authorization Platform Edits .....	5-96
Merchant Advice Codes .....	5-98
Merchant Advice Codes Used with Response Codes .....	5-98
M/Chip Processing Services .....	5-99
Program use of M/Chip Processing Service Data Elements .....	5-100
Chip To Magnetic Stripe Conversion .....	5-101
Authorization and Stand-In Processing.....	5-102
M/Chip Cryptogram Pre-validation .....	5-105
Validation of the Application Cryptogram.....	5-106
Generation of the Issuer Chip Authentication Data .....	5-107
DE 60 (Advice Reason Code) .....	5-108
Combined Service Option.....	5-109
M/Chip Cryptogram Validation in Stand-In Processing.....	5-109
Validation of the Application Cryptogram.....	5-110
Generation of the Issuer Chip Authentication Data .....	5-111
DE 60—Advice Reason Code.....	5-112
Mobile Remote Payments .....	5-113
Authorization Platform Edits .....	5-114
Partial Approvals.....	5-115
Authorization Request/0100—Partial Approval.....	5-115
Authorization Request Response/0110—Partial Approval.....	5-116
Reversal Request/0400—Partial Approval .....	5-117

Reversal Advice/0420—Partial Approval.....	5-117
Authorization Advice/0120—Issuer-generated (to RiskFinder) .....	5-118
Authorization Advice/0120—Acquirer-generated.....	5-118
Alternate Processing .....	5-119
Authorization Platform Edits .....	5-119
Payment Transactions .....	5-121
Authorization Request/0100—Payment Transaction Message .....	5-121
Authorization Request Response/0110—Payment Transaction .....	5-122
Authorization Platform Edits .....	5-123
PayPass CVC 3 Processing Service .....	5-125
Authorization Request/0100—CVC 3 .....	5-126
Dynamic CVC 3 Application Transaction Counter (ATC) Processing .....	5-127
Dynamic CVC 3 Application Transaction Counter (ATC) Information .....	5-128
MCC109 ( <i>PayPass Application Transaction Counter File</i> ).....	5-128
Authorization Platform Edits .....	5-129
Card Validation Code Result .....	5-130
Optional Non-valid CVC 3 Processing .....	5-130
ATC Data Extract File.....	5-131
Alternate Processing .....	5-132
PayPass Mapping Service for <i>PayPass M/Chip</i> and Contact <i>M/Chip</i> Transactions .....	5-132
<i>PayPass Mapping Service Processing of PayPass M/Chip and Contact M/Chip Transactions</i> .....	5-133
Authorization Platform Edits .....	5-134
Pay with Rewards Service .....	5-135
Authorization Request/0100—Pay with Rewards .....	5-135
Authorization Request Response/0110—Pay With Rewards .....	5-136
Authorization Platform Edits .....	5-137
PIN Management Service .....	5-140
Chip PIN Management Service .....	5-140
Authorization Request/0100—PIN Change (Chip Card).....	5-141
Authorization Request Response/0110—PIN Change (Chip Card) .....	5-142
Reversal Request/0400—PIN Change (Chip Card).....	5-143
Magnetic Stripe PIN Management Service.....	5-143
Authorization Request/0100—PIN Change (Magnetic Stripe Card).....	5-144
Authorization Request Response/0110—PIN Change (Magnetic Stripe Card).....	5-145
Reversal Request/0400—PIN Change (Magnetic Stripe Card) .....	5-145
Authorization Request/0100 Edits (Magnetic Stripe Card).....	5-146
Authorization Advice/0120—Acquirer-generated Edits (Magnetic Stripe Card) .....	5-148

## **Program and Service Format Requirements**

---

Reversal Request/0400 Edits (Magnetic Stripe Card).....	5-148
Issuer Response Options to a Magnetic Stripe PIN Change Request .....	5-149
PIN Processing for Europe Region Members .....	5-150
PIN Translation Edits .....	5-150
PIN Validation.....	5-151
PIN Validation Edits .....	5-153
PIN Key Management .....	5-156
PIN Verification Value (PVV)/PIN Offset on File Service .....	5-156
Processing Transactions Using PVV/PIN Offset .....	5-156
Processing Parameters .....	5-156
PVV/PIN Offset File Format.....	5-157
Alternate Processing .....	5-158
PIN Processing for non-Europe Members.....	5-159
Acquirer Requirements .....	5-159
Support either Static or Dynamic PIN Encryption Key (PEK) Exchanges .....	5-159
MasterCard Magnetic Stripe Compliance Program Compliance .....	5-160
Authorization Request/0100—PIN Transactions.....	5-160
Authorization Request Response/0110—PIN Transactions.....	5-161
Issuer Requirements.....	5-163
Receive Purchase Transactions that Contain a PIN .....	5-163
Support Static or Dynamic PEK Exchanges .....	5-163
Authorization Request/0100—PIN Messages.....	5-164
Authorization Advice/0120—PIN Messages .....	5-165
Reversal Advice/0420—PIN Messages .....	5-165
Alternate Processing .....	5-166
Support for Both Acquiring and Issuing Processing .....	5-166
Cleartext Use Prohibited .....	5-166
Emergency Static PEK or Emergency KEK Process .....	5-167
Previous PEKs.....	5-167
PIN Verification Value on File Service.....	5-167
PVV/PIN Offset File Format.....	5-168
Alternate Processing .....	5-169
PIN Translation and Verification Process .....	5-170
Detection of PEK Corruption Using Sanity Checks.....	5-173
Authorization Platform Sanity Check Error .....	5-174
Issuer Sanity Check Error.....	5-176
Private Label Processing .....	5-177
Authorization Request/0100—Private Label Processing .....	5-177

Authorization Platform Edits .....	5-178
Private Label with Balance Inquiry .....	5-178
Authorization Request/0100—Private Label with Balance Inquiry.....	5-178
Merchant Verification Service.....	5-178
Authorization Platform Edits .....	5-179
Co-brand Proprietary Transaction Management Service .....	5-179
Alternate Processing .....	5-181
Card Activation for Private Label Processing .....	5-181
Authorization Request/0100 and Reversal Request/0400—Card Activation at Point of Sale .....	5-182
Alternate Processing .....	5-183
Authorization Platform Edits .....	5-184
Card Activation Plus Initial Load for Private Label Processing.....	5-185
Product Inquiry Service .....	5-186
Authorization Request/0100—Product Inquiry Service .....	5-187
Proximity Payments .....	5-187
Authorization Request/0100—Proximity Payments.....	5-187
Purchase of Goods or Services with Cash Back.....	5-189
Authorization Request/0100—Purchase of Goods or Services with Cash Back .....	5-189
Issuer Response Options .....	5-190
Reversal Request/0400 .....	5-191
Reversal Advice/0420.....	5-192
Authorization Advice/0120.....	5-192
Authorization Advice/0120—Acquirer-generated.....	5-193
Alternate Processing .....	5-193
Authorization Platform Edits .....	5-194
Real-time Substantiation.....	5-197
Participation in Real-time Substantiation.....	5-197
Merchant Terminal Verification .....	5-198
Real-time Substantiation Amounts .....	5-198
Transaction Processing Examples .....	5-199
Authorization Platform Edits .....	5-202
Recurring Payment Test Transactions .....	5-204
Reversal Processing.....	5-205
Full Reversals.....	5-205
Partial Reversals .....	5-205
Reversals of Balance Inquiry Transactions.....	5-205
Reversals of Purchase of Goods or Services with Cash Back Transactions.....	5-206

## **Program and Service Format Requirements**

---

Alternate Processing .....	5-207
Authorization Platform Edits .....	5-208
RiskFinder.....	5-209
Authorization Advice/0120—To RiskFinder .....	5-209
Authorization Advice Response/0130—From RiskFinder.....	5-210
Network Management/08xx—To and From RiskFinder.....	5-210
Administrative Advice/0620 .....	5-211
DE 120 Layout for RiskFinder .....	5-212
Administrative Advice Response/0130 .....	5-216
Transaction Blocking .....	5-216
Transaction Block Setup Configuration.....	5-216
Authorization Platform Edits .....	5-217
Transaction Blocking for Inactive BINs.....	5-217
Authorization Platform Edits .....	5-217
Visa Custom Payment Service.....	5-218
Authorization Request/0100—Visa Custom Payment Service.....	5-218
Authorization Request Response/0110—Visa Custom Payment Service .....	5-219
DE 48 Structure in a Visa Custom Payment Service Transaction.....	5-220
Visa Programs .....	5-221
Visa CVV2 .....	5-221
Authorization Request/0100—Visa CVV2.....	5-221
Authorization Request Response/0110—Visa CVV2.....	5-222
Visa Fleet Card ID.....	5-222
Authorization Request/0100—Visa Fleet Card ID .....	5-222
Visa Commercial Card Inquiry .....	5-223
Authorization Request/0100—Visa Commercial Card Inquiry.....	5-223
Authorization Request Response/0110—Visa Commercial Card Inquiry.....	5-223

## Product Value Constraints

Product value constraints list types of transactions permitted by card program, and the inter-related value constraints for certain data elements carried in the Authorization Platform messages.

The business rules related to the card programs MasterCard supports differentiate between the nature of the transactions permitted for:

- MCC (MasterCard)
- DMC (Debit MasterCard)
- MSI (Maestro)
- CIR (Cirrus)
- MCE (MasterCard Electronic)
- PVL (Private Label)

## Permitted Transactions by Card Program

Following are the types of transactions permitted by card program and the inter-related value constraints for certain data elements in Authorization Platform messages.

The inter-related data elements are:

- DE 3 (Processing Code)
- DE 22 (Point-of-Service [POS] Entry Mode)
- DE 61 (Point-of-Service [POS] Data)

**Table 5.1–Permitted Transactions by Card Program**

Use the reference number in the Ref column in the following table with the specific value constraints in Table 5.2.

Ref	Transaction Type	PAN Entry Mode	No CVM	MCC	DMC	MSI	CIR	MCE	PVL
<b>ATM Withdrawal</b>									
1.1	ATM <sup>1</sup>	Magnetic Stripe	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X	X		
1.2	ATM <sup>1</sup>	Chip	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X	X		
<b>Cash Advance</b>									

1. For this message, DE 18 must contain value 6011 (Automated Cash Disbursement)

## Program and Service Format Requirements

### Product Value Constraints

Ref	Transaction Type	PAN Entry Mode	No CVM	MCC	DMC	MSI	CIR	MCE	PVL
2.1	Cash Advance <sup>2</sup>	Manual	Signature	X	X				
2.2	Cash Advance <sup>2</sup>	Magnetic Stripe	Signature	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	
2.3	Cash Advance <sup>2</sup>	Magnetic Stripe	Online PIN	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	
2.4	Cash Advance <sup>2</sup>	Chip	Offline PIN	X	X			X	
2.5	Cash Advance <sup>2</sup>	Chip	Online PIN	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	
2.6	Cash Advance <sup>2</sup>	Chip	Signature	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	
2.7	Electronic Cash Advance <sup>2</sup>	Magnetic Stripe	Online PIN			X	X		
2.8	Electronic Cash Advance <sup>2b</sup>	Chip	Offline PIN			X	X		
2.9	Electronic Cash Advance <sup>2</sup>	Chip	Online PIN			X	X		
<b>Purchase of Goods and Services</b>									
3.1	Purchase	Manual	Signature	X	X			X	
3.2	Purchase	Magnetic Stripe	Signature	X <sup>a</sup>	X <sup>a</sup>	X <sup>c</sup>		X <sup>a</sup>	X
3.3	Purchase	Magnetic Stripe	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X		X <sup>a</sup>	
3.4	Purchase	Chip	Offline PIN	X	X	X		X	
3.5	Purchase	Chip	Signature	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	X
3.6	Purchase	Chip	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X		X <sup>a</sup>	
3.7	Purchase	Chip	No CVM			X <sup>a</sup>			
3.8	CAT Level 1	Magnetic Stripe	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X	X		
3.9	CAT Level 1	Chip	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X			
3.10	CAT Level 1	Chip	Offline PIN	X <sup>a</sup>	X <sup>a</sup>	X <sup>a</sup>			

2. For this message, DE 18 must contain value 6010 (Manual Cash Disbursement)

## Program and Service Format Requirements

### Product Value Constraints

<b>Ref</b>	<b>Transaction Type</b>	<b>PAN Entry Mode</b>	<b>No CVM</b>	<b>MCC</b>	<b>DMC</b>	<b>MSI</b>	<b>CIR</b>	<b>MCE</b>	<b>PVL</b>
3.11	CAT Level 2	Magnetic Stripe	No CVM	X <sup>a</sup>	X <sup>a</sup>	X <sup>a</sup>			X
3.12	CAT Level 2	Chip	No CVM	X <sup>a</sup>	X <sup>a</sup>	X <sup>a</sup>			X
3.13	CAT Level 3 <sup>d</sup>	Magnetic Stripe	No CVM	X <sup>a</sup>	X <sup>a</sup>				X
3.14	CAT Level 3 <sup>d</sup>	Chip	No CVM	X <sup>a</sup>	X <sup>a</sup>				X
3.15	CAT Level 4	Magnetic Stripe	No CVM	X	X	X <sup>a</sup>			X
3.16	CAT Level 4	Chip	No CVM	X	X	X <sup>a</sup>			X
3.17	MO/TO	Manual	No CVM	X	X	X <sup>f</sup>			X
3.18	CAT Level 6	Electronic Commerce	No CVM	X	X	X		X <sup>d</sup>	X
3.19	CAT Level 6	Electronic Commerce	Offline PIN	X	X	X			
3.20	CAT Level 6	Electronic Commerce	Online PIN	X	X	X			
3.21	CAT Level 7	N/A <sup>e</sup>	N/A <sup>e</sup>	X	X				X
<b>Payments</b>									
4.1	Payment Transactions	N/A <sup>e</sup>	No CVM	X	X	X		X	X
<b>PIN Change Management</b>									
5.1	ATM PIN unblock <sup>1</sup>	Chip	Online PIN	X	X	X	X	X	X
5.2	ATM PIN change <sup>1</sup>	Chip	Online PIN	X	X	X	X	X	X
5.3	ATM PIN change <sup>1</sup>	Magnetic Stripe	Online PIN	X	X	X	X	X	X
<b>Balance Inquiry</b>									
6.1	ATM Balance Inquiry <sup>1 g</sup>	Magnetic Stripe	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X	X	X <sup>a</sup>	
6.2	ATM Balance Inquiry <sup>1 g</sup>	Chip	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X	X	X <sup>a</sup>	
6.3	POS Balance Inquiry <sup>h</sup>	Magnetic Stripe	Signature	X <sup>a</sup>	X <sup>a</sup>	X		X <sup>a</sup>	X

## Program and Service Format Requirements

### Product Value Constraints

Ref	Transaction Type	PAN Entry Mode	No CVM	MCC	DMC	MSI	CIR	MCE	PVL
6.4	POS Balance Inquiry <sup>h</sup>	Magnetic Stripe	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X	X	X <sup>a</sup>	X
6.5	POS Balance Inquiry <sup>h</sup>	Chip	Offline PIN	X	X	X		X	X
6.6	POS Balance Inquiry <sup>h</sup>	Chip	Signature	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	X
6.7	POS Balance Inquiry <sup>h</sup>	Chip	Online PIN	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	X
6.8	SMS Balance Inquiry	eCommerce	No CVM	X	X				

### Purchase with Cash Back (PWCB)

7.1	PWCB	Magnetic Stripe	Signature	X <sup>j</sup>	X <sup>a</sup>				
7.2	PWCB	Magnetic Stripe	Online PIN	X <sup>j</sup>	X				
7.3	PWCB	Chip	Offline PIN	X <sup>j</sup>	X				
7.4	PWCB	Chip	Online PIN	X <sup>j</sup>	X				
7.5	PWCB	Manual	Signature			X <sup>i</sup>			

### Refund

8.1	Refund <sup>h</sup>	Manual	Signature	X	X				X
8.2	Refund <sup>h</sup>	Magnetic Stripe	Signature	X <sup>a</sup>	X <sup>a</sup>	X			X
8.3	Refund <sup>h</sup>	Magnetic Stripe	Online PIN			X			
8.4	Refund <sup>h</sup>	Chip	Signature	X <sup>a</sup>	X <sup>a</sup>				
8.5	Refund <sup>h</sup>	Chip	Online PIN			X <sup>a</sup>			
8.6	Refund <sup>h</sup>	Chip	Offline PIN	X	X	X <sup>a</sup>			

Ref	Transaction Type	PAN Entry Mode	No CVM	MCC	DMC	MSI	CIR	MCE	PVL
8.7	Refund <sup>h</sup>	Chip	No CVM			X <sup>a</sup>			

**Table Key:**<sup>a</sup> PayPass transactions permitted. No CVM is required for transactions under PayPass limits.<sup>b</sup> A waiver is required for this item. Issuers must register.<sup>c</sup> Country restrictions apply.<sup>d</sup> Only allowed for MasterCard Electronic Card transactions when SecureCode UCAF data is present.<sup>e</sup> No specific constraints defined.<sup>f</sup> By domestic agreement only.<sup>g</sup> Applies to prepaid cards only.<sup>h</sup> Refund Transactions apply only to Private Label and Swedish Domestic Authorization Switching Service (SASS).<sup>i</sup> Applies to UK Domestic Maestro only.<sup>j</sup> Approved domestic countries, as indicated in *MasterCard Rules*.

## Value Constraints by Transaction Type

Following are value constraints by transaction type.

**Table 5.2–Value Constraints by Transaction Type**

Ref	Transaction Type, PAN Entry Mode, and Cardholder Verification Method	DE 3 values	DE 22 values	CVM Method	DE 61, SF 10 values
<b>ATM Withdrawal</b>					
1.1	ATM, Magnetic Stripe, Online PIN <sup>3</sup>	010000	901 or 91x (or 801)	P	0 or 1
1.2	ATM, Chip, Online PIN <sup>3</sup>	010000	051 or 071	P	0 or 1
<b>Cash Advance</b>					
2.1	Cash Advance, Manual, Signature <sup>4</sup>	170000	00x, 01x (or 79x)	S	0
2.2	Cash Advance, Magnetic Stripe, Signature <sup>4</sup>	170000	90x or 91x (or 80x)	S	0
2.3	Cash Advance, Magnetic Strip, Online PIN <sup>4</sup>	170000	90x or 91x (or 80x)	P	0
2.4	Cash Advance, Chip, Offline PIN <sup>4</sup>	170000	051	S	0
2.5	Cash Advance, Chip Online PIN <sup>4</sup>	170000	051 or 071	P	0

3. For this message, DE 18 must contain value 6011 (Automated Cash Disbursement)

4. For this message, DE 18 must contain value 6010 (Manual Cash Disbursement)

## Program and Service Format Requirements

### Product Value Constraints

Ref	Transaction Type, PAN Entry Mode, and Cardholder Verification Method	DE 3 values	DE 22 values	CVM Method	DE 61, SF 10 values
2.6	Cash Advance, Chip, Signature <sup>4</sup>	170000	05x or 07x	S	0
2.7	Electronic Cash Advance, Magnetic Stripe, Online PIN <sup>4</sup>	010000	901	P	0
2.8	Electronic Cash Advance, Chip, Offline PIN <sup>4</sup>	010000	051	S	0
2.9	Electronic Cash Advance, Chip Online PIN <sup>4</sup>	010000	051	P	0
<b>Purchase of Goods and Services</b>					
3.1	Purchase, Manual, Signature	00xx00	00x, 01x (or 79x)	S	0
3.2	Purchase, Magnetic Stripe, Signature	00xx00	90x or 91x (or 80x)	S	0
3.3	Purchase, Magnetic Stripe, Online PIN	00xx00	901 or 911 (or 80x)	P	0
3.4	Purchase, Chip, Offline PIN	00xx00	051	S	0
3.5	Purchase, Chip, Signature	00xx00	05x or 07x	S	0
3.6	Purchase, Chip, Online PIN	00xx00	051 or 071	P	0
3.7	Purchase, Chip, No CVM	00xx00	05x or 07x	S	0
3.8	CAT Level 1, Magnetic Stripe, Online PIN	00xx00	901 or 911 (or 801)	P	1
3.9	CAT Level 1, Chip, Online PIN	00xx00	051 or 071	P	1
3.10	CAT Level 1, Chip, Offline PIN	00xx00	051	S	1
3.11	CAT Level 2, Magnetic Stripe, No CVM	00xx00	90x or 91x (or 80x)	S	2
3.12	CAT Level 2, Chip, No CVM	00xx00	05x or 07x	S	2
3.13	CAT Level 3, Magnetic Stripe, No CVM	00xx00	90x or 91x (or 80x)	S	3
3.14	CAT Level 3, Chip, No CVM	00xx00	05x or 07x	S	3
3.15	CAT Level 4, Magnetic Stripe, No CVM	00xx00	90x (or 80x)	S	4
3.16	CAT Level 4, Chip, No CVM	00xx00	05x	S	4
3.17	MO/TO, Manual, No CVM	00xx00	01x	S	0
3.18	CAT Level 6, Electronic Commerce, No CVM	00xx00	81x or 82x	S	6

## Program and Service Format Requirements

### Product Value Constraints

<b>Ref</b>	<b>Transaction Type, PAN Entry Mode, and Cardholder Verification Method</b>	<b>DE 3 values</b>	<b>DE 22 values</b>	<b>CVM Method</b>	<b>DE 61, SF 10 values</b>
3.19	CAT Level 6, Electronic Commerce, Offline PIN	00xx00	81x	S	6
3.20	CAT Level 6, Electronic Commerce, Online PIN	00xx00	81x or 82x	P	6
3.21	CAT Level 7	00xx00	No constraints	No constraints	7
<b>Payments</b>					
4.1	Payment Transactions, No CVM	280000	No constraints	S	No constraints
<b>PIN Change Management</b>					
5.1	ATM PIN unblock, Chip, Online PIN <sup>3</sup>	910000	051	P	0 or 1
5.2	ATM PIN change, Chip, Online PIN <sup>3</sup>	920000	051	P	0 or 1
5.3	ATM PIN change Magnetic Stripe, Online PIN	920000	021 or 901	P	0 or 1
<b>Balance Inquiry</b>					
6.1	ATM Balance Inquiry, Magnetic Stripe, Online PIN <sub>3</sub>	30xx00	901 or 911	P	0 or 1
6.2	ATM Balance Inquiry, Chip, Online PIN	30xx00	051 or 071	P	0 or 1
6.3	POS Balance Inquiry, Magnetic Stripe, Signature	300000 or 303000	90x or 91x (or 80x)	S	0
6.4	POS Balance Inquiry, Magnetic Stripe, Online PIN	300000 or 303000	901 or 911 (or 801)	P	0
6.5	POS Balance Inquiry, Chip, Offline PIN	300000 or 303000	051	S	0
6.6	POS Balance Inquiry, Chip, Signature	300000 or 303000	05x or 07x	S	0
6.7	POS Balance Inquiry, Chip, Online PIN	300000 or 303000	051 or 071	P	0
6.8	SMS Balance Inquiry				
<b>Purchase with Cash Back (PWCB)</b>					

## Program and Service Format Requirements

### Account Status Inquiry Service

Ref	Transaction Type, PAN Entry Mode, and Cardholder Verification Method	DE 3 values	DE 22 values	CVM Method	DE 61, SF 10 values
7.1	PWCB, Magnetic Stripe, Signature	09xx00	90x (or 80x)	S	0
7.2	PWCB, Magnetic Stripe, Online PIN	09xx00	901 (or 801)	P	0
7.3	PWCB, Chip Offline PIN	09xx00	051	S	0
7.4	PWCB, Chip Online PIN	09xx00	051	P	0
7.5	PWCB, Manual, Signature	09xx00	01x	S	0
<b>Refund</b>					
8.1	Refund, Manual, Signature	20xx00	00x or 01x	S	0
8.2	Refund, Magnetic Stripe, Signature	20xx00	90x or 91x (or 80x)	S	0
8.3	Refund, Magnetic Stripe, Online PIN	20xx00	901 (or 801)	P	0
8.4	Refund, Chip, Signature	20xx00	05x or 07x	S	0
8.5	Refund, Chip, Online PIN	20xx00	051	P	0
8.6	Refund, Chip, Offline PIN	20xx00	051	S	0

## Account Status Inquiry Service

Account Status Inquiry Service allows acquirers to send Account Status Inquiry transactions to validate aspects of a cardholder account.

### Acquirer Requirements

- Acquirers that choose to support Account Status Inquiry Service transactions must be able to send Authorization Request/0100 messages containing DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service) and DE 4 (Amount, Transaction) with a transaction amount of zero when submitting Account Status Inquiry Service transaction requests.
- Acquirers no longer may submit transactions with an amount greater than zero to check account status. Acquirers may continue to send USD 1 (or local currency equivalent) or less on status checks for Automated Fuel Dispenser (AFD) transactions indicated by DE 18 (Merchant Type, value MCC 5542 (Merchant Category Code) and aggregated MasterCard® PayPass™ transit transactions.
- Account Status Inquiry Service transactions may include requests for Address Verification Service (AVS), CVC 2 validation, or both, by the acquirer. Acquirers must include DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service Request), value 52 (AVS and Authorization Request/0100) for AVS requests and DE 48, subelement 92 (CVC 2) for CVC 2 requests.

- At the issuer's discretion, the acquirer may receive an Authorization Request Response/0110 message where DE 39 may contain either the value 00 (Approved), 05 (Do not honor), or 85 (Not declined). If the issuer is unable to reply, the acquirer will receive a response code of 91 (Authorization System or issuer system inoperative).

### **Issuer Requirements**

- Issuers must be able to receive Authorization Request/0100 messages containing DE 61, subfield 7, value 8, and DE 4 with a transaction amount of zero in Account Status Inquiry Service transaction requests.
- At a minimum, issuers must validate that the account is valid, that funds are available, and the account is not listed on the Electronic Warning Bulletin (EWB).
- Issuers must be able to receive AVS requests containing DE 48, subelement 82, value 52 and to respond with the appropriate value in DE 48, subelement 83 (Address Verification Service Response).
- Issuers must be able to receive CVC 2 requests in DE 48, subelement 92 and to respond with the appropriate value in DE 48, subelement 87.
- The issuer, at its discretion, will send the acquirer an Authorization Request Response/0110 message where DE 39 may contain either the value 00, 05, or 85. If the issuer is unable to reply, the acquirer will receive a response code of 91 (Authorization System or issuer system inoperative).

### **NOTE**

**DE 61, subfield 7, value 8 should not be included in any request type other than the Account Status Inquiry Service request or it will be rejected.**

Account Status Inquiry Service transactions are not supported for Authorization Advice/0120 and Reversal Request/0400 messages. If an acquirer sends an Authorization Advice/0120—Acquirer-generated or Reversal Request/0400 message, the acquirer will receive an automated reply from the Authorization Platform responding to the message where DE 39 contains value 12 (Invalid transaction). DE 39, value 12 will be sent back in an automated reply for all other message types.

### **Automated Fuel Dispenser Transactions and MasterCard PayPass Transit Transactions**

An Authorization Request/0100 message for an AFD transaction that includes DE 18 (Merchant Type), value of 5542 (Fuel Dispenser Automated) will continue to submit USD 1 (or local currency equivalent) authorization requests.

Aggregated MasterCard® PayPass™ transit transactions generated by the transit authority and held for a period of time before being cleared, will continue to submit USD 1 (or local currency equivalent) authorization requests.

## **Program and Service Format Requirements**

### **Account Status Inquiry Service**

## **Authorization Request/0100—Account Status Inquiry**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code)	M	•	M	00 = Purchase
DE 4 (Amount, Transaction)	M	•	M	Must be zero.
DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service)	C	•	C	52 = AVS and Authorization Request/0100
DE 48 (Additional Data—Private Use), subelement 92 (CVC 2)	C	•	C	CVC 2 value from the signature panel of the card when applicable.
DE 61 (Point-of-Service POS] Data), subfield 7 (POS Transaction Status)	M	•	M	8 = Account Status Inquiry Service

## **Authorization Request Response/0110—Account Status Inquiry**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code)	ME	•	ME	00 = Purchase
DE 4 (Amount, Transaction)	CE	X	M	Must be zero.
DE 39 (Response/Code)	M	•	M	00 = Approved 05 = Do not honor or 85 = Not declined
DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service)	CE	•	CE	52 = AVS and Authorization Request/0100
DE 48 (Additional Data—Private Use), subelement 83 (Address Verification Service Response)	C	•	C	The AVS verification response code.
DE 48 (Additional Data—Private Use), subelement 87 (Card Validation Code Result)	C	•	C	The CVC 2 result code.
DE 48 (Additional Data—Private Use), subelement 92 (CVC 2)	CE	•	CE	CVC 2 value from the signature panel of the card when applicable.

## Authorization Platform Edits

The Authorization Platform performs the following edits on Account Status Inquiry transactions.

WHEN...	THEN the Authorization Platform...
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains value 8 (Account Status Inquiry Service) and DE 4 (Amount, Transaction) contains a value other than zero	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format error)</li><li>• DE 44 (Additional Response Data) = 004 (indicating the data element in error)</li></ul>
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains value 8 (Account Status Inquiry Service) and DE 4 (Amount, Transaction) contains a value equal to zero and DE 3 (Processing Code) contains a value other than 00 (Purchase)	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 003</li></ul>
The acquirer sends an Authorization Advice/0120 or acquirer-generated Reversal Request/0400 message with the value combinations above	Sends the acquirer an Authorization Advice/0130 or Reversal Request Response/0410 message where DE 39 = 12 (Invalid transaction).

## Address Verification Service

Address Verification Service (AVS) is a fraud deterrent service that provides greater security to merchants and cardholders. It helps to protect against fraudulent use of cards by verifying the cardholder's billing address.

### How AVS Works

The acquirer requests the cardholder billing address verification as part of the Authorization Request/0100. The issuer performs the verification and returns the appropriate information to the acquirer in the Authorization Request Response/0110.

### Alternate Processing

The Stand-In and X-Code systems do not perform the Address Verification Service. Transactions that contain an AVS request in an Account Status Inquiry Service request will receive a response indicating the service is not available. Transactions that contain an authorization request and an AVS request will receive the appropriate authorization response in addition to a response indicating the AVS service is not available.

## Program and Service Format Requirements

### Address Verification Service

---

#### Participation

Acquirer participation in AVS is optional. To request AVS, the acquirer provides additional data elements in its Authorization Request/0100. The acquirer must be able to receive the AVS response data in the Authorization Request Response/0110.

Participation in AVS is required for all U.S. issuers. U.S. issuers must validate addresses when requested in an Authorization Request/0100 message. Refer to the *Authorization Manual* for additional requirements and service options.

### Authorization Request/0100—AVS and Authorization Request

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

#### NOTE

**The AVS Only request was discontinued 28 June 2011.**

Data Element	Org	Sys	Dst	Values/Comments
DE 4 (Amount, Transaction)	M	•	M	Must be a valid amount for authorization request with AVS requests.
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	Must be a valid TCC.
DE 48, subelement 82 (Address Verification Request)	M	•	M	52 = AVS and Authorization Request
DE 120 (Record Data)				<p>The acquirer must provide the non-condensed cardholder billing address.</p> <p>Note: Some merchant/acquirers are currently limited to supporting only numeric data.</p> <p>The issuer will receive only one occurrence of DE 120 subfields depending on the AVS Service Indicator identified in DE 94 of the Network Management Request/0800 message. The AVS Service Indicator identifies how the issuer expects to receive address data.</p>
DE 120, subfield 1 (AVS Service Indicator 1)	M	•	C	<p>Postal code (an-9) Address (ans...20 MasterCard) Address (ans...20 Visa)</p> <p>Note: At a minimum the Postal Code must be provided and cannot be less than nine bytes long (Postal code left justified and blank filled if necessary up to nine bytes).</p>

Data Element	Org	Sys	Dst	Values/Comments
DE 120, subfield 2 (AVS Service Indicator 2)	•	X	C	Postal Code (an-9) Address (an-5)
DE 120, subfield 3 (AVS Service Indicator 3)	•	X	C	Postal Code (an-9) Address (an-5)
DE 120, subfield 4 (AVS Service Indicator 4)	•	X	C	Postal Code (an-9) Address (an-5)

## Authorization Request Response/0110—AVS and Authorization Request

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

### NOTE

The AVS Only response was discontinued 28 June 2011.

Data Element	Org	Sys	Dst	Values/Comments
DE 4 (Transaction Amount)	ME	•	ME	Must be the same value as in the original Authorization Request/0100 message.
DE 39 (Response Code)	M	•	M	Contains one of the response codes listed for this data element in the “Data Element Definitions” chapter.
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	ME	•	ME	Must be the same value as in the original Authorization Request/0100 message.
DE 48, subelement 82 (Address Verification Request)	ME	•	ME	Must be the same value as in the original Authorization Request/0100 message.
DE 48, subelement 83 (Address Verification Response)	M	•	M	Contains one of the response codes listed for this data element in the “Data Element Definitions” chapter.
DE 120 (Record Data)	ME	•	ME	Must be the same value as in the original Authorization Request/0100 message.

### NOTE

Acquirers always receive the original information in DE 120 of the Authorization Request Response/0110 (the non-condensed subfield 01 contents) that they provided in the Authorization Request/0100.

## **Program and Service Format Requirements**

### **Address Verification Service**

---

## **Network Management Request/0800—AVS Sign-on**

Following is a list of the data elements and values applicable to this message type. All mandatory Network Management Request/0800—AVS Sign-on data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 94 (Service Indicator), position 3 (Address Data Indicator)	M	•	M	0 = AVS not supported 1 = Issuer supports AVS, receives all the address data (non-condensed) 2 = Issuer supports AVS, receives condensed address data 3 = Issuer supports AVS, receives condensed address data 4 = Issuer supports AVS, receives condensed numeric postal code and condensed numeric address data only.

## **Alternate Processing**

When the issuer is unavailable the transaction is processed by Stand-In or X-Code as follows.

### **NOTE**

**The AVS Only request was discontinued 28 June 2011.**

---

## **Authorization Request/0100—Request and Address Verification Service**

---

<b>WHEN...</b>	<b>THEN the Authorization Platform....</b>
The Authorization Request/0100 contains DE 48, subelement 82 value 52	Sends an Authorization Request Response/0110 message containing DE 39, value (based on the decision for the authorization request portion of the transaction).  If the issuer supports AVS then DE 48, subelement 83 contains value R  If the issuer does not support AVS then DE 48, subelement 83 contains value S

---

## **DE 48 and DE 120 Structure in AVS Transactions**

Following is the structure of DE 48 and DE 120 in AVS transactions.

The following table illustrates DE 48, subelements 82 (Address Verification Service Request) option code and subelement 83 (Address Verification Service Response) result code in an AVS transaction.

LLL	<b>VAR—999 maximum bytes (TCC + AVS Data)</b>						
3 bytes	1 byte	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	1 byte
Total Data Element Length	TCC	<b>AVS Request Data</b>			<b>AVS Response Data</b>		
		SE ID 82	SE Length 02	AVS Request Code	SE ID 83	SE Length 01	AVS Result Code
<b>1002 maximum bytes (LLL + TCC + AVS Data)</b>							

The following table illustrates DE 120 contents for subfield 01 (AVS Service Indicator 1).

LLL	<b>VAR—33 maximum bytes (MasterCard) – VAR—53 maximum bytes (Visa)</b>			
3 bytes	2 bytes	2 bytes	9 bytes	1-20 bytes (MasterCard) 1-40 bytes (Visa)
Total Data Element Length	Subfield ID 01	Subfield Length Variable	Cardholder postal/ZIP code	Cardholder Address

The following table illustrates DE 120 contents for subfield 02-04 (AVS Service Indicator 2-4).

LLL	Fixed 18 bytes			
3 bytes	2 bytes	2 bytes	9 bytes	5 bytes
Total Data Element Length	Subfield ID 02, or 03, or 04	Subfield Length	Cardholder postal/ZIP code	Cardholder Address

## Authorization Platform Edits

The Authorization Platform performs the following edits for an AVS-only transaction.

### NOTE

**The AVS Only request will be discontinued 28 June 2011.**

The Authorization Platform performs the following edits for AVS and Authorization Request/0100 messages.

## Program and Service Format Requirements

### Automated Fuel Dispenser Completion

---

WHEN the acquirer...	THEN the Authorization Platform...
Sends an Authorization Request/0100 message with DE 48, subelement 82 (AVS Request Data) = 52 (AVS and Authorization Request) and DE 120 (Record Data), subfield 01 (AVS Service Indicator 1) is less than nine bytes long	Sends the acquirer an Authorization Request Response/0110 message with: <ul style="list-style-type: none"><li>• DE 39 = 30 (Format Error)</li><li>• DE 44 = 120</li></ul>

## Automated Fuel Dispenser Completion

Acquirers use the Automated Fuel Dispenser Completion messages to advise the issuer of the total amount of the Automated Fuel Dispenser (AFD) transaction within 60 minutes after the transaction is completed.

The acquirer sends an Authorization Request/0100 message to verify a minimum availability of funds in the cardholder's account for an Automated Fuel Dispenser (AFD) CAT Level 2 transaction. If the request is not declined, the acquirer sends an Authorization Advice/0120—Acquirer-generated message to the issuer, specifying the total amount of the AFD transaction. The value in DE 60, subfield 1 (Advice Reason Code) is 191 (Acquirer Processing System [APS] Completed Authorization Transaction).

The Authorization Platform forwards all Authorization Advice/0120—Acquirer-generated messages directly to the issuer. The issuer must respond with an Authorization Advice Response/0130 (Responding to an Acquirer-generated 0120) message acknowledging receipt of the Authorization Advice/0120—Acquirer-generated message. If the issuer is not available or does not respond within timer limits, the Authorization Advice/0120—Acquirer-generated message will be sent to the Stand-In System. The Stand-In System responds with an Authorization Advice Response/0130—System-generated message to the acquirer to acknowledge receipt of the Authorization Advice/0120—Acquirer-generated message. The advice message will be added to the SAF for later distribution to the issuer.

For information about requesting a pre-authorization on Maestro Petrol transactions, see [Maestro Pre-authorized Transactions](#).

## AFD Message Scenarios

MasterCard is supporting the following usage scenarios for AFD authorization messages.

<b>WHEN the AFD Authorization Request Response/0110 contains...</b>	<b>THEN the AFD acquirer...</b>
DE 39 (Response Code), value 00 (Approved or completed successfully)	Submits the Authorization Advice/0120—Acquirer-generated message for the pumped amount.
DE 39, value 10 (Partial Approval)	Submits the Authorization Advice/0120—Acquirer-generated message for the pumped amount when the pumped amount is less than, equal to, or greater than the partial approval amount.
DE 39, value 00 (Approved or completed successfully) or value 10 (Partial Approval) and the transaction is canceled at the pump	Submits a Reversal Request/0400 message to cancel the AFD transaction.

**NOTE**

**The AFD Authorization Advice/0120—Acquirer-generated message is not a replacement for the First Presentment/1240 message to the clearing system on a credit transaction.**

## **Authorization Request/0100—Automated Fuel Dispenser Completion**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 4 (Amount, Transaction)	M	•	M	Must be at least an amount no less than the equivalent of USD 1.
DE 18 (Merchant Type)	M	•	M	5542 = Fuel Dispenser, Automated
DE 61 (Point of Service Data), subfield 7 (POS Transaction Status)	M	•	M	May contain one of the following values: 0 = Normal request (original presentment) 4 = Preauthorized request
DE 61, subfield 10 (Cardholder Activated Terminal Level)	M	•	M	2 = Authorized Level 2 CAT: Self-service terminal

## **Authorization Advice/0120—Acquirer-generated (Automated Fuel Dispenser Completion)**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Advice/0120 data elements apply.

## Program and Service Format Requirements

### Automated Fuel Dispenser Completion

Data Element	Org	Sys	Dst	Values/Comments
DE 4 (Amount, Transaction)	M	•	M	Contains the completed transaction amount and not the requested amount.
DE 18 (Merchant Type)	M	•	M	5542 = Fuel Dispenser, Automated
DE 39 (Response Code)	M	•	M	Valid values: 00 = Approved or completed successfully 10 = Partial Approval
DE 48 (Additional Data—Private Use), subelement 15 (Authorization Platform Advice Date and Time), subfield 1 (Date)	•	X	M	Contains the valid date of the Authorization Advice/0120—Acquirer-generated inserted by the Authorization Platform in MMDD format.
DE 48, subelement 15, subfield 2 (Time)	•	X	M	Contains the valid time of the Authorization Advice/0120—Acquirer-generated inserted by the Authorization Platform in hhmmss format.
DE 48, subelement 20 (Cardholder Verification Method)	M	X	•	
DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code)	M	•	M	191 = (Acquirer Processing System [APS] Completed Authorization Transaction)

#### NOTE

**Acquirers must not submit DE 48, subelement 82 (Address Verification Service Request) or subelement 92 (CVC 2) as these services are not performed on the Authorization Advice/0120—Acquirer-generated message and will cause the 0120 message to be rejected by the Dual Message System.**

### Authorization Advice/0120—Acquirer-generated (Automated Fuel Dispenser Completion)

Acquirers of Automated Fuel Dispenser (AFD) merchants located in the U.S. and Canada regions must send an Authorization Advice/0120 message to the issuer providing the actual transaction amount for each approved AFD transaction no more than 60 minutes after the original Authorization Request/0100 message was submitted. Global acquirers may optionally support this message for MasterCard and Debit MasterCard AFD transactions.

Customers should be aware of the critical requirements for proper processing of card acceptor business code (MCC) 5542 (Fuel Dispenser, Automated) transactions.

#### Critical AFD Advice Message Data

The following information provides a summary of the critical acquirer requirements for processing AFD transactions:

- Authorization Advice/0120 (Automated Fuel Dispenser Completion) messages must contain DE 60 (Advice Reason Code), subfield 1 (Advice

Reason Code), value 191 (completed authorization) for AFD transactions with an original Authorization Request/0100 message.

- The following Authorization Advice/0120 message data elements must match the value submitted within the original Authorization Request/0100 message for issuer transaction matching purposes:
  - DE 2 (Primary Account Number)
  - DE 7 (Transmission Date and Time)
  - DE 11 (System Trace Audit Number [STAN])
  - DE 32 (Acquiring Institution ID Code)
  - DE 33 (Forwarding Institution ID Code), if present in the Authorization Request/0100 message
  - DE 38 (Authorization ID Response) and DE 39 (Response Code) with the same value as received in the original Authorization Request Response/0110 message
  - DE 48 (Additional Data), subelement 98 (MasterCard Corporate Fleet Card® ID/Driver Number) and/or subelement 99 (MasterCard Corporate Fleet Card® Vehicle Number), with the same values as submitted in the original Authorization Request/0100 message, if present.
  - DE 121 (Authorizing Agent ID Code), with same value as was received in the original Authorization Request Response/0110 message, if present.

### **Track Data in AFD Advice Message—Acquirers**

The Authorization Advice/0120 message layout shows DE 35 (Track 2 Data) and DE 45 (Track 1 Data) as optional. Acquirers of AFD merchants are reminded that presence of track data in the card-present Authorization Request/0100 message does not necessitate inclusion within the AFD Advice message. This data is not needed by issuers for matching an AFD advice to an original authorization, and storage of track data for submission of the AFD Advice may not be PCI compliant.

### **Track Data in AFD Advice Message—Issuers**

Issuers are reminded that Authorization Advice/0120—Acquirer-generated messages are not card-activated and may not contain card-present data, regardless of a card-present Point-of-Service (POS) entry mode value in DE 22. The AFD advice message contains the completion amount and other reference data from the original Authorization Request/0100 message data. The inclusion of card-present DE 35 and DE 45 track data is optional. As such, the absence or presence of track data in the AFD Advice message should not result in a format error from issuers for card-present fuel purchases.

For details about data requirements, see the *Customer Interface Specification* manual.

---

## **Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated)**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Advice Response/0130—Issuer-generated (Responding to an Acquirer-generated) data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48, (Additional Data—Private Use), subelement 15 (Authorization Platform Advice Date and Time), subfield 1 (Date)	•	X	M	The Authorization Platform provides this data element, if required.
DE 48, (Additional Data—Private Use), subelement 15 (Authorization Platform Advice Date and Time), subfield 2 (Time)	•	X	M	The Authorization Platform provides this data element, if required.

### **Alternate Processing**

Alternate processing is provided if an issuer does not respond or is unable or unavailable to receive the Authorization Advice/0120—Acquirer-generated AFD completion messages.

The Authorization Platform responds to the acquirer with an Authorization Advice Response/0130 message containing DE 39 (Response Code), value 00 (Approved or completed successfully) and sends the Authorization Advice/0120—Acquirer-generated message to SAF. SAF messages will be sent to the issuer when the issuer is available. DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) keeps value 191 (Acquirer Processing System [APS] Completed Authorization Transaction) when delivered from SAF.

## Account Level Management

MasterCard Account Level Management provides issuers the flexibility of qualifying cardholder accounts for competitive interchange as well as upgrading cardholder accounts to a different card product.

Account Level Management includes the following authorization services:

- **MasterCard Product Graduation (Product Graduation)**—Supports the migration of cardholders to different card products without changing the account number (for example, an issuer upgrades a Gold MasterCard® card to a World MasterCard™ card).
- **MasterCard Enhanced Value (Enhanced Value)**—Supports differentiated interchange for cards registered for Enhanced Value.
- **MasterCard High Value (High Value)**—Provides an economic structure for qualifying card accounts by entitling issuers to increased interchange on those high spending accounts and ensuring that cardholders receive a minimum level of reward value.

## Enhanced Value and Product Graduation in Dual Message System Processing

MasterCard supports enhanced value and product graduation processing in Authorization messages as described here.

When the cardholder account in the Authorization Request/0100 message participates in Enhanced Value or the combination of Enhanced Value and Product Graduation and DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) is value 00 (Purchase) or 09 (Purchase with Cash Back), then MasterCard will process the transaction based on Account Level Management rules as defined in the table below.

The following table illustrates:

- The product code values and the Account Category values the Authorization Platform will provide in Authorization Request/0100 messages to the issuer based on the transaction's Account Level Management program participation.
- The product code values and Account Category values the issuer should return in the Authorization Request Response/0110 message when approving the transaction.

## Program and Service Format Requirements

### Account Level Management

WHEN...	THEN the Authorization Platform will populate the Authorization Request/0100 to the issuer with...	WHEN approving the transaction, the issuer must populate the Authorization Request Response/0110 with...
The transaction qualifies for Enhanced Value only	<ul style="list-style-type: none"><li>• DE 48, subelement 38, value B</li><li>• DE 63, subfield 1 with the registered product code associated with the authorization account range</li></ul>	<ul style="list-style-type: none"><li>• DE 38, position 6 containing value B</li><li>• DE 63, subfield 1 containing the value from DE 63, subfield 1 of the Authorization Request/0100</li></ul>
The transaction qualifies for Product Graduation only	<ul style="list-style-type: none"><li>• DE 48, subelement 38, value P</li><li>• DE 63, subfield 1 of the Authorization Request/0100 message with the licensed graduated product code</li></ul>	<ul style="list-style-type: none"><li>• DE 38, position 6 containing value P</li><li>• DE 63, subfield 1 containing the value from DE 63, subfield 1 of the Authorization Request/0100</li></ul>
The transaction qualifies for Enhanced Value and Product Graduation	<ul style="list-style-type: none"><li>• DE 48, subelement 38, value M</li><li>• DE 63, subfield 1 of the Authorization Request/0100 message with the licensed graduated product code</li></ul>	<ul style="list-style-type: none"><li>• DE 38, position 6 containing value M</li><li>• DE 63, subfield 1 containing the value from DE 63, subfield 1 of the Authorization Request/0100</li></ul>
The account range does participate in Account Level Management but the specific cardholder account does not participate	<ul style="list-style-type: none"><li>• DE 48, subelement 38, value Z</li><li>• DE 63, subfield 1 with the registered product code associated with the authorization account range</li></ul>	<ul style="list-style-type: none"><li>• DE 38, position 6 containing value Z</li><li>• DE 63, subfield 1 containing the value from DE 63, subfield 1 of the Authorization Request/0100</li></ul>

Because the Account Category code in DE 38, position 6 does not represent an individual product but rather the Account Level Management program in which the cardholder account participates, it is critical that when approving the transaction, the issuer returns both DE 63 and DE 38 so that the acquirer can properly qualify the transaction for the appropriate Account Level Management program. The Authorization Platform currently performs edits on the Authorization Request Response/0110 message to ensure that DE 38, position 6 is the same value provided to the issuer in DE 48, subelement 38 of the Authorization Request/0100 message and that DE 63, subfield 1 contains the same value provided to the issuer in the Authorization Request/0100 message.

The Authorization Platform also inserts the licensed graduated product code in DE 63, subfield 1 of the following messages if the cardholder account is eligible for Product Graduation:

- Authorization Advice/0120—Acquirer-generated—DE 63, subfield 1 contains the product code associated with the authorization account range.
- Authorization Advice/0120—System-generated—For advice messages delivered to issuers through the Store-and-Forward (SAF) process and advice messages generated by the Authorization Platform for RiskFinder

- Reversal Advice/0420—System-generated

The Authorization Platform does not insert the graduated product code into the following messages:

- Authorization Advice/0120—Issuer-generated for RiskFinder—The issuer received the graduated product code in the Authorization Request/0100 message and can choose to populate DE 63, subfield 1 of the Authorization Advice/0120—Issuer-generated message for RiskFinder with the graduated product. However, the Authorization Platform does not validate that this is the correct product code before routing the message to RiskFinder.
- Reversal Request/0400—DE 63, subfield 1 contains the product code associated with the authorization account range.

The Authorization Platform will perform the following edit on the Authorization Request Response/0110 message.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 48, subelement 38 is included in the Authorization Request/0100 message provided to the issuer with appropriate Account Level Management account category code and DE 38, position 6 of the Authorization Request Response/0110 message from the issuer does not match the value provided by the Authorization Platform in DE 48, subelement 38 of the Authorization Request/0100 message to the issuer when the issuer has populated DE 39 of the Authorization Request Response/0110 message with one of the following values that indicate an approval: <ul style="list-style-type: none"><li>• 00 (Approved or completed successfully)</li><li>• 08 (Honor with ID)</li><li>• 10 (Partial Approval)</li><li>• 87 (Purchase Amount Only, No Cash Back Allowed)</li></ul>	Sends the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 (Response Code) = (Format error) DE 44 (Additional Response Data) = 038 (identifying the data element in error)

## High Value in Dual Message System Processing

When a cardholder account participates in High Value or a combination of High Value and Product Graduation and DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) is value 00 (Purchase) or 09 (Purchase with Cash Back), then MasterCard will process the transaction based on Account Level management rules defined in the table below.

The following table illustrates:

- The product code values and the Account Category values the Authorization Platform will provide in Authorization/0100 messages to the issuer based on the transaction's Account Level Management program participation.
- The product code values and Account Category values the issuer should return in the Authorization Request Response/0110 message when approving the transaction.

<b>WHEN...</b>	<b>THEN the Authorization Platform will populate the Authorization Request/0100 to the issuer with...</b>	<b>WHEN approving the transaction, the issuer must populate the Authorization Request Response/0110 with...</b>
The transaction qualifies for High Value only	<ul style="list-style-type: none"><li>• DE 48, subelement 38 value S</li><li>• DE 63, subfield 1 with the licensed product code associated with the authorization account range</li></ul>	<ul style="list-style-type: none"><li>• DE 38, position 6 value S</li><li>• DE 63, subfield 1 containing the value from DE 63, subfield 1 of the Authorization Request/0100 message</li></ul>
The transaction qualifies for High Value and participates in Product Graduation	<ul style="list-style-type: none"><li>• DE 48, subelement 38 value T</li><li>• DE 63, subfield 1 with the licensed product code associated with the authorization account range</li></ul>	<ul style="list-style-type: none"><li>• DE 38, position 6, value T</li><li>• DE 63, subfield 1 containing the value from DE 63, subfield 1 of the Authorization Request/0100 message</li></ul>
The account range is a participant in Account Level Management; however, the specific cardholder account does not participate	<ul style="list-style-type: none"><li>• DE 48, subelement 38 value Z</li><li>• DE 63, subfield 1 containing the registered product code associated with the authorization account range</li></ul>	<ul style="list-style-type: none"><li>• DE 38, position 6, value Z</li><li>• DE 63, subfield 1 containing the same value as in the Authorization Request/0100 message</li></ul>

The Authorization Platform will perform the following edit on the Authorization Request Response/0110 message.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>DE 48, subelement 38 is included in the Authorization Request/0100 message provided to the issuer with appropriate Account Level Management account category code and</p> <p>DE 38, position 6 of the Authorization Request Response/0110 message from the issuer does not match the value provided by the Authorization Platform in DE 48, subelement 38 of the Authorization Request/0100 message to the issuer when the issuer has populated DE 39 of the Authorization Request Response/0110 message with one of the following values that indicate an approval:</p> <ul style="list-style-type: none"> <li>• 00 (Approved or completed successfully)</li> <li>• 08 (Honor with ID)</li> <li>• 10 (Partial Approval)</li> <li>• 87 (Purchase Amount Only, No Cash Back Allowed)</li> </ul>	<p>Sends the issuer an Authorization Response Negative Acknowledgement/0190 message where:</p> <p>DE 39 (Response Code) = (Format error)  DE 44 (Additional Response Data) = 038 (identifying the data element in error)</p>

## ATM Bill Payment Service

Bill payment transactions at the ATM help increase the acquirer's transaction volume by providing a convenient method for cardholders to initiate bill pay request transactions.

ATM Bill Payment service supports:

- Europe acquired ATM Bill Payment transactions
- Non-Europe acquired ATM Bill Payment transactions

### Authorization Request/0100—ATM Bill Payment, Europe Acquired

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

## Program and Service Format Requirements

### ATM Bill Payment Service

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	00 = Purchase
DE 18 (Merchant Type)	M	•	M	Contains value 6050 = Quasi Cash—Member Financial Institution or a more precise MCC related to the nature of the bill that is being paid, for example, MCC 4900 (Utilities-Electric, Gas, Heating Oil, Sanitary, Water) for utilities bills. MCC 6011 (Member Financial Institution-Automated Cash Disbursements) must not be used.
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	U = Unique
DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level Indicator)	M	•	M	0 = Not a CAT transaction 1 = Authorized Level 1 CAT: automated dispensing machine with PIN
DE 124 (Member Defined Data)	O	•	C	Contains details relating to the bill being paid.

## Authorization Request/0100—ATM Bill Payment, Non-Europe Acquired

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	00 = Purchase
DE 18 (Merchant Type)	M	•	M	Must contain value 6539 = Funding transaction [Excluding <i>MoneySend</i> ]
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	U = Unique
DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level Indicator)	M	•	M	One of the following values: 1 = Authorized Level 1 CAT: automated dispensing machine with PIN 2 = Authorized Level 1 CAT: self service terminal
DE 124 (Member Defined Data)	O	•	C	Contains details relating to the bill being paid.

## Authorization Platform Edits

The Authorization Platform applies the following edits on ATM Bill Payment Service transactions.

WHEN the acquirer...	THEN the Authorization Platform...
Sends an Authorization Request/0100, Authorization Advice/0120, or Reversal Request/0400 message containing DE 18 (Merchant Type), value 6539 (Funding Transaction, Excluding <i>MoneySend</i> )	Sends the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 message with DE 39 (Response Code), value 58 (Transaction not permitted to acquirer/terminal).

## ATM Credit Card Cash Advance in Installments

This service allows cardholders to initiate an inquiry at the ATM requesting a credit card cash advance to be repaid in monthly installments (for example, 6, 12, or 18 months).

With this enhancement, a cardholder can initiate an inquiry at the ATM requesting a credit card cash advance to be repaid in monthly installments (for example, 6, 12, or 18 months). The issuer can accept the installment terms requested by the cardholder, decline the request, or decline the request and offer an alternate installment schedule. The cardholder has the option to accept or reject the issuer's terms and conditions for the installment payments. If the cardholder accepts the issuer's terms and conditions for repayment, the issuer will then approve or decline the cash advance transaction. If approved, the cardholder will receive the funds, along with the installment payment details printed on the ATM receipt. The issuer will bill the cardholder for the amount of the transaction in the agreed-upon installments.

Acquirers entering this market must be able to:

- Provide ATM screens that offer an installment payment option.
- Provide the ability to print the issuer's installment payment details on the ATM receipt.

The ATM Credit Card Cash Advance in Installments service is currently available to single message transactions (Single Message System-acquired activity).

The ATM Credit Card Cash Advance in Installments service is not available to ATM acquirers in the Europe region.

## Authorization Request/0100—ATM Installment Inquiry

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

## **Program and Service Format Requirements**

### **ATM Credit Card Cash Advance in Installments**

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	01 (Withdrawal)
DE 4 (Amount, Transaction)	M	•	M	Contains the amount of the cash advance
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status)	M	•	M	Identifies that the cardholder has initiated an ATM installment inquiry transaction 3 = ATM Installment Inquiry
DE 112 (Additional Data—National Use), subelement 001 (Installment Payment Data)	C	•	C	Identifies the transaction type. 80xx = (ATM Installment Inquiry, Number of Installments) 81xx = (ATM Installment Withdrawal, Number of Installments)
DE 112, subelement 027 (ATM Credit Card Cash Advance Installments), subfield 1 (Transaction Type)	C	•	C	80 = ATM Installment Inquiry
DE 112, subelement 027 (ATM Credit Card Cash Advance Installments), subfield 2 (Requested Number of Installments)	C		C	01–99 = (the number of installments requested by the cardholder)

### **Authorization Request Response/0110—ATM Installment Inquiry**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	ME	•	ME	01 (Withdrawal)
DE 4 (Amount, Transaction)	CE	X	CE	Contains the amount of the cash advance
DE 112 (Additional Data—National Use), subelement 001 (Installment Payment Data)	C	•	C	Identifies the transaction type. 80xx = (ATM Installment Inquiry, Number of Installments) 81xx = (ATM Installment Withdrawal, Number of Installments)
DE 112, subelement 027 (ATM Credit Card Cash Advance Installments), subfield 1 (Transaction Type)	C	•	C	80 = ATM Installment Inquiry

**Program and Service Format Requirements****ATM Credit Card Cash Advance in Installments**

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 112, subelement 027, subfield 2 (Requested Number of Installments)	C	•	C	01–99 = (the number of installments requested by the cardholder)
DE 112, subelement 027, subfield 3 (Approved Number of Installments)	C	•	C	The number of installment payments approved by the issuer
DE 112, subelement 027, subfield 4 (Installment Amount)	C	•	C	The monthly payment amount
DE 112, subelement 027, subfield 5 (Total Transaction Amount)	C	•	C	The amount of the cash advance and the interest for the transaction
DE 112, subelement 027, subfield 6 (Yearly Interest Rate)	C	•	C	The interest rate that will be charged to the cardholder by the issuer
DE 112, subelement 027, subfield 7 (Currency Code)	C	•	C	The currency code the issuer is charging the cardholder for repayment
DE 112, subelement 027, subfields 8–11 (Member-defined Data)	C	•	C	Member-defined data

**Authorization Request/0100—ATM Installment Withdrawal**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	01 = Withdrawal
DE 4 (Amount, Transaction)	M	•	M	Contains the amount of the cash advance.
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status)	M	•	M	Identifies that the cardholder has initiated an ATM installment inquiry transaction. 0 = Normal request (original presentment)
DE 112 (Additional Data—National Use), subelement 001 (Installment Payment Data)	C	•	C	Identifies the transaction type. 81xx = ATM Installment Withdrawal, Number of Installments

## **Program and Service Format Requirements**

### **ATM Credit Card Cash Advance in Installments**

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 112, subelement 027 (ATM Credit Card Cash Advance Installments), subfield 1 (Transaction Type)	C	•	C	81 = ATM Installment Withdrawal
DE 112, subelement 027 (ATM Credit Card Cash Advance Installments), subfield 2 (Requested Number of Installments)	C	•	C	01–99 = The number of installments requested by the cardholder

### **Authorization Request Response/0110—ATM Installment Withdrawal**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	ME	•	ME	01 = Withdrawal
DE 4 (Amount, Transaction)	CE	X	CE	Contains the amount of the cash advance.
DE 112 (Additional Data—National Use), subelement 001 (Installment Payment Data)	C	•	C	Identifies the transaction type. 81xx = ATM Installment Withdrawal, Number of Installments
DE 112, subelement 027 (ATM Credit Card Cash Advance Installments), subfield 1 (Transaction Type)	C	•	C	81 = ATM Installment Withdrawal
DE 112, subelement 027, subfield 2 (Requested Number of Installments)	C	•	C	01–99 = The number of installments requested by the cardholder.
DE 112, subelement 027, subfield 3 (Approved Number of Installments)	C	•	C	01–99 = The number of installment payments approved by the issuer.
DE 112, subelement 027, subfield 4 (Installment Amount)	C	•	C	The cardholder's monthly payment amount.
DE 112, subelement 027, subfield 5 (Total Transaction Amount)	C	•	C	The amount of the cash advance and the interest for the transaction.
DE 112, subelement 027, subfield 6 (Yearly Interest Rate)	C	•	C	The interest rate that will be charged to the cardholder by the issuer.

Data Element	Org	Sys	Dst	Values/Comments
DE 112, subelement 027, subfield 7 (Currency Code)	C	•	C	The currency code the issuer is charging the cardholder for repayment.
DE 112, subelement 027, subfields 8-11	C	•	C	Member-defined data.

## Balance Inquiry—ATM

The ATM Balance Inquiry service provided through the MasterCard/Cirrus ATM Network, allows MasterCard cardholders to inquire upon their account balance at Cirrus ATM terminals. Issuers that participate in this service must request certification from the Customer Operations Services team. Cirrus is the controlling gateway. It forwards Balance Inquiry requests only to issuers who are certified for receipt. Issuers must then reply with a Balance Inquiry response.

### Authorization Request/0100—ATM Balance Inquiry

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code)	M	•	M	Must be 30xx00
DE 4 (Amount, Transaction)	M	•	M	Must be zero unless an acquirer applied an ATM transaction fee for an ATM transaction in a country where application of an ATM transaction fee is allowed.
DE 18 (Merchant Type)	M	•	M	MCC must be one of the following values: 6010 (Member Financial Institution - Manual Cash Disbursement) 6011 (Member Financial Institution - Automated Cash Disbursements)
DE 28 (Amount, Transaction Fee)	C	•	C	May contain an ATM transaction fee, if applicable for transactions in a country where application of an ATM transaction fee is allowed.
DE 35 (Track 2 Data)	C	•	C	Must omit if DE 45 present
DE 41 (Card Acceptor Terminal ID)	M	•	M	
DE 43 (Card Acceptor Name and Location)	M	•	M	

## **Program and Service Format Requirements**

### **Balance Inquiry—ATM**

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 45 (Track 1 Data)	C	•	C	Must omit if DE 35 present
DE 52 (Personal ID Number [PIN] Data)	M	•	M	

### **Authorization Request/0100—ATM Balance Inquiry Edits**

In addition to the standard Authorization Platform edits on Authorization Request/0100 messages, the Authorization Platform will apply the following edits on an Authorization Request/0100—ATM balance inquiry message.

<b>IF...</b>	<b>THEN the Authorization Platform...</b>
The issuer does not participate in ATM balance inquiry	Returns the Authorization Request Response/0110 message containing: DE 39 = 57 (Transaction not permitted to issuer/cardholder).
DE 18 (Merchant Type) is <b>not</b> 6010 or 6011	Returns the Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 018
If neither DE 45 (Track 1 Data) nor DE 35 (Track 2 Data) is present in the Authorization Request/0100 message	Returns the Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 035
DE 54 (Additional Amounts) is present	Returns the Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 054

### **Authorization Request Response/0110—ATM Balance Inquiry**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 28 (Amount, Transaction Fee)	CE	X	CE	Must be the same value as in the original Authorization Request/0100 message, if present.
DE 39 (Response Code)	M	•	M	00 = Approved or completed successfully or 85 = Not declined

Data Element	Org	Sys	Dst	Values/Comments
DE 54 (Additional Amounts), subfield 1 (Account Type)	M	•	M	Must be the same value as DE 3, subfield 2 in the original Authorization Request/0100 message
DE 54, subfield 2 (Amount Type)	M	•	M	02 = Available Balance Issuers in the United Kingdom may provide the ledger balance (01) in addition to the available balance (02) for intracountry ATM balance inquiry needs.
DE 54, subfield 3 (Currency Code)	M	•	M	Must be a valid three-digit currency code that matches the issuer's currency code.
DE 54, subfield 4 (Amount)	M	•	M	C = Credit amount plus 12 digits or D = Debit amount plus 12 digits

## Authorization Request Response/0110—ATM Balance Inquiry Edits

In addition to the standard Authorization Platform edits on Authorization Request Response/0110 messages, the Authorization Platform will apply the following edits on an Authorization Request Response (ATM balance inquiry)/0110 message.

IF...	THEN...
DE 39 (Response Code) contains the value 00 or 85 and DE 54 (Additional Amounts) is not present	The Authorization Platform will send to the issuer an Authorization Negative Acknowledgement/0190 message containing:  DE 39 = 30 DE 44 = 054
DE 54, subfield 3 (Currency Code) is not a valid currency code	The Authorization Platform will generate an Authorization Response Negative Acknowledgement/0190 message containing:  DE 39 = 30 DE 44 = 054
DE 54, subfield 4 (Amount) is not C plus 12 digits or D plus 12 digits	The Authorization Platform will generate an Authorization Response Negative Acknowledgement/0190 message containing:  DE 39 = 30 DE 44 = 054

## **Authorization Advice/0120—Acquirer-generated—ATM Balance Inquiry Edits**

The Authorization Platform will perform the following edit on Authorization Advice/0120—Acquirer-generated messages for ATM Balance Inquiry transactions.

<b>IF...</b>	<b>THEN...</b>
The acquirer submits an Authorization Advice/0120—Acquirer-generated message containing DE 3 (Processing Code), value 30 (Balance Inquiry)	The Authorization Platform will reject the message and forward the acquirer an Authorization Advice Response/0130 message containing: DE 39 = 30 DE 44 = 003

## **Alternate Processing**

ATM Balance inquiry transactions are not eligible for alternate (Stand-In or alternate issuer host routing) or X-Code processing.

If the primary issuer is not available to the ATM balance inquiry request, an Authorization Request Response/0110 is returned to the acquirer with DE 39 (Response Code) value 91 (Authorization Platform or issuer system inoperative).

## **Balance Inquiry—Point-of-Sale**

When attempting to make a purchase at the point of sale, cardholders uncertain of the remaining balance on a MasterCard prepaid card or a private label card can initiate a balance inquiry at the point of sale to make a more fully informed decision about how to use the card's funds for the purchase. POS balance inquiry helps the cardholder to completely redeem the funds on the prepaid card, reduces the potential of a declined authorization request when the purchase amount exceeds the funds available on the card, and helps to avoid extended checkout times and lost sales.

The acquirer will receive the cardholder account balance in both the issuer's currency and the transaction currency. The acquirer has the option to provide the merchant with the cardholder account balance in the issuer's currency, transaction currency, or both. The merchant will then display the appropriate account balance on the customer's printed receipt.

Acquirer participation in POS balance inquiry is optional. To request a POS balance inquiry, the acquirer provides the appropriate data elements as defined below.

Issuer participation in POS balance inquiry is optional. To request participation, issuers must submit the Point-of-Sale (POS) Balance Inquiry Participation form to Customer Operations Services.

## Authorization Request/0100—POS Balance Inquiry

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	30 (Balance Inquiry)
DE 3, subfield 2 (Cardholder “From Account” Type Code)	M	•	M	00 (Default Account) or 30 (Credit Card Account)
DE 3, subfield 3 (Cardholder “To Account” Type Code)	M	•	M	00 (Default Account)
DE 4 (Amount, Transaction)	M	•	M	Must be zero.
DE 18 (Merchant Type)	M	•	M	For POS balance inquiries, the MCC must be a value other than: 6010 = Member Financial Institution—Manual Cash Disbursements or 6011 = Member Financial Institution—Automated Cash Disbursements
DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	Must contain one of the following values: 02 = PAN auto-entry via magnetic stripe 05 = PAN auto-entry via chip 07 = PAN auto-entry via contactless M/Chip 80 = Chip card at chip-capable terminal was unable to process transaction using data on the chip; therefore, the terminal defaulted to the magnetic stripe-read PAN. 90 = PAN auto-entry via magnetic stripe 91 = PAN auto-entry via contactless magnetic stripe
DE 35 (Track 2 Data)	C	•	C	Track information encoded on the magnetic stripe must be presented from either Track 2 or Track 1.
DE 41 (Card Acceptor Terminal ID)	M	•	M	Must contain terminal ID at the card acceptor location.
DE 43 (Card Acceptor Name/Location)	M	•	M	Must contain name and location of the card acceptor as known by the cardholder.
DE 45 (Track 1 Data)	C	•	C	Track information encoded on the magnetic stripe must be presented from either Track 1 or Track 2.

## Program and Service Format Requirements

### Balance Inquiry—Point-of-Sale

---

## Authorization Request Response/0110—POS Balance Inquiry

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

Issuers participating in POS balance inquiry and responding to an Authorization Request/0100—POS Balance Inquiry message must send an Authorization Request Response/0110 message containing balance information in DE 54 (Additional Amounts) when DE 39 contains the value 00 (Approved or completed successfully) or 85 (Not declined).

Data Element	Org	Sys	Dst	Values/Comments
DE 39 (Response Code)	M	•	M	00 = Approved or completed successfully or 85 = Not declined
DE 54 (Additional Amounts), subfield 1 (Account Type)	M	•	M	Must be the same value as DE 3, subfield 2 in the original Authorization Request/0100 message 00 = Default Account or 30 = Credit Card Account
DE 54, subfield 2 (Amount Type)	M	•	M	02 = Available Balance
DE 54 , subfield 3 (Currency Code)	M	•	M	Must be a valid three-digit currency code that matches the issuer's currency code.
DE 54 , subfield 4 (Amount)	M	•	M	C = Credit amount plus 12 digits or D = Debit amount plus 12 digits

## Authorization Request/0100—POS Balance Inquiry Edits

In addition to the standard Authorization Platform edits on Authorization Request/0100 messages, the Authorization Platform will apply the following edits on an Authorization Request/0100—POS balance inquiry message.

IF...	THEN the Authorization Platform...
The issuer participates in POS balance inquiry	Forward the POS balance inquiry to the issuer.
The issuer does not participate in POS balance inquiry	Returns the Authorization Request Response/0110 message containing: DE 39 = 57 (Transaction not permitted to issuer/cardholder).

<b>IF...</b>	<b>THEN the Authorization Platform...</b>
DE 4 (Transaction Amount) is not zero	Returns the Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 004
DE 18 (Merchant Type) is 6010 or 6011	Returns the Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 018
DE 22 (Point-of-Service (POS) Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) is not 02, 05, 07, 80, 90, or 91	Returns the Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 022
DE 41 (Card Acceptor Terminal ID) is not present	Returns the Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 041
DE 43 (Card Acceptor Name/Location) is not present	Returns the Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 043
If neither DE 45 (Track 1 Data) nor DE 35 (Track 2 Data) is present in the Authorization Request/0100 message	Returns the Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 035
DE 54 (Additional Amounts) is present	Returns the Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 054

## Authorization Request/0110—POS Balance Inquiry Edits

In addition to the standard Authorization Platform edits on Authorization Request Response/0110 messages, the Authorization Platform will apply the following edits on an Authorization Request Response (POS balance inquiry)/0110 message.

## **Program and Service Format Requirements**

### **Balance Inquiry—Point-of-Sale**

<b>IF...</b>	<b>THEN...</b>
DE 39 (Response Code) contains the value 00 or 85 and DE 54 (Additional Amounts) is not present	The Authorization Platform will send to the issuer an Authorization Negative Acknowledgement/0190 message containing: DE 39 = 30 DE 44 = 054
DE 39 contains a value other than 00 or 85 and DE 54 is present	The Authorization Platform will remove DE 54 from the Authorization Request Response/0110 message before sending the message to the acquirer
DE 54, subfield 2 (Amount Type) is not 02 (Available Balance)	The Authorization Platform will generate an Authorization Response Negative Acknowledgement/0190 message containing: DE 39 = 30 DE 44 = 054
DE 54, subfield 3 (Currency Code) is not a valid currency code	The Authorization Platform will generate an Authorization Response Negative Acknowledgement/0190 message containing: DE 39 = 30 DE 44 = 054
DE 54, subfield 4 (Amount) is not C plus 12 digits or D plus 12 digits	The Authorization Platform will generate an Authorization Response Negative Acknowledgement/0190 message containing: DE 39 = 30 DE 44 = 054

### **Authorization Advice/0120—Acquirer-generated—POS Balance Inquiry Edits**

The Authorization Platform will perform the following edit on Authorization Advice/0120—Acquirer-generated messages for POS Balance Inquiry transactions.

<b>IF...</b>	<b>THEN...</b>
The acquirer submits an Authorization Advice/0120—Acquirer-generated message containing DE 3 (Processing Code), value 30 (Balance Inquiry)	The Authorization Platform will reject the message and forward the acquirer an Authorization Advice Response/0130 message containing: DE 39 = 30 DE 44 = 003

## Alternate Processing

POS Balance inquiry transactions are not eligible for alternate (Stand-In or alternate issuer host routing) or X-Code processing.

If the primary issuer is not available to the POS balance inquiry request, an Authorization Request Response/0110 is returned to the acquirer with DE 39 (Response Code) value 91 (Authorization Platform or issuer system inoperative).

## Balance Inquiry—Short Message Service

The Balance Inquiry Short Message Service (SMS) provides cardholders with real-time access to their account balance information via their mobile devices.

Issuers that want to participate in the SMS Balance Service Program must complete a contract and Issuer SMS Balance Inquiry Service information form.

Issuers participating in the new SMS Balance Inquiry service will receive these balance inquiries with DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), value 81 (PAN entry via electronic commerce, including chip).

## Authorization Request/0100—Short Message Service Balance Inquiry

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	30 = Balance Inquiry
DE 18 (Merchant Type)	M	•	M	5969 = Mail Order/Telephone Order Providers
DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	81 = PAN entry via electronic commerce, including chip
DE 48 (Additional Data—Private Use), subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), position 3 (UCAF Collection Indicator)	M	•	M	zero

## **Program and Service Format Requirements**

### **Balance Inquiry—Mobile Remote Payments Program**

---

## **Balance Inquiry—Mobile Remote Payments Program**

The Balance Inquiry—Mobile Remote Payments Program provides cardholders participating in the program with access to their account balance information by an application on their mobile device.

Issuers participating in the Mobile Remote Payments Program will receive these balance inquiries with DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), value 82 (PAN auto entry via server).

### **Authorization Request/0100—Mobile Remote Payments Program Balance Inquiry**

Following is a list of data elements and value applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code), Subfield 1 (Cardholder Transaction Type Code)	M	•	M	Must be 30xx00
DE 4 (Amount, Transaction)	M	•	M	Must be zero
DE 18 (Merchant Type)	M	•	M	Must be a value other than 6010 (Member Financial Institution-Manual Cash) 6011 (Member Financial Institution-Automated Cash)
DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	Must be 82 (PAN Auto Entry via Server [issuer, acquirer, or third party vendor system])
DE 41 (Card Acceptor Terminal ID)	M	•	M	Must contain terminal ID at the card acceptor location
DE 43 (Card Acceptor Name/Location) by the cardholder	M	•	M	Must contain name and location of the card acceptor as known
DE 48 (Additional Data—Private Use), subelement 48 (Mobile Remote Payments Program Indicators), subfield 1 (Remote Payments Program Type Identifier)	M	•	M	Must be 1 (Issuer domain) or 2 (Acquirer Domain)

## **Chip-Specific Value Constraints**

The Authorization Platform supports the authorization of chip transactions—i.e., transactions generated using an integrated circuit card (ICC).

Acquirers may choose to acquire chip-related data in one of the two modes

- Chip Partial Grade mode
- Chip Full Grade mode

The content of chip-related Authorization Request/0100 messages will vary, depending on the mode used. Issuers of ICCs must be able to accept authorization requests in either mode.

## Chip Partial Grade Value Constraints

Following is a list of specific data elements and data element values required in the Authorization Request/0100 message for a chip partial grade transaction.

<b>DE 22, subfield 1</b>	<b>DE 22, subfield 1 value</b>	<b>DE 35</b>	<b>DE 52 and DE 23</b>
Offline PIN	05	ICC data as EMV tag 57 (Track 2 Equivalent Data)	Not provided
Online PIN			Must be provided
Signature			Not provided
No CVM			Not provided

<b>Data Element</b>	<b>Requirements</b>
DE 22	For chip transactions, acquirers must provide value 05x. For a chip transaction where the magnetic stripe was used as a fallback technology, acquirers must provide the value 80x. In this case, acquirers must provide the full, unaltered track data. For a chip transaction where manual PAN entry was used as a fallback technology, acquirers may provide the value 79x.)
DE 23	The card sequence number may now be provided in chip partial grade transactions where DE 55 is not present. DE 23 must be provided if EMV tag 5F34 (Application PAN Sequence Number) is present on the ICC.
DE 35	The ICC data as EMV tag 57 (Track 2 Equivalent Data). This data corresponds with the data stored in Track 2 of the magnetic stripe. For chip transactions, acquirers must provide DE 35 EMV tag 57 if the data object was present on the ICC. For a chip transaction where the magnetic stripe was used as a fallback technology, DE 35 must contain the actual Track 2 data from the magnetic stripe.
DE 52	DE 52 must be provided if the Cardholder verification method was Online PIN.

## Program and Service Format Requirements

### Chip-Specific Value Constraints

---

#### Chip Full Grade Value Constraints

This mode is for acquirers who accept chip transactions and whose infrastructure allows them to provide chip-specific data. Acquirers operating in this mode must comply with all chip partial grade requirements and the chip full grade requirements.

Data Element	Requirements
DE 23	DE 23 must be provided if EMV tag 5F34 is present on the ICC.
DE 37	DE 37, subfield 2 contains the value of "Transaction Sequence Counter" (EMV Tag 9F41), right-justified, left-padded with zeros.
DE 52	DE 52 must be provided if the CVM is Online PIN.
DE 55	DE 55 must be provided as specified in the Message Layouts. DE 55 must be TLV encoded and must contain the information (mandatory and optional) as specified in the Data Element Definitions.
DE 125	Acquirers must provide DE 125 for PIN change transactions where DE 52 also must be present.

#### Contact and Contactless Chip Specific Value Constraints

Following is the usage of DE 61, subfield 11 in conjunction with DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PIN Entry Mode). DE 22, subfield 1 values indicate the method by which the PAN was entered into the interchange system.

Values	
0	= Unknown or unspecified
1	= No terminal used (voice/ARU authorization) DE 22, subfield 1 applicable value 00 (PAN entry mode unknown)
2	= Magnetic stripe reader only DE 22, subfield 1 applicable values: <ul style="list-style-type: none"><li>• 90 (PAN auto-entry via magnetic stripe-track data is required)</li><li>• 02 (PAN auto-entry via magnetic stripe-track data is not required)</li></ul>
3	= Contactless M/Chip (Proximity Chip) Value 3 indicates that the terminal supports <i>Paypass</i> M/Chip and <i>Paypass</i> magstripe transactions. The terminal may also support other card input types, including contact transactions.

**Values**

4	=	Contactless Magnetic Stripe (Proximity Chip) only Value 4 indicates that the terminal supports <i>Paypass</i> magstripe transactions. The terminal may also support other card input types, including contact transactions.
5	=	EMV specification (compatible chip reader) and magnetic stripe reader. The terminal also may support contactless transactions, however these values must only be used for contact transactions. DE 22, subfield 1 applicable values: <ul style="list-style-type: none"><li>• 05 (PAN auto-entry via chip)</li><li>• 79 (Hybrid terminal with an online connection to acquirer failed in sending chip to magnetic stripe fallback or reading the chip card)</li><li>• 80 (Chip card at chip-capable terminal was unable to process transaction; therefore, terminal defaulted to the magstripe-read PAN)</li><li>• 90 (PAN auto-entry via magnetic stripe-track data is required)</li></ul>
6	=	Key entry only DE 22, subfield 1 applicable value 01 (PAN manual entry)
7	=	Magnetic stripe reader and key entry DE 22, subfield 1 applicable values: <ul style="list-style-type: none"><li>• 01 (PAN manual entry)</li><li>• 02 (PAN auto-entry via magnetic stripe-track data is not required)</li><li>• 90 (PAN auto-entry via magnetic stripe-track data is required)</li></ul>
8	=	EMV specification (compatible chip reader), magnetic stripe reader and key entry. The terminal also may support contactless transactions; however, these values must only be used for contact transactions. DE 22, subfield 1 applicable values: <ul style="list-style-type: none"><li>• 01 (PAN manual entry)</li><li>• 05 (PAN auto-entry via chip)</li><li>• 79 (Hybrid terminal with an online connection to acquirer failed in sending chip to magstripe fallback or reading the chip card)</li><li>• 80 (Chip card at chip-capable terminal was unable to process transaction using data on the chip)</li><li>• 90 (PAN auto-entry via magnetic stripe-track data is required)</li></ul>
9	=	EMV specification (compatible chip reader) only The terminal also may support contactless transactions; however, this value only must be used for contact transactions. DE 22, subfield 1 applicable value 05 (PAN auto-entry via chip)

## **Card Validation Code 2**

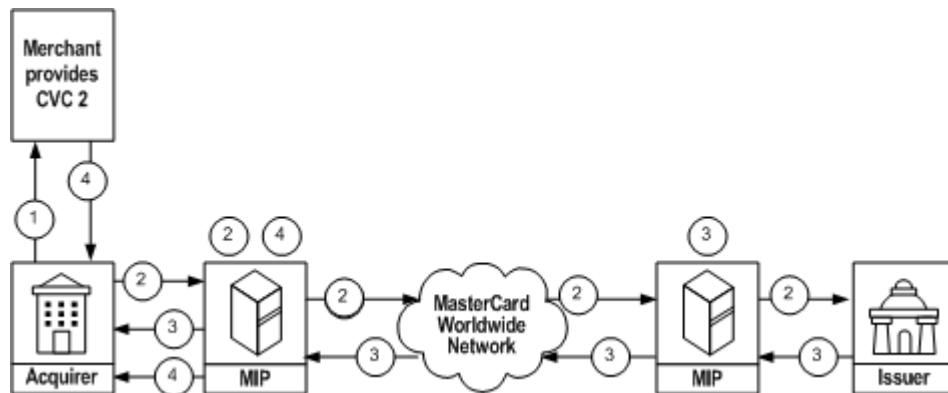
To comply with card validation code 2 (CVC 2) requirements, acquirers and issuers must process transactions according to the guidelines in this topic.

The following message flows describe authorization message processing for CVC 2 verification transaction in these scenarios:

- When the CVC 2 is verified
- When the CVC 2 is unverified (because the issuer was temporarily unable to receive the CVC 2 value)
- When the CVC 2 is processed by Stand-In
- When the CVC 2 is processed by X-Code
- When the CVC 2 is processed by Limit-1

### **Authorization Request/0100—CVC 2 Verified**

Following are the stages of an Authorization Request/0100—CVC2 transaction when the value is verified.

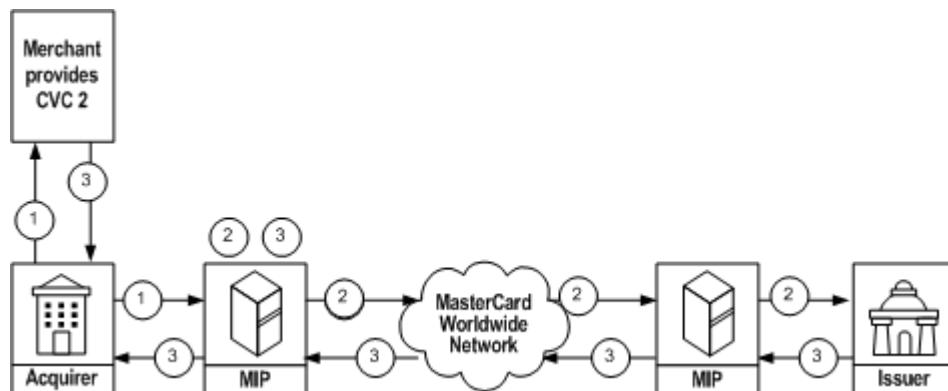


1. The merchant provides the CVC 2 value, and the acquirer generates an Authorization Request/0100 message with the CVC 2 value in DE 48, subelement 92.
2. The acquirer MIP forwards the Authorization Request/0100 message to the issuer.
3. After the issuer transmits the Authorization Request Response/0110 message, the issuer MIP verifies that one of the following values appears in DE 48, subelement 87:
  - M (Valid CVC 2—match)
  - N (Invalid CVC 2—non-match)
  - P (CVC 2 not processed—issuer temporarily unavailable)

<b>IF DE 48, subelement 87 contains...</b>	<b>AND IF the transaction was...</b>	<b>THEN...</b>	<b>AND THEN...</b>
No response or an invalid response	Not approved	The acquirer MIP forwards the Authorization Request Response/0110 message to the acquirer with DE 48, subelement 87 = P	The issuer will not receive an Authorization Response Negative Acknowledgement/0190 message.
No response or an invalid response	Approved	The acquirer MIP forwards the Authorization Request/0100 message to the alternate authorization service provider for processing.	The issuer will receive an Authorization Response Negative Acknowledgement/0190 message.

## Authorization Request/0100—CVC 2 Unverified

Following are the stages of an Authorization Request/0100—CVC 2 unverified transaction (issuer temporarily unable to receive the CVC 2 value).



1. The merchant provides the CVC 2 value, and the acquirer generates an Authorization Request/0100 message with the CVC 2 value in DE 48, subelement 92.
2. The acquirer MIP forwards the Authorization Request/0100 message to the issuer, but the issuer is temporarily unable to receive the CVC value. The MIP forwards the Authorization Request/0100 message to the issuer without DE 48, subelement 92.

## Program and Service Format Requirements

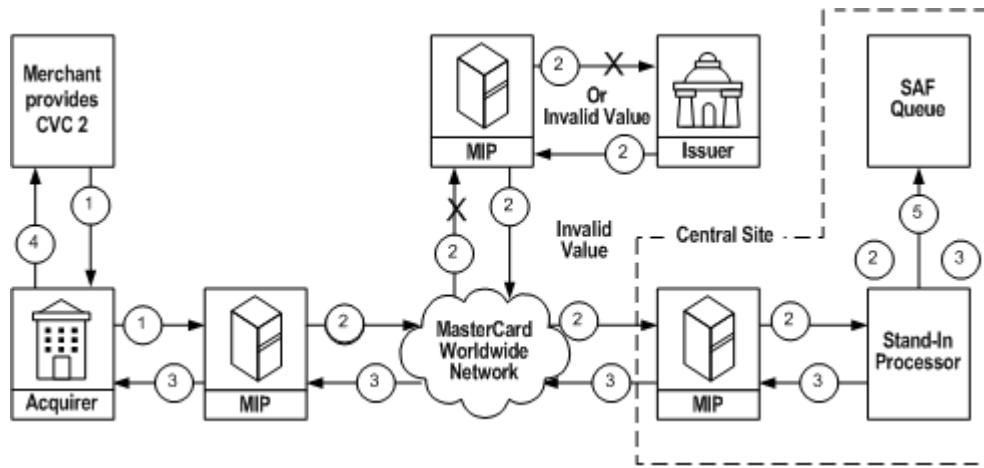
### Card Validation Code 2

3. After the issuer transmits the Authorization Request Response/0110 message, the acquirer MIP places value U (CVC 2 unverified — MasterCard use only) in DE 48, subelement 87 and forwards it to the acquirer.

The acquirer transmits the CVC 2 response code, provided by MasterCard in DE 48, subelement 87 of the Authorization Request Response/0110 message, to the merchant. The acquirer is responsible for ensuring that the merchant receives the CVC 2 response code.

## Authorization Request/0100—CVC 2 Processed by Stand-In

Following are the stages of an Authorization Request/0100—CVC 2 transaction processed by the Stand-In system.



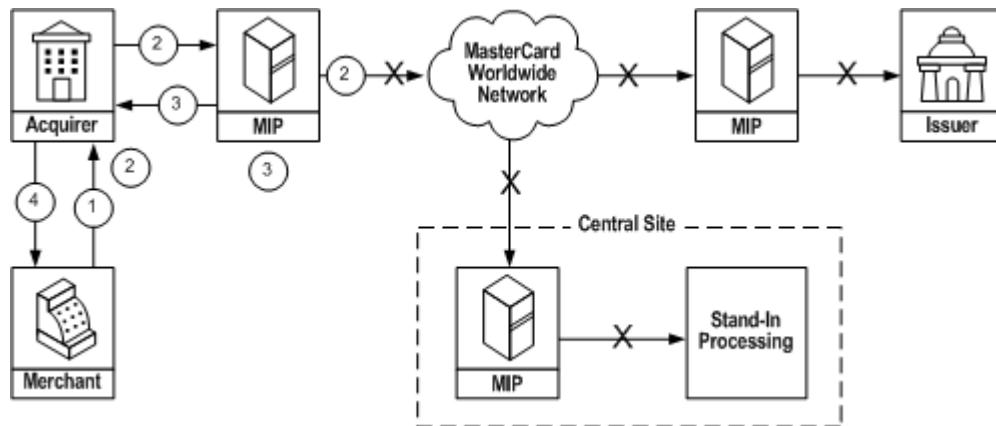
1. The merchant provides the CVC 2 value, and the acquirer generates an Authorization Request/0100 message with the CVC 2 value in DE 48, subelement 92.
2. Stand-In processing responds in the following conditions:
  - The issuer is not signed in.
  - The transaction cannot be delivered to the issuer.
  - The issuer is not responding.
  - The issuer's Authorization Request Response/0110 message fails an edit check and is rejected.
3. The Stand-In System generates the Authorization Request Response/0110 message.

WHEN the issuer is...	THEN the Authorization Platform...
Temporarily unable to receive the CVC 2 value	Places value U (CVC 2 unverified—MasterCard use only) in DE 48, subelement 87 and forwards the Authorization Request Response/0110 message to the acquirer.
Temporarily unable to process the CVC 2 value	Places a P (CVC 2 not processed—issuer temporarily unavailable) in DE 48, subelement 87 and forwards the Authorization Request Response/0110 message to the acquirer.

4. The acquirer transmits the CVC 2 response code, provided by the issuer or MasterCard in DE 48, subelement 87 of the Authorization Request Response/0110 message, to the merchant. The acquirer is responsible for ensuring that the merchant receives the CVC 2 response code.
5. The Stand-In System also generates Authorization Advice/0120 messages as appropriate and stores the advice in the Store-and-Forward (SAF) queue. The Stand-In System will include value U or P in DE 48, subelement 87 for issuers that are temporarily unavailable or otherwise unable to process the transaction.

## Authorization Request/0100—CVC 2 Processed by X-Code

Following are the stages of an Authorization Request/0100—CVC 2 transaction processed by the X-Code System.



1. The merchant supplies the CVC 2 value to acquirer.
2. The acquirer creates an Authorization Request/0100 message with the CVC 2 value, but the transmission is not successful.
3. The X-Code System by the acquirer's MIP responds based on current X-Code processing rules.

## Program and Service Format Requirements

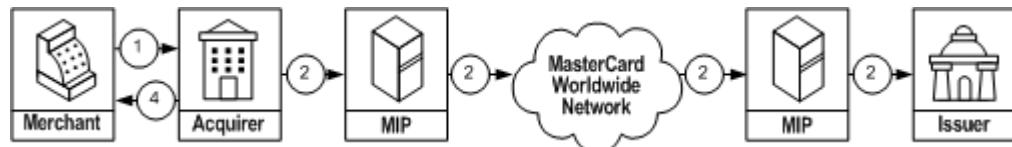
### Card Validation Code 2

WHEN the issuer is...	THEN the Authorization Platform...
Temporarily unable to receive the CVC 2 value	Places value U (CVC 2 unverified—MasterCard use only) in DE 48, subelement 87 and forwards the Authorization Request Response/0110 message to the acquirer.
Temporarily unable to process the CVC 2 value	Places a P (CVC 2 not processed—issuer temporarily unavailable) in DE 48, subelement 87 and forwards the Authorization Request Response/0110 message to the acquirer.

4. The acquirer transmits the CVC 2 response code, provided by MasterCard in DE 48, subelement 87 of the Authorization Request Response/0110 message, to the merchant. The acquirer is responsible for ensuring that the merchant receives the CVC 2 response code.
5. The Authorization Platform sends an Authorization Advice/0120 message to the issuer.

### Authorization Request/0100—Processed by Limit-1

Following are the stages of an Authorization Request/0100—CVC 2 transaction processed by Limit-1 processing.



1. The merchant supplies the CVC 2 value to acquirer.
2. If the issuer has chosen Limit-1 processing, and if CVC 2 is present in the Authorization Request/0100 message, the acquirer MIP bypasses Limit-1 processing and forwards the request to the issuer for processing.

### CVC 2 DE 48 Structure

The following diagram illustrates DE 48 subelements related to CVC 2 transactions.

LLL	“VAR”							
	1 byte	2 bytes	2 bytes	3 bytes	2 bytes	2 bytes	1 byte	
3 bytes Total Data Element Length	TCC	SE ID 92	SE Length 03	CVC 2 Value	SE ID 87	SE Length 01	Card Validation Code Result	

## Authorization Request/0100—CVC 2

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 14 (Date, Expiration)	C	•	C	Required for issuers to validate CVC 2 value
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	Must contain the appropriate TCC code.
DE 48, subelement 87 (Card Validation Code Result)		•	X	If an issuer's BIN is temporarily unable to receive the CVC 2 value, the Authorization Platform inserts the following value: U = CVC 2 unverified (MasterCard use only)
DE 48, subelement 92 (CVC 2)	C	•	C	Must be the three-digit CVC 2 value sent by the merchant to the acquirer.

## Authorization Request Response/0110—CVC 2

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	ME	•	ME	Must be present for registered CVC 2 issuers. Must also be present for unregistered CVC 2 issuers if the issuer is providing additional subelements (such as AVS response.) Must be present for all issuers.
DE 48, subelement 87 (Card Validation Code Result), CVC 1 and CVC 2	M	•	M	Contains one of the following CVC 2 response codes: M = Valid CVC 2 (match) N = Invalid CVC 2 (non-match) P = CVC 2 not processed (issuer temporarily unavailable) U = Issuer unregistered to process CVC 2 unverified (MasterCard use only) Y = Invalid CVC 1 (only if track data is present)
DE 48, subelement 92 (CVC 2)	CE	X	CE	Contains the CVC 2 code provided by the merchant to the acquirer.

## **Card Validation Code 3**

MasterCard supports card validation code 3 (CVC 3) result data in Authorization Request Response/0110 messages using DE 48, subelement 87 (Card Validation Code Result). Issuers performing CVC 3 validation in-house on *PayPass* transactions may use these CVC 3 values. When the CVC 3 is valid, the Authorization Request Response/0110 message should not contain DE 48, subelement 87.

### **Authorization Request Response/0110—CVC 3 Result**

MasterCard encourages issuers to include DE 48, subelement 87 when they perform CVC 3 validation and there is an issue with the CVC 3. When the CVC 3 is not valid, the issuer should send the acquirer the Authorization Request Response/0110 message containing CVC 3 result data. Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48 (Additional Data—Private use), subelement 87 (Card Validation Code Result)	C	•	C	E = Length of unpredictable number was not a valid length P = Could not be validated Y = Invalid

## **Currency Conversion**

The Authorization Platform automatically provides a currency conversion service to acquirers and issuers to allow processing of Authorization/01xx and Reversal/04xx messages in the customer's preferred currency.

Acquirers and issuers always will receive amount-related data elements in the acquirer's transaction currency and the issuer's cardholder billing currency even if they use the same currency. Acquirers and issuers have the option to receive amount-related data elements in the settlement currency (always U.S. dollars).

It is optional for the acquirer and issuer to receive amount-related data elements in the settlement currency (U.S. dollars) with the exception of issuers that send Authorization Advice/0120—Issuer-generated messages to RiskFinder. Issuers that send Authorization Advice/0120—Issuer-generated messages to RiskFinder are **required** to receive settlement amount-related data elements because RiskFinder processes in U.S. dollars.

Members that want to receive the currency conversion settlement amount-related data elements must complete Currency Conversion Parameters-Acquirer Issuer Form. Please contact a Customer Operations Services representative.

## Amount-Related Data Elements in Authorization and Reversal Messages

The following table lists how acquirers and issuers will send and receive amount-related data elements in authorization and reversal messages.

<b>DE</b>	<b>Acquirer Sends</b>	<b>Issuer Receives</b>	<b>Issuer Returns</b>	<b>Acquirer Receives</b>
4	In acquirer's transaction currency	In acquirer's transaction currency	In acquirer's transaction currency (echo except when responding with partial approval or purchase amount only—no cash back allowed)	In acquirer's transaction currency
5	N/A	In U.S. dollars if issuer receives settlement amount-related data elements  Not present if issuer does not receive settlement amount-related data elements	In U.S. dollars if issuer receives settlement amounts (echo except when responding with partial approval or purchase amount only—no cash back allowed)  Not present if issuer does not receive settlement amount-related data elements	In U.S. dollars if acquirer receives settlement amount-related data elements.  Not present if acquirer does not receive settlement amount-related data elements
6	N/A	In issuer's cardholder billing currency	In issuer's cardholder billing currency (echo except when responding with partial approval or purchase amount only—no cash back allowed)	In issuer's cardholder billing currency
9	N/A	Rate used to convert DE 4 amount from acquirer's transaction currency to U.S. dollars, if issuer receives settlement amount-related data elements  Not present if issuer does not receive settlement amount-related data elements	Rate used to convert DE 4 amount from acquirer's transaction currency to U.S. dollars, if issuer receives amount-related data elements (echo)  Not present if issuer does not receive settlement amount-related data elements	Rate used to convert DE 4 amount from the acquirer's transaction currency to U.S. dollars, if acquirer receives settlement amount-related data elements  Not present if acquirer does not receive settlement amount-related data elements

## Program and Service Format Requirements

### Currency Conversion

<b>DE</b>	<b>Acquirer Sends</b>	<b>Issuer Receives</b>	<b>Issuer Returns</b>	<b>Acquirer Receives</b>
10	N/A	Rate used to convert DE 4 amount from acquirer's transaction currency to issuer's cardholder billing currency	Rate used to convert DE 4 amount from acquirer's transaction currency to issuer's cardholder billing currency (echo)	Rate used to convert DE 4 amount from acquirer's transaction currency to issuer's cardholder billing currency
16	N/A	Month and day conversion rate is effective	Month and day conversion rate is effective (echo)	Month and day conversion rate is effective
28	Acquirer's transaction currency	Acquirer's transaction currency	Acquirer's transaction currency (echo)	Acquirer's transaction currency
49	Acquirer's transaction currency code.	Acquirer's transaction currency code	Acquirer's transaction currency code (echo)	Acquirer's transaction currency code
50	N/A	Settlement currency code (840) if issuer receives settlement amount-related data elements  Not present if issuer does not receive settlement amount-related data elements	Settlement currency code (840) if issuer receives settlement amount-related data elements (echo)  Not present if issuer does not receive settlement amount-related data elements	Settlement currency code (840) if acquirer receives settlement amount-related data elements  Not present if acquirer does not receive settlement amount-related data elements
51	N/A	Issuer's cardholder billing currency code	Issuer's cardholder billing currency code (echo)	Issuer's cardholder billing currency code
54	If applicable to the transaction, one occurrence of each amount type in acquirer's transaction currency	One occurrence of each amount type in acquirer's transaction currency  One occurrence of each amount type in issuer's cardholder billing currency	If applicable to the transaction, one occurrence of each amount type in issuer's cardholder billing currency (not an echo of what the acquirer sent)	One occurrence of each amount type in acquirer's transaction currency  One occurrence of each amount type in issuer's cardholder billing currency
95	If applicable, DE 95, subfield 1 in acquirer's transaction currency. DE 95, subfields 2–4 contain zeros	DE 95, subfield 1 in acquirer's transaction currency  DE 95, subfield 2 in U.S. dollars if issuer receives settlement amount-related data elements  DE 95, subfield 2 zero-filled if issuer does not receive settlement	Same values as received (echo)	DE 95, subfield 1 in acquirer's transaction currency  DE 95, subfield 2 in U.S. dollars if acquirer receives settlement amount-related data elements  DE 95, subfield 2 zero-filled if acquirer does not receive settlement

<b>DE</b>	<b>Acquirer Sends</b>	<b>Issuer Receives</b>	<b>Issuer Returns</b>	<b>Acquirer Receives</b>
		amount-related data elements		amount-related data elements
		DE 95, subfield 3 in issuer's cardholder billing currency		DE 95, subfield 3 in issuer's cardholder billing currency
		DE 95, subfield 4 zero-filled		DE 95, subfield 4 zero-filled

## Dual Message System Processing

The following Dual Message System processing notes apply to currency conversion processing.

If the acquirer provides DE 5, DE 6, DE 9, DE 10, DE 16, DE 50, or DE 51, the Authorization Platform will overwrite with the appropriate values in the message sent to the issuer. DE 5, DE 6, DE 9, DE 10, DE 16, DE 50, or DE 51 will be present, as defined, except when the Authorization Platform has declined an Authorization Request/0100 message and was unable to complete currency conversion processing.

If the settlement currency (U.S. dollars) is the same as the acquirer's currency, DE 5 will be the same value as in DE 4 and DE 9 will contain the value 61000000.

If the acquirer and issuer are the same currency, DE 6 will be the same value as in DE 4 and DE 10 will contain the value 61000000.

DE 54 will **not** contain additional occurrences of amount types in the settlement currency. DE 54 will only contain occurrences of amount types in U.S. dollars if it is the currency of the acquirer or issuer.

## Acquirer Send MTIs in Authorization and Reversal Messages

Acquirers are required to send and receive the following data elements in authorization and reversal messages.

<b>DE</b>	<b>Note</b>	<b>0100</b>	<b>0120</b>	<b>0400</b>
4	Acquirer's transaction currency	P	P	P
5	Always U.S. dollars			
6	Issuer's cardholder billing currency			
9	Factor used in conversion from transaction amount to settlement amount			
10	Factor used in conversion from transaction amount to cardholder billing amount			

## Program and Service Format Requirements

### Currency Conversion

DE	Note	0100	0120	0400
16	Always present			
28	Acquirer's transaction currency	P	P	P
49	Acquirer's transaction currency code	P	P	P
50	Always 840			
51	Issuer's cardholder billing currency code			
54	Occurrence of each amount type in acquirer's transaction currency			
54	Occurrence of each amount type in issuer's cardholder billing currency	P	P	P
95, sf 1	Acquirer's transaction currency			P
95, sf 2	Always U.S. dollars if acquirer chooses to receive settlement amounts, zero fill if not selected			Z
95, sf 3	Issuer's cardholder billing currency			Z
95, sf 4	Zero fill			Z

#### Table Key:

P under MTI = indicates that the data element will be present in that message.

X under MTI = indicates that the data element will be present if the acquirer chooses to receive settlement amount-related data elements.

Z under 0400 = indicates that if DE 95, subfield 1 is present, subfields 2-4 are zero-filled.

## Acquirer Receive MTIs in Authorization and Reversal Messages

Following are the acquirer receive MTS in Authorization and Reversal messages.

DE	Note	0110	0130	0410
4	Acquirer's transaction currency	P	P	P
5	Always U.S. dollars	X	X	X
6	Issuer's cardholder billing currency	P	P	P
9	Factor used in conversion from transaction amount to settlement amount	X	X	X
10	Factor used in conversion from transaction amount to cardholder billing amount	P	P	P
16	Always present	P	P	P
28	Acquirer's transaction currency	P	P	P

## Program and Service Format Requirements

### Currency Conversion

<b>DE</b>	<b>Note</b>	<b>0110</b>	<b>0130</b>	<b>0410</b>
49	Acquirer's transaction currency code	P	P	P
50	Always 840	X	X	X
51	Issuer's cardholder billing currency code	P	P	P
54	Occurrence of each amount type in acquirer's transaction currency	P		
54	Occurrence of each amount type in issuer's cardholder billing currency	P		
95, sf 1	Acquirer's transaction currency	P	P	
95, sf 2	Always U.S. dollars if acquirer chooses to receive settlement amounts, zero fill if not selected		X	
95, sf 3	Issuer's cardholder billing currency		P	
95, sf 4	Zero fill		P	

**Table Key:**

P under MTI = indicates that the data element will be present in that message.

X under MTI = indicates that the data element will be present if the acquirer chooses to receive settlement amount-related data elements.

## Issuer Receive MTIs in Authorization and Reversal Messages

Issuers are required to receive and send the following data elements in authorization and reversal messages.

<b>DE</b>	<b>Note</b>	<b>0100</b>	<b>0120</b>	<b>0130</b>	<b>0400</b>	<b>0420</b>	<b>0620</b>
4	Acquirer's transaction currency	P	P	P	P	P	P
5	Always U.S. dollars	X	X	P	X	X	P
6	Issuer's cardholder billing currency	P	P	P	P	P	P
9	Factor used in conversion from transaction amount to settlement amount	X	X	P	X	X	P
10	Factor used in conversion from transaction amount to cardholder billing amount	P	P	P	P	P	P
16	Always present	P	P	P	P	P	P
28	Acquirer's transaction currency	P	P	P	P	P	P
49	Acquirer's transaction currency code	P	P	P	P	P	P
50	Always 840	X	X	P	X	X	P
51	Issuer's cardholder billing currency code	P	P	P	P	P	P

## Program and Service Format Requirements

### Currency Conversion

DE	Note	0100	0120	0130	0400	0420	0620
54	Occurrence of each amount type in acquirer's transaction currency	P	P		P	P	P
54	Occurrence of each amount type in issuer's cardholder billing currency	P	P		P	P	P
95, sf 1	Acquirer's transaction currency				P	P	
95, sf 2	Always U.S. dollars if selected, zero fill if not selected				X	X	
95, sf 3	Issuer's cardholder billing currency				P	P	
95, sf 4	Zero fill				P	P	

**Table Key:**

P under MTI = indicates that the data element will be present in that message

X under MTI = indicates that the data element will be present if the issuer chooses to receive settlement amount-related data elements.

### Issuer Send MTIs in Authorization and Reversal Messages

Following are the data elements issuer send in authorization and reversal currency conversion transactions.

DE	Note	0110	0120	0130	0410	0430
4	Acquirer's transaction currency	P	P	P	P	P
5	Always U.S. dollars	X	P	X	X	X
6	Issuer's cardholder billing currency	P	P	P	P	P
9	Factor used in conversion from transaction amount to settlement amount	X	P	X	X	X
10	Factor used in conversion from transaction amount to cardholder billing amount	P	P	P	P	P
16	Always present	P	P	P	P	P
28	Acquirer's transaction currency	P	P	P	P	P
49	Acquirer's transaction currency code	P	P	P	P	P
50	Always 840	X	P	X	X	X
51	Issuer's cardholder billing currency code	P	P	P	P	P
54	Occurrence of each amount type in acquirer's transaction currency			P		
54	Occurrence of each amount type in issuer's cardholder billing currency	P	P			

DE	Note	0110	0120	0130	0410	0430
95, sf 1	Acquirer's transaction currency			P	P	
95, sf 2	Always U.S. dollars if selected, zero fill if not selected			X	X	
95, sf 3	Issuer's cardholder billing currency			P	P	
95, sf 4	Zero fill			P	P	

**Table Key:**

P under MTI = indicates that the data element will be present in that message.

I under MTI = indicates that the issuer will return the data element in the response message if the issuer chooses to receive settlement amount-related data elements in the original request or advice message

## Currency Conversion in RiskFinder Transactions

Following are considerations in currency conversion processing in RiskFinder transactions.

Authorization Advice/0120 messages that the issuer sends to RiskFinder always must contain settlement amount-related data elements because RiskFinder processes in U.S. dollars. This is why issuers that send Authorization Advice/0120—Issuer-generated messages to RiskFinder are required to receive settlement amount-related data elements. As such, issuers must also be prepared to receive settlement amount-related data elements in DE 120 of Administrative Advice/0620—RiskFinder messages.

Issuers that have chosen to have the Authorization Platform generate Authorization Advice/0120 messages to RiskFinder must be prepared to receive settlement amount-related data elements in DE 120 of Administrative Advice/0620—RiskFinder messages, because the Authorization Platform also will send settlement amount-related data elements in the Authorization Advice/0120 messages to RiskFinder. This is regardless of whether the issuer is enabled to receive settlement amount-related data elements.

## Alternate Processing

Following are details regarding currency conversion in alternate processing.

Authorization Advice/0120 and Reversal Advice/0420 messages that the issuer receives through Store-and-forward (SAF) processing will always contain amount-related data elements in the acquirer's transaction currency and the issuer's cardholder billing currency.

SAF messages will contain amount-related data elements in the settlement currency (U.S. dollars) according to the issuer's preference for receiving these data elements.

## Authorization Platform Edits

The Authorization Platform ensures that amount-related data elements, if present in the following response messages from the issuer, are the same values as provided in the request messages sent to the issuer.

Issuers should echo amount-related data elements in response messages as they were received in the request messages. The exception is when an issuer provides DE 39 (Response Code), value 10 (Partial approval) or 87 (Purchase amount only, no cash back allowed) in an Authorization Request Response/0110 message. When providing either of these responses, the issuer is required to provide DE 6 and DE 51 according to the specifications for partial approvals and purchase of goods or services with cash back.

<b>IF...</b>	<b>THEN the Authorization Platform...</b>
<b>Authorization Request Response/0110</b>	
The value in DE 39 is not 10 (Partial approval) or 87 (Purchase only, no cash back allowed), and the amount-related data elements returned by the issuer are different from the values received by the issuer	Generates and forwards to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = the data element in error
<b>Reversal Request Response/0410</b>	
The amount-related data elements returned by the issuer are different from the values received by the issuer	Generates and forwards to the issuer an Authorization Response Negative Acknowledgement/0190 where: DE 39 = 30 DE 44 = the data element in error
<b>IF...</b>	<b>THEN the Authorization Platform...</b>
<b>Authorization Request/0100 or Authorization Advice/0120</b>	
No occurrence of DE 54, subfield 3 (Currency Code) is equal to the currency code in DE 49	Generates and forwards to the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: DE 39 = 30 DE 44 = 054
DE 54 contains more than two occurrences of the DE 54 subfields	Generates and forwards to the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: DE 39 = 30 DE 44 = 054

IF...	THEN the Authorization Platform...
DE 54 contains more than one occurrence of the DE 54 subfields for a given amount type (subfield 2)	Generates and forwards to the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: DE 39 = 30 DE 44 = 054
The combined length of one occurrence of DE 54 subfields 1–4 is not equal to 20 bytes	Generates and forwards to the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: DE 39 = 30 DE 44 = 054
DE 54, subfields 1–3 are not numeric	Generates and forwards to the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: DE 39 = 30 DE 44 = 054
The first position in DE 54, subfield 4 is not C or D, followed by 12 numeric digits	Generates and forwards to the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: DE 39 = 30 DE 44 = 054
<b>Authorization Request Response/0110</b>	
No occurrence of DE 54, subfield 3 (Currency Code) is equal to the currency code in DE 51	Generates and forwards to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 054
The value in DE 39 is not 10 or 87 and DE 54 contains more than two occurrences of the DE 54 subfields	Generates and forwards to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 054
The value in DE 39 is 10 or 87 and DE 54 contains more than one occurrence of DE 54, subfield 2 (Amount Type) that is not equal to 57 (Original Amount)	Generates and forwards to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 054

## Program and Service Format Requirements

### Electronic Commerce Processing

IF...	THEN the Authorization Platform...
DE 54 contains more than one occurrence of DE 54 subfields for a give amount type (subfield 2)	Generates and forwards to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 054
The combined length of one occurrence of DE 54 subfields 1–4 is not equal to 20 bytes	Generates and forwards to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 054
DE 54, subfields 1–3 are not numeric	Generates and forwards to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 054
The first position in DE 54, subfield 4 is not C or D, followed by 12 numeric digits	Generates and forwards to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 054

## Electronic Commerce Processing

Electronic commerce transactions are non-face-to-face online transactions using electronic media over any public network, such as the Internet, or private network, such as an extranet. Electronic commerce processing allows transactions to be initiated from a cardholder-controlled device, such as a PC, for purchasing goods and services on the Internet.

All electronic commerce transactions must be uniquely identified by the acquirer in the authorization. This permits the issuer to assess the degree of risk associated with the transaction and to support any processing requirements associated with interchange compliance.

The Authorization Request/0100 includes the security level indicator (in DE 48, subelement 42) that indicates the following security attributes of electronic commerce transactions:

- Security protocol, which indicates the security protocol that was used to facilitate the transaction (for example, channel encryption).
- Cardholder authentication, which indicates the method of cardholder authentication used to facilitate the transactions.

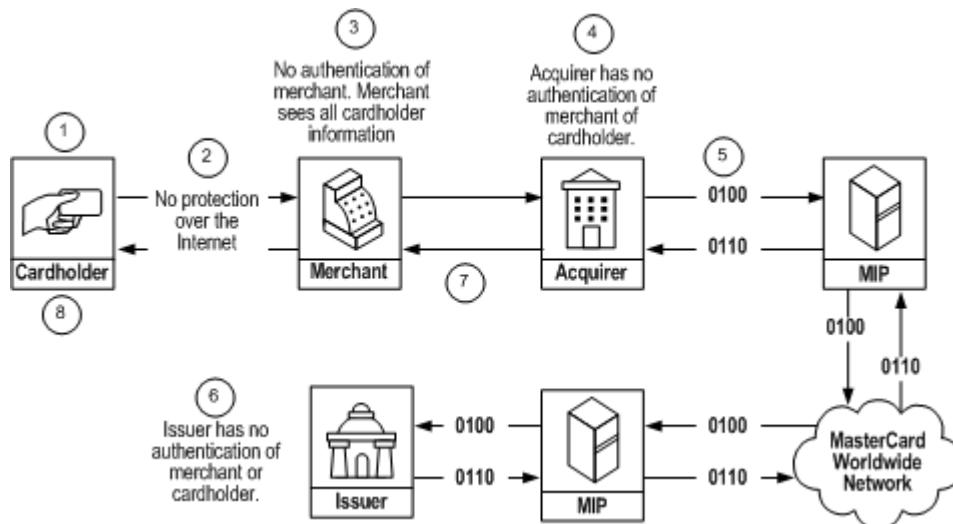
- UCAF collection indicator, which indicates both merchant UCAF readiness and inclusion of any specific authentication data in the UCAF field (DE 48, subelement 43).

MasterCard messaging requirements regarding the security of electronic commerce transactions may vary depending upon the security protocol involved in the transaction. Methods may include:

- No security protocol
- Channel encryption
- MasterCard® SecureCode™ Transaction using the Universal Cardholder Authentication Field (UCAF)®

## No Security Protocol

This message flow describes an Authorization Request/0100—Electronic Commerce transaction with no security protocol.



1. The cardholder browses the Internet until the cardholder is ready to make a purchase from a merchant. In this example, the cardholder does not have authentication of the merchant at any time.
2. The cardholder's browser sends the purchase and payment information over the Internet to the merchant. In this example, no security protocol protects the request.
3. The merchant receives the purchase information and has access to all of the cardholder account data that the cardholder provided (including payment information).
4. The merchant requests authorization from the acquirer.
5. The acquirer generates an Authorization Request/0100 message, including both of the following:

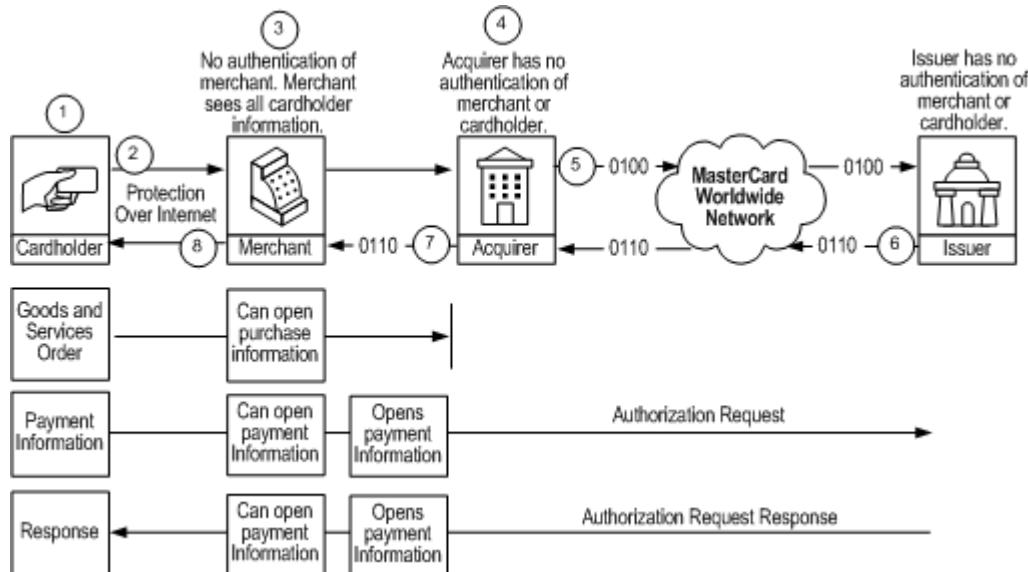
## Program and Service Format Requirements

### Electronic Commerce Processing

- Cardholder payment data
  - Appropriate data element values that identify this as an e-commerce transaction with no security protocol and no cardholder authentication
6. The issuer receives the authorization request and generates an Authorization Request Response/0110 message.
  7. The acquirer receives the Authorization Request Response/0110 message and sends the response back to the merchant.
  8. The merchant provides acknowledgement to the cardholder (still unprotected as it travels over the Internet).

## Channel Encryption

This message flow describes an Authorization Request/0100—Electronic Commerce transaction that uses channel encryption protocol between the cardholder and the merchant.



1. The cardholder browses the Internet until the cardholder is ready to make a purchase from a merchant.
2. The cardholder's browser, which supports channel encryption (that is, SSL), sends the purchase and payment information to the merchant. Channel encryption protects the information over the Internet.
3. The merchant receives the purchase information and has access to all of the cardholder account data that the cardholder provided.
4. The merchant requests authorization from the acquirer.
5. The acquirer generates an Authorization Request/0100 message, including both of the following:
  - The cardholder payment data

- The appropriate data element values that identify this as an e-commerce transaction with channel encryption protocol and no cardholder authentication.
6. The issuer receives the authorization request and generates an Authorization Request Response/0110 message.
  7. The acquirer receives the Authorization Request Response/0110 and sends the response back to the merchant.
  8. The merchant provides acknowledgement to the cardholder (protected by channel encryption as it travels over the Internet).

## Authorization Request/0100—Electronic Commerce Purchase

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 22 (Point-of-Service (POS) Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	81 = PAN entry via electronic commerce, including chip
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	Contains one of the following values: P = Payment Transaction T = Phone, Mail, or Electronic Commerce Order U = Unique X = Airline and Other Transportation Services (irrespective of the transaction origin is face to face or not)
DE 48, subelement 40 (Electronic Commerce Merchant/Cardholder Certificate Serial Number [Visa Only]), subfield 1 (Merchant/Certificate Serial Number)	C	•	C	DE 48 subelement 40 is not required for any MasterCard e-commerce programs. Merchant certificate serial number in binary format
DE 48, subelement 40, subfield 2 (Cardholder Certificate Serial Number)	C	•	C	Cardholder certificate serial number in binary format
DE 48, subelement 42 (Electronic Commerce Security Level Indicator)	M	•	M	Contains security level in positions 1 and 2 and UCAF collection indicator in position 3. Position 1 = Security Protocol Position 2 = Cardholder Authentication Position 3 = UCAF Collection Indicator

## Program and Service Format Requirements

### Electronic Commerce Processing

Data Element	Org	Sys	Dst	Values/Comments
DE 48, subelement 43 (Universal Cardholder Authentication) For MasterCard SecureCode issuer or cardholder generated authentication data	C	•	C	Authentication data generated by SecureCode-compliant solution.
DE 48, subelement 43 (Universal Cardholder Authentication)	C	•	C	A static Accountholder Authentication Value assigned by MasterCard for use with this Program.
DE 48, subelement 43 (Universal Cardholder Authentication) for Visa 3-D Secure Electronic Commerce Verification Service (Visa Only)	C	•	C	Position 1 (Visa 3-D Secure Electronic Commerce Transaction Indicator) 8 = Indicates Secure Electronic Commerce Transaction Position 2–21 (Visa 3-D Secure Electronic Commerce Cardholder Authentication Verification Value [CAVV]) = Cardholder Authentication Verification Value (CAVV)
DE 48, subelement 44 (Electronic Commerce Transaction Identifier [XID] [Visa Only])	C	•	C	Contains the 3-D Secure Electronic Commerce Transaction Identifier (XID) value in binary format.
DE 61 (Point-of-Service (POS) Data), subfield 3 (POS Terminal Location)	M	•	M	2 = Off premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA)
DE 61, subfield 4 (POS Cardholder Presence)	M	•	M	For a recurring payment arrangement in which the first payment is an electronic commerce transaction, use: 4 = Standing order/recurring transactions (required for the first transaction in a recurring payment arrangement) For all other e-commerce transactions use: 5 = Electronic order (home PC, Internet, mobile phone, PDA)
DE 61, subfield 7 (POS Transaction Status)	M	•	M	Must not contain value 2 (SecureCode Phone Order)
DE 61, subfield 10 (Cardholder-Activated Terminal Level)	M	•	M	6 = Authorized Level 6 CAT: Electronic commerce

## Authorization Request Response/0110—Electronic Commerce Purchase

When any response data is present in DE 48 (such as AVS response, CVC 2 response), the issuer uses a normal Authorization Request Response/0110, with all of the subelements present in the original Authorization Request/0100 message echoed back. Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	CE	•	CE	Must be the same value as in the original Authorization Request/0100 message.
DE 48, subelement 40 (Electronic Commerce Merchant/Cardholder Certificate Serial Number [Visa Only])	CE	•	CE	Must be the same value as in the original Authorization Request/0100 message, if present.
DE 48, subelement 42 (Electronic Commerce Security Level Indicator)	ME	•	ME	Must be the same value as in the original Authorization Request/0100 message.
DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF])	CE	•	CE	Must be the same value as in the original Authorization Request/0100 message, if present.
DE 48, subelement 44 Electronic Commerce Transaction Identifier [XID] [Visa Only]	CE	•	CE	Must be the same value as in the original Authorization Request/0100 message, if present. (Visa Only.)
DE 48, subelement 45 (Three-Domain (3-D) Secure Electronic Commerce Transaction Response Code [Visa Only])	C	•	C	Contains the Visa 3-D Secure CAVV Results Code, if present. (Visa only).

## Authorization Platform Edits

MasterCard performs the following edits on Authorization Request/0100 messages for MasterCard Electronic Card transactions.

## **Program and Service Format Requirements**

### **Electronic Commerce Processing**

---

<b>WHEN...</b>	<b>THEN The Authorization Platform...</b>
DE 22, subfield 1 contains value 81 and DE 61, subfield 4 contains value 4 or 5 and DE 61, subfield 10 contains value 6 and DE 48, subelement 42, subfield 1, position 3 does not contain value 2 or 3	Performs a cross edit (found in DE 61) between DE 48, subelement 42, subfield 1, position 3 and DE 61.
This edit passes...	Performs the existing cross-edit between DE 48, subelement 42, subfield 1, position 3 and DE 48, subelement 43 to ensure that the Authorization Request/0100 message contains the UCAF field.
This edit fails...	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 30 DE 44 = 048

## **MasterCard SecureCode**

The MasterCard® *SecureCode*™ program encompasses varying solution-oriented protocols that all build upon the infrastructure requirements for channel encryption with the additional benefit of cardholder authentication. When used in conjunction with components of the MasterCard payment infrastructure, this program provides a mechanism for online merchants to potentially receive an enhanced payment guarantee similar to what retailers (non-Internet) receive with qualifying physical point-of-sale transactions.

When participating in the MasterCard *SecureCode* program, the UCAF data must be included in the authorization to the issuer when it is available (in DE 48, subelement 43). It is a variable length (maximum 32 characters) field with a flexible data structure that can be tailored to support the needs of issuer security and authentication approaches.

### **Universal Cardholder Authentication Field**

The Universal Cardholder Authentication Field (UCAF) is a standard, globally interoperable method of collecting cardholder authentication data at the point of interaction.

Within the MasterCard authorization networks, UCAF is a universal, multipurpose data transport infrastructure that is used to communicate authentication information between cardholders, merchants, issuers, and acquirers. It is a variable length (maximum 32 characters) field with a flexible data structure that can be tailored to support the needs of issuer security and authentication approaches.

## Accountholder Authentication Value

The Accountholder Authentication Value (AAV) is a MasterCard *SecureCode*-specific implementation of UCAF related to issuer authentication platforms that incorporate the Secure Payment Application (SPA) algorithm. SPA is a MasterCard security method designed to authenticate cardholders when they pay online.

AAV is generated by the issuer and presented to the merchant for placement in the authorization request upon successful authentication of the cardholder.

UCAF is used to transmit the AAV from the merchant to the issuer for authentication purposes during the authorization process.

Issuers that want to use AAV verification may implement the following AAV verification services:

- MasterCard *SecureCode* AAV Verification
- MasterCard *SecureCode* Dynamic AAV Verification in Stand-In Processing

### MasterCard *SecureCode* AAV Verification Service

For issuers that want to have MasterCard verify the AAV before providing the Authorization Request/0100 message to the issuer, MasterCard offers AAV verification service on every authorization transaction that contains UCAF data—regardless of whether the issuer's host system is available or unavailable to respond to the Authorization Request/0100 message.

When the issuer's host system is available and after the verification process is complete, MasterCard includes in the Authorization Request/0100 message DE 48, subelement 71 (On-behalf Services) containing:

- Subfield 1 (On-behalf [OB] Service) with the value 05
- Subfield 2 (On-behalf [OB] Result 1) with the value I, U, or V

In the event that the issuer's host system is unavailable, MasterCard processes the Authorization Request/0100 message on behalf of the issuer and Stand-In processing creates an Authorization Advice/0120 (SAF) message where DE 48, subelement 71 contains:

- Subfield 1 (On-behalf [OB] Service) with the value 05
- Subfield 2 (On-behalf [OB] Result 1) with the value U
- Subfield 3 (On-behalf [OB] Result 2) value blank

MasterCard *SecureCode* AAV Verification service is an optional service.

### **MasterCard *SecureCode* Dynamic AAV Verification in Stand-In Processing**

For issuers that want to have MasterCard verify AAV in Stand-In processing only, MasterCard offers AAV verification service for authorization transactions processed by Stand-In processing that contain AAV data in DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]) of the Authorization Request/0100 message.

Issuers that want to participate in the MasterCard *SecureCode* Dynamic AAV verification in Stand-In processing will provide the confidential key data for MasterCard use in the verification process. MasterCard applies an algorithm to the issuer's confidential key data, the AAV, and the issuer's PAN to determine the validity of the AAV data provided by the acquirer.

MasterCard uses DE 48, subelement 71 (On-behalf Services) in the Authorization Advice/0120 message to communicate the results of the AAV verification test to the issuer:

- Subfield 1 (On-behalf [OB] Service) contains value 06 (MasterCard *SecureCode* Dynamic AAV Verification Service).
- Subfield 2 (On-behalf [OB] Result 1) with the value I, U, or V
- Subfield 3 (On-behalf [OB] Result 2) is blank (space)

MasterCard *SecureCode* Dynamic AAV Verification in Stand-In Processing is an optional service.

For more information about *SecureCode*, including detailed transaction flows and participation requirements, see the *SecureCode Member Enrollment and Implementation Guide*.

## **Static AAV and the Maestro and MasterCard Advance Registration Programs**

The Maestro® Advance Registration Program™ and MasterCard® Advance Registration Program™ enable enrolled merchants that have met specific qualification criteria, to accept Maestro and MasterCard cards for electronic commerce (e-commerce) transactions without using MasterCard® *SecureCode*™ to authenticate every transaction. Merchants are required to perform full MasterCard *SecureCode* authentication on the first transaction they perform for any individual cardholder.

As part of the Maestro and MasterCard Advance Registration programs, MasterCard:

- Assigns participating merchants a static Accountholder Authentication Value (AAV) for use with transactions that are processed without MasterCard *SecureCode* authentication.
- Allocates participating merchants a MasterCard Assigned ID

MasterCard static AAV UCAF data is identified in Authorization Request/0100 messages by DE 48 (Additional Data—Private Use), subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), position 3 (UCAF Collection Indicator), value 3 (UCAF data collection is supported by the merchant, and (UCAF [MasterCard assigned Static Accountholder Authentication Value] data must be present)

Acquirers must provide the MasterCard assigned merchant ID in DE 48, subelement 32 (MasterCard Assigned ID) of Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages.

The combination of static AAV data submitted in the Universal Cardholder Authentication Field (DE 48, subelement 43) and the MasterCard assigned merchant ID (DE 48, subelement 32) is unique and is verified by the Authorization Platform.

#### **NOTE**

**The MasterCard SecureCode AAV Verification Service and MasterCard SecureCode Dynamic AAV Verification in Stand-In Processing will not be performed on Maestro e-commerce transactions that are processed under the Maestro or MasterCard Advance Registration Program. These on-behalf services will continue to be performed on Maestro e-commerce transactions that are authenticated using MasterCard SecureCode.**

## **Forgotten Card at ATM**

Forgotten card at ATM service invokes when a cardholder leaves the terminal without taking his or her card or when the cardholder cannot retrieve the card from the terminal for a technical reason. This service is available only to customers that participate in Swedish Domestic Authorization Switching Service (SASS).

### **Reversal Request/0400—Forgotten Card**

Following is a list of the data elements and values applicable to this message type. All mandatory Reversal Request/0400 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	Contains one of the following values: 01 = Withdrawal 30 = Balance Inquiry
DE 4 (Amount, Transaction)	M	•	M	Contains value zero
DE 48 (Additional Data—Private Use), subelement 58 (ATM Additional Data)	O	X	C	Subfield data may be present for Swedish ATMs

## Program and Service Format Requirements

### Fraud Scoring Service

---

#### NOTE

If the issuer does not support DE 48, subelement 58, the Authorization Platform will send the acquirer a Reversal Request Response/0410 message containing DE 39 (Response Code), value 57 (Transaction not permitted to issuer/cardholder).

## Fraud Scoring Service

This optional service enhances MasterCard fraud management services by providing issuers with a real-time score on dual message authorization transactions, using state-of-the-art predictive modeling technology. The score indicates the measure of how likely it is that the transaction is fraudulent.

The fraud score on an authorization transaction is a 3-digit number ranging from 000 through 999. The higher the score, the more likely it is that the transaction is fraudulent.

### Authorization Request/0100—Fraud Scoring

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 48, subelement 71 (On-behalf Services), subfield 1 (On-behalf [OB] Service)	•	X	C	18 = Fraud Scoring Service
DE 48, subelement 71 (On-behalf Services), subfield 2 (On-behalf Result 1)	•	X	C	Contains one of the following values: C = Expert Monitoring Fraud Scoring Service was performed successfully U = Expert Monitoring Fraud Scoring Service was not performed successfully
DE 48, subelement 75 (Fraud Scoring Data), subfield 1 (Fraud Score Data)	•	X	C	The Authorization Platform inserts this subelement when the Expert Monitoring Fraud Scoring Service is performed on the transaction.  Fraud Scoring System provides the risk score of 000–999 in subfield 1, where 999 is more likely to be fraudulent than a score of 000.
DE 48, subelement 75 (Fraud Scoring Data), subfield 2 (Score Reason Code)	•	X	C	Fraud Scoring System provides the score reason code in subfield 2, which indicates the key factors that influenced the fraud score.  Subfield 2 is provided whenever a fraud score is provided in subfield 1 (Fraud Score Data).

## Alternate Processing

The following table indicates the Authorization Advice/0120 content when the transaction is qualified for the Fraud Scoring Service, but the issuer is unavailable and Stand-In processing is invoked.

Stand-In and X-code processing do not consider the fraud assessment score when performing an authorization decision for an issuer.

IF...	THEN the Authorization Advice/0120—System-generated message will contain...
If the original Authorization Request/0100 message was successfully scored	DE 48, subelement 75 and DE 48, subelement 71, subfield 1, value 18 and subfield 2, value C indicating Expert Monitoring Fraud Scoring Service was performed on the transaction
If the original Authorization Request/0100 message was not successfully scored	DE 48, subelement 71, subfield 1, value 18 and Subfield 2, value U indicating Expert Monitoring Fraud Scoring Service was not performed on the transaction

## Gaming Payment Transactions

Gaming payment transactions allows participating acquirers to send gaming payment transactions only to issuers in countries where online gaming and the crediting of gaming winnings to cards is permitted by law.

Participating acquirers in the Europe region that want to process payment transactions on gaming winnings can use the Authorization Request/0100—Gaming Payment and Reversal Request/0400—Gaming Payment messages.

## Authorization Request/0100—Gaming Payment

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	28 = Payment Transaction
DE 4 (Amount, Transaction)	M	•	M	Maximum amount EUR 5,000
DE 18 (Merchant Type)	M	•	M	Must contain value 7995 = Gambling Transaction

## **Program and Service Format Requirements**

### **Gaming Payment Transactions**

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode),	M	•	M	81 = PAN entry via electronic commerce, including chip
DE 48, (Additional Data—Private Use), TCC	M	•	M	P = (Payment Transaction)
DE 48, subelement 77 (Payment Transaction Type Indicator)	M	•	M	C04 = Gaming Re-pay

### **Reversal Request/0400—Gaming Payment**

Following is a list of the data elements and values applicable to this message type. All mandatory Reversal Request/0400 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	28 = Payment Transaction
DE 4 (Amount, Transaction)	M	•	M	Maximum amount EUR 5,000
DE 18 (Merchant Type)	M	•	M	Must contain value 7995 = Gambling Transaction
DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode),	M	•	M	81 = PAN entry via electronic commerce, including chip
DE 48, (Additional Data—Private Use), TCC	M	•	M	P = (Payment Transaction)
DE 48, subelement 77 (Payment Transaction Type Indicator)	M	•	M	C04 = Gaming Re-pay

## Authorization Platform Edits

The following edits apply to Gaming Payment transactions.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 3, subfield 1 = 28 DE 18 = 7995 DE 48, TCC = P and The acquirer is not a registered gaming participant	Sends the acquirer an Authorization Request Response/0110 or a Reversal Request Response/0410 message where: DE 39 = 58 (Transaction not permitted to acquirer/terminal)
DE 3, subfield 1 = 28 DE 18 = 7995 DE 48, TCC = P and The issuer country does not allow gaming payment transactions	Sends the acquirer an Authorization Request Response/0110 or a Reversal Request Response/0410 message where: DE 39 = 57 (Transaction not permitted to issuer/cardholder)
DE 3, subfield 1 = 28 DE 18 = 7995 DE 48, TCC = P and The amount in DE 4 exceeds EUR 5,000	Sends the acquirer an Authorization Request Response/0110 or a Reversal Request Response/0410 message where: DE 39 = 13 (Invalid amount)

## Maestro Pre-authorized Transactions

The Authorization Platform allows acquirers to request pre-authorization on transactions for which the amount is not yet determined. Once the issuer approves the pre-authorization request and after the transaction has taken place and the final amount is determined, the acquirer must then send an Authorization Advice/0120 message to the issuer within 20 minutes of the authorization response message completion. This service is available only for Maestro Petrol transactions.

### Authorization Request/0100—Maestro Pre-Authorization

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 4 (Amount, Transaction)	M	•	M	Maximum amount determined by the acquirer or merchant.
DE 18 (Merchant Type)	M	•	M	Must contain value 5542 = Fuel Dispenser, Automated

## **Program and Service Format Requirements**

### **Maestro Recurring Payments Program**

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status)	M	•	M	Must contain value 4 = Preauthorized request.
DE 61, subfield 10 (Card-Activated Terminal Level)	M	•	M	1 = Authorized Level 1 CAT: Automated dispensing machine with PIN

### **Authorization Advice/0120—Maestro Pre-Authorization Completion**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Advice/0120 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 4 (Amount, Transaction)	M	•	M	Must contain the final transaction amount
DE 48 (Additional Data—Private Use), subelement 15 (Authorization Platform Advice Date and Time)	•	X	M	Authorization Platform supplies date and time.
DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code)	M	•	M	191 = Acquirer Processing System (APS) completed Note: Issuers must also be prepared to receive value 190 (Acquirer Processing System (APS) approved)

### **Matching Request and Advice Messages**

To match the original Authorization Request/0100 with the Authorization Advice/0120, the following DEs should be used:

- DE 2 (Primary Account Number [PAN])
- DE 7 (Transmission Date and Time)
- DE 11 (System Trace Audit Number [STAN])
- DE 32 (Acquiring Institution ID Code)
- DE 33 (Forwarding Institution ID Code)

## **Maestro Recurring Payments Program**

Maestro® Recurring Payments Program™, enables the Maestro brand to accept recurring payments for electronic commerce (e-commerce) transactions. This program enables Maestro branded products to build on the existing Maestro Advance Registration Program by providing enhanced value to customers.

## Acquirer Requirements

- Acquirers in the Europe region that process Maestro e-commerce transactions may participate in the Maestro Recurring Payments Program. Acquirers registered for the Maestro Advance Registration Program automatically will be able to participate in the Maestro Recurring Payments Program.
- Participating acquirers must submit the following values in Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, and Reversal Request/0400—Acquirer-generated messages to identify Maestro e-commerce recurring payment transactions received from enrolled merchants:
  - DE 22 (Point of Service Data Code), subfield 1 (Terminal Data: Card Data Input Capability), value 81 (PAN manual entry via e-commerce)
  - DE 48 (Additional Data—Private Use), subelement 32 (MasterCard Assigned ID)
  - DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), position 3 (UCAF Collection Indicator), value 3 (UCAF data collection is supported by the merchant, and UCAF (MasterCard Assigned Static AAV) data must be present)
  - DE 48, subelement 43 (Static AAV for Maestro or MasterCard Advance Registration Program)
  - DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence), value 4 (Standing order/recurring transactions)
  - DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level), value 6 (CAT Level 6: Electronic commerce transaction

## Issuer Requirements

- Maestro issuers must support receipt and processing of recurring payment e-commerce transactions, as identified by the presence of the following data elements in Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, Authorization Advice/0120—System-generated, Reversal Request/0400—Acquirer-generated, and Reversal Request/0400—System-generated messages:
  - DE 22, subfield 1, value 81
  - DE 48, subelement 32
  - DE 48, subelement 42, subfield 1, position 3, value 3
  - DE 48, subelement 43
  - DE 61, subfield 4, value 4
  - DE 61, subfield 10, value 6

## Program and Service Format Requirements

### Maestro Recurring Payments Program

---

- Maestro issuers also must provide the following data elements in Authorization Request Response/0110, Authorization Advice Response/0130—System-generated, and Reversal Request Response/0410 messages:
  - DE 48, subelement 42
  - DE 48, subelement 43

### Authorization Request/0100—Maestro Recurring Payment

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element ID and Name	Org	Sys	Dst	Comments
DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	81 = PAN entry via electronic commerce, including chip.
DE 48 (Additional Data—Private Use), subelement 32 (MasterCard Assigned ID)	C	•	C	The value assigned by MasterCard
DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), position 3 (UCAF Collection Indicator)	C	•	C	3 = UCAF data collection is supported by the merchant, and UCAF (MasterCard assigned static Accountholder Authentication Value) data must be present. <b>Note:</b> DE 48, subelements 32 and 43 are required for Static AAV transactions.
DE 48, subelement 43 (Static AAV for Maestro or MasterCard Advance Registration Program)	C	•	C	Contains the contents of positions 1–28. When DE 48, subelement 43 contains a static AAV, DE 48, subelement 32 is mandatory.
DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence)	M	•	M	4 = Standing order/recurring payment
DE 61, subfield 10 (Cardholder-Activated Terminal Level)	M	•	M	6 = Authorized Level 6 CAT: Electronic Commerce

### Authorization Platform Edits

The following edits are performed on Authorization Request/0100 messages for Maestro Recurring Payment Program transactions.

MasterCard uses the following edit to verify participation in the Maestro Recurring Payments Program. Authorization Platform uses this edit to validate the value in DE 48, subelement 32 for Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages.

**NOTE**

**Note that the same Static AAV value can be used for both the Maestro Advance Registration Program and the Maestro Recurring Payments Program.**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
An Authorization Request/0100 or Authorization Advice/0120 System-generated message with DE 48, subelement 42, subfield 1, position 3, value 3	Validates that DE 48, subelement 32 and subelement 43 are present and contain valid values.

**Existing Edits**

The following existing Maestro Advance Registration Program edits will be applied to the Maestro Recurring Registration Payment Program in the Authorization Platform where the value 3 (UCAF data collection is supported by the merchant, and UCAF [MasterCard assigned Static Accountholder Authentication Value] data must be present for Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages submitted under the Maestro Recurring Payments Program for e-commerce initiated transactions.

<b>WHEN...</b>	<b>THEN...</b>
DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), position 3 (UCAF Collection Indicator) has the following value:	<p>DE 48, subelement 43 (Static AAV for Maestro or MasterCard Advance Registration Program) must contain one of the following values:</p> <ul style="list-style-type: none"> <li>• 3 (UCAF data collection supported by merchant, and UCAF [MasterCard Assigned Static AAV Value] data is present)</li> <li>• The static AAV assigned by MasterCard for the MasterCard Advance Registration Program <b>or</b> Maestro Advance Registration Program</li> <li>• The static AAV assigned by MasterCard for Maestro Recurring Payments Program for e-commerce transactions.</li> </ul>
DE 48, subelement 43 (Static AAV for Maestro or MasterCard Advance Registration Program) contains one of the following values:	<p>DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), position 3 (UCAF Collection Indicator) must contain the value 3 (UCAF data collection supported by merchant, and UCAF [MasterCard-assigned Static AAV Value] data is present)</p> <ul style="list-style-type: none"> <li>• The static AAV assigned by MasterCard for the MasterCard Advance Registration Program or Maestro Advance Registration Program</li> <li>• The static AAV assigned by MasterCard for the Maestro Advance Registration Program</li> </ul>

## Program and Service Format Requirements

### Magnetic Stripe Compliance

WHEN...	THEN...
<ul style="list-style-type: none"><li>The static AAV assigned by MasterCard for the Maestro Recurring Payments Program for e-commerce transactions</li></ul>	<p>DE 48, subelement 42, subfield 1, position 3 (UCAF Collection Indicator) has the value 3 (UCAF data collection supported by merchant, and UCAF [MasterCard Assigned Static AAV Value] data is present)</p> <p>For recurring payment e-commerce transactions:</p> <ul style="list-style-type: none"><li>DE 61 (Point-of-Service Data) subfield 4 (POS Cardholder Presence) must contain a value of 4 (Standing order/recurring transactions) and</li><li>DE 61, subfield 10 (Cardholder-Activated Terminal Level) must contain a value of 6 (Authorized Level 6 CAT: Electronic commerce)</li></ul>

## Magnetic Stripe Compliance

The Authorization Platform provides for positive identification of “card-read” transactions and transactions in which software, hardware, or card failures prevent complete and accurate data capture. A “card-read” transaction is one in which the entire unaltered track 1 or track 2 is read and captured by the POS device, then transmitted without truncation in an Authorization Request/0100. As a function of this process, the Authorization Platform performs online edits of track data on MasterCard transactions. If the system finds deficiencies, the findings are forwarded to the issuer and acquirer.

Acquirers and issuers must process transactions according to the guidelines in this subsection to comply with the MasterCard magnetic stripe program.

### Acquirer Requirements

When the entire unaltered magnetic stripe from track 1 or track 2 encoded on the card is present in DE 45 (Track 1 Data) or DE 35 (Track 2 Data), acquirers must provide DE 22 (Point-of-Service [POS] Entry Mode, subfield 1 (POS Terminal PAN Entry Mode), with the value 80, 90, or 91 in the Authorization Request/0100.

Acquirers also must provide the proper customer ID that MasterCard assigned directly to the entity acting on the acquiring institution's behalf in DE 32 (Acquiring Institution ID Code). However, if the Authorization Request/0100 is routed to the MasterCard Worldwide Network via a customer processor system (CPS) or intermediate network facility (INF), the proper customer ID that MasterCard assigned directly to the processor entity must be provided in DE 33 (Forwarding Institution ID Code).

The Authorization Platform provides track data validation and point of interaction validation. If the track data, DE 61 (Point-of-Service [POS] Data), or TCC in DE 48 (Additional Data—Private Use) contains an edit error, the Authorization Platform will provide DE 48, subelement 89 (Magnetic Stripe Compliance Error Indicator) in the Authorization Request/0100 and Authorization Request Response/0110 messages.

If a valid acquirer customer ID is not provided in DE 32, the Authorization Platform:

- Changes the value in DE 22, subfield 01 from 80, 90, or 91 to 02.
- Provides DE 48, subelement 88, with a value of Y.

When applicable, this information is provided in the Authorization Request/0100 message sent to the issuer and the Authorization Request Response/0110 message sent to the acquirer to indicate this condition.

### **Issuer Requirements**

Issuers must encode the CVC 1 value on both track 1 and track 2. In addition, issuers must indent print the CVC 2 value into the signature panel after the account number.

Issuers can receive DE 22, subfield 1, value 02 if:

- An acquirer does not comply; therefore, MasterCard changed the 80, 90, or 91 to 02.
- An acquirer did not submit a 80, 90, or 91 but rather a 02. Issuers must be able to process a 80, 90, or 91 in DE 22 and optionally process error codes in DE 48.

Issuers may indicate a CVC 1 error by providing a Y in DE 48, subelement 87.

Use the Authorization Request/0100 for transmitting magnetic stripe-read transactions. (Refer to the *Security Rules and Procedures* manual for subelement information for DE 45 (Track 1 Data) and DE 35 (Track 2 Data))

## **Authorization Request/0100—Magnetic Stripe-read**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

## **Program and Service Format Requirements**

### **MasterCard Hosted Mobile Phone Top-up ATM Transactions**

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	Must be one of the following values: 80 = Chip card at chip-capable terminal was unable to process transaction using data on the chip 90 = PAN auto-entry via magnetic stripe 91 = PAN auto-entry via contactless magnetic stripe
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	Contains a valid transaction category code.
DE 48, subelement 88 (Magnetic Stripe Compliance Status Indicator)	•	X	C	Y = Authorization Platform replaced DE 22 value 90 or 91 with value 02.
DE 48, subelement 89 (Magnetic Stripe Compliance Error Indicator)	•	X	C	Authorization Platform provides this subelement, when applicable. Indicates Track data, POS data, or TCC errors.

### **Authorization Request Response/0110—Magnetic Stripe-read**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	CE	•	CE	Must contain the same value as in the Authorization Request/0100.
DE 48, subelement 87 (Card Validation Code Result)	C	•	C	Issuer provides this subelement, when applicable.
DE 48, subelement 88 (Magnetic Stripe Compliance Status Indicator)	CE	•	CE	Must contain the same value as in the Authorization Request/0100.
DE 48, subelement 89 (Magnetic Stripe Compliance Error Indicator)	CE	•	CE	Must contain the same value as in the Authorization Request/0100.

## **MasterCard Hosted Mobile Phone Top-up ATM Transactions**

MasterCard Hosted Mobile Phone Top-up supports Maestro®, Debit MasterCard®, and MasterCard® card transactions performed via ATMs in the Europe region. Mobile phone top-up functionality enables customers to top-up (that is, add credit to) their prepaid mobile phone service. Mobile Phone Top-up enables acquirers to provide cardholders the ability to “pay as you go” at the ATM for additional mobile phone minutes.

## **Authorization Request/0100—MasterCard Hosted Mobile Phone Top-up**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	00 = Purchase
DE 4 (Amount, Transaction)	M	•	M	The top-up amount
DE 12 (Time, Local Transaction)	C	•	C	The local time at which the transaction takes place at the point of card acceptor location
DE 13 (Date, Local Transaction)	C	•	C	The local month and day on which the transaction takes place at the point of card acceptor location.
DE 18 (Merchant Type)	M	•	M	Card acceptor business code (MCC) 4814 (Telecommunication Services including but not limited to prepaid phone services and recurring phone services)
DE 43 (Card Acceptor Name/Location for ATM Transactions)	C	•	C	
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	Z = ATM Cash Disbursement
DE 48, subelement 13 (MasterCard Hosted Mobile Phone Top-up Request Data)	C	•	C	Subfield 1 = Mobile Phone Number (Must be left-justified and cannot contain all spaces or all zeros.) Subfield 2 = Mobile Phone Service Provider Name (Must be left-justified and cannot contain all spaces or all zeros.)
DE 52 (Personal ID Number [PIN] Data)	M	X	M	DE 52 is mandatory for all ATM transactions.
DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level)	C	•	C	1 = (Authorized Level 1 CAT: Automated dispensing machine with PIN)

### **NOTE**

**Alternate processing is not applicable for MasterCard Hosted Mobile Phone Top-up transactions. If the primary issuer is not available or does not provide a timely response, the Authorization Platform will send the acquirer an Authorization Request Response/0110 message with DE 39, value 91 (Authorization Platform or issuer system inoperative).**

## **Program and Service Format Requirements**

### **MasterCard Hosted Mobile Phone Top-up ATM Transactions**

---

## **Authorization Platform Edits**

The following edits are performed on Authorization Request/0100 messages for MasterCard Hosted Mobile Phone Top-up transactions.

### **Authorization Request/0100 Edits**

<b>WHEN the message contains...</b>	<b>THEN the Authorization Platform...</b>
DE 48, subelement 13 and One of the following data elements is not present: <ul style="list-style-type: none"><li>• DE 12</li><li>• DE 13</li><li>• DE 43</li></ul>	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 (Response Code) = 30 (Format error) DE 44 (Additional Response Data) = the data element in error
DE 48, subelement 13 is incorrectly formatted (for example, incorrect length, subfield 1 or 2 is not present, or subfield 1 or 2 contains all zeros or spaces)	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 30 DE 44 = 048

### **Authorization Request Response/0110 Edits**

<b>WHEN....</b>	<b>THEN the Authorization Platform...</b>
The value in DE 48, subelement 13 is different from the original Authorization Request/0100 message	Sends the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 048

### **Authorization Advice/0120—Acquirer-generated Edits**

<b>WHEN the message contains...</b>	<b>THEN the Authorization Platform...</b>
DE 48, subelement 13	Declines the request with an Authorization Advice Response/0130 message where: DE 39 = 30 DE 44 = 048

**Reversal Request/0400 Edits**

<b>WHEN the message contains...</b>	<b>THEN the Authorization Platform...</b>
DE 3, subfield 1 (Transaction Type Code) is 00 (Purchase) and DE 48 position 1 (TCC) is Z and DE 48, subelement 13 (MasterCard Hosted Mobile Phone Top-up Request Data) is present	Declines the request with a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 003

**MasterCard inControl Service**

The MasterCard inControl® platform provides for a number of advanced authorization, transaction routing, and alert controls designed to assist issuers in creating new and enhanced payment products.

**Features**

The MasterCard inControl platform allows issuers to leverage “off-the-shelf” solutions and to create customized offerings depending on the needs of their customers.

Among the advanced new features issuers can leverage to support their commercial card portfolios are:

- Enhanced authorization controls that direct how, when, and where cards may be used to a greater level of specificity than previously supported
- Robust alert functionality that provides personalized real-time communication about transaction activities
- A limited use number feature that allows authorization, spending limits, and usability controls to be set on a transaction-by-transaction basis, providing enhanced levels of security, control, data capture, and traceability on every purchase

**Authorization Request/0100—inControl Purchase Control**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply. This layout applies to participating issuers only.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 2 (Primary Account Number)	M	•	M	Contains the cardholder's real account number
DE 14 (Date, Expiration)	C	•	C	The cardholder's real account number expiration date

## Program and Service Format Requirements

### MasterCard inControl Service

Data Element	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data—Private Use), subelement 33, (PAN Mapping File Information), subfield 1 (Account Number Indicator)	•	X	C	Indicates MasterCard inControl™ virtual card number V = Virtual Card Number
DE 48, subelement 33, subfield 2 (Account Number)	•	X	C	Virtual card number
DE 48, subelement 33, subfield 3 (Expiration Date)	•	X	C	VCN Expiration date
DE 48, subelement 71 (On-Behalf Services), subfield 1 (On-Behalf [OB] Service)	•	X	C	17 = inControl Virtual Card Service
DE 48, subelement 71 (On-Behalf Services), subfield 2 (On-Behalf [OB] Result 1)	•	X	C	V = Valid Note: If the Purchase Control service is unsuccessful, refer to <a href="#">Subfield 2—On-behalf Result 1</a> for a list of other valid values.

## Dual Message System Processing

This message describes Dual Message System processing of a MasterCard inControl Purchase Control transaction.

1. The acquirer sends an Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or a Reversal Request/0400 message to the MasterCard Worldwide Network containing the inControl virtual card number in DE 2 (Primary Account Number [PAN]).
2. The Authorization Platform applies unique controls for the inControl virtual card number and performs mapping to the cardholder's primary account number.
3. The Authorization Platform sends an Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or a Reversal Request/0400 message to the issuer containing:
  - DE 2 (Primary Account Number [PAN]) and DE 14 (Date, Expiration) with the cardholder's real account number and associated expiration date.
  - DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information) where subfield 1 (Account Number Indicator) = value V (Virtual Card Number), subfield 2 (Account Number) = VCN (Virtual card number), and subfield 3 (Expiration Date) = VCN expiration date
  - DE 48, subelement 71 (On-Behalf Services) where subfield 1 (On-Behalf Services) = value 17 (inControl Virtual Card Service), subfield 2 (On-Behalf [OB] Result 1)—value V (Valid)
4. The issuer approves or declines the authorization request by sending an Authorization Request Response/0110, Authorization Advice

Response/0130—Issuer-generated, or a Reversal Request Response/0410 message.

5. The Authorization Platform maps the cardholder's primary account number back to the inControl virtual card number, places it in DE 2 (Primary Account number [PAN]), and then forwards the Authorization Request Response/0110, Authorization Advice Response/0130, and Reversal Request Response/0410 messages to the acquirer.
6. The acquirer forwards the virtual card number and the authorization response information to the merchant.
7. If inControl processing cannot be completed, the Authorization Platform sends the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 containing DE 39 (Response Code), value 96 (System error).

## **MasterCard inControl Real Card Spend Control**

The MasterCard inControl Real Card Spend Control service provides cardholders the ability to establish spend control rules for their pre-existing payment cards that are enforced during the authorization process.

These rules can be defined for both card-present and card-not-present transaction environments, and depending on the cardholder's pre-defined response rules, may result in an alert notification being generated to the cardholder or the transaction being declined on their behalf.

### **NOTE**

**Spend control rules can only be applied to transactions that flow through the MasterCard Worldwide Network. Spend control rules are not applied to Authorization Advice/0120—Acquirer-generated and Reversal Request/0400 messages.**

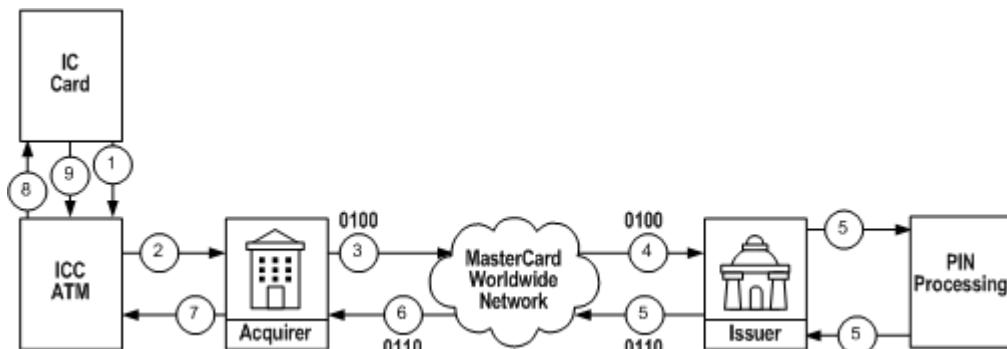
## **Process of a MasterCard inControl Service Eligible Transaction**

This message flow describes the stages of the Dual Message System processing for a MasterCard inControl Service-eligible transaction.

The acquirer sends the Authorization Request/0100 message containing the MasterCard inControl real card number in DE 2 (Primary Account Number [PAN]) to the MasterCard Worldwide Network.

<b>WHEN...</b>	<b>THEN inControl...</b>
The transaction complies with the control rules established by the cardholder	Sends the issuer the Authorization Request/0100 message where DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 1 (On-behalf [OB] Service) contains value 20 (inControl—RCN Spend Control) and subfield 2 (On-behalf [OB] Result 1) contains value V (Valid).
The transaction does not comply with the control rules established by the cardholder and The cardholder has registered an action response of “decline and alert notification” upon rule failure	Declines the transaction and sends the acquirer an Authorization Request Response/0110 message where DE 39 (Response Code) contains a decline response. and Sends the issuer an Authorization Advice/0120—System-generated message where: <ul style="list-style-type: none"><li>• DE 48, subelement 71:<ul style="list-style-type: none"><li>– Subfield 1 contains value 20</li><li>– Subfield 2 contains the spend control rule that failed</li></ul></li></ul>

WHEN...	THEN inControl...
The transaction does not comply with the spend control rules established by the cardholder and The cardholder has registered an action response of “alert notification only” upon rule failure, but no decline action	<ul style="list-style-type: none"> <li>• DE 60 (Advice Reason Code): <ul style="list-style-type: none"> <li>– Subfield 1 (Advice Reason Code) contains value 200 (inControl Processing Advice to Issuer)</li> <li>– Subfield 2 (Advice Detail Code) contains a valid advice reason code</li> </ul> </li> </ul> <p>and</p> <p>Sends the cardholder an alert notification indicating rule failure.</p>
	<p>Sends the issuer an Authorization Request/0100 message where DE 48, subelement 71, subfield 1 is value 20 and subfield 2 indicates the spend control rule that failed.</p> <p>and</p> <p>Sends the cardholder an alert notification indicating rule failure.</p>



If the transaction is declined (by the issuer, alternate issuer, Stand-In processing, or X-Code processing), or the issuer/alternate issuer performs a partial approval or purchase amount only approval, then the Authorization Platform sends an Authorization Advice/0120—System-generated message to MasterCard inControl to update the disposition of the transaction.

WHEN...	THEN the Authorization Platform...
MasterCard inControl is unavailable or responds late or The spend control rules have recently been removed	Populates DE 48, subelement 71 with subfield 1, value 20 and subfield 2, value U (Unable to process) and forwards the transaction to issuer.

**Program and Service Format Requirements**  
**MasterCard inControl Real Card Spend Control**

---

## **Authorization Request/0100—inControl Real Card Spend Control**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 2 (Primary Account Number)	M	•	M	Account range must participate in inControl Real Card Spend Control Service DE 2 contains the MasterCard inControl real card number
DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 1 (On-behalf [OB] Service)	•	X	C	20 = inControl RCN Spend Control Service
DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 2 (On-behalf [OB] Result 1)	•	X	C	Indicates the results of the service processing. Valid subfield 2 values: D, E, F, G, H, J, K, L, M, P, U, or V

## **Authorization Advice/0120—inControl Real Card Spend Control**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Advice/0120 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 2 (Primary Account Number)	•	M	M	Account range must participate in inControl Real Card Spend Control Service
DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 1 (On-behalf [OB] Service)	•	M	M	20 = inControl RCN Spend Control Service
DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 2 (On-behalf [OB] Result 1)	•	M	M	Indicates the results of the service processing. Valid subfield 2 values: D, E, F, G, H, J, K, L, M, P, U, or V
DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code)	•	M	M	200 = inControl Processing Advice to Issuer

**Program and Service Format Requirements**  
**MasterCard inControl Virtual Card Mapping and Spend Control Service**

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code)	•	M	M	Reject reason
DE 121 (Authorizing Agent ID Code)	•	C	C	000003 = Applicable only to issuers participating in the inControl services and will only be present in Authorization Advice/0120—System-generated messages notifying issuers of a declined request due to a failed spend control rule defined by the cardholder

## **MasterCard inControl Virtual Card Mapping and Spend Control Service**

The MasterCard inControl platform leverages the same authorization and clearing data elements for mapping virtual card numbers to their real card account numbers as in the MasterCard inControl Purchase Control service and the MasterCard *PayPass* Mapping service. Issuers currently supporting the MasterCard *PayPass* Mapping service need only to recognize new data values in existing data elements to support the MasterCard inControl Virtual Card Mapping and Spend Control service.

### **Authorization Request/0100—inControl Virtual Card Mapping and Spend Control Service**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 2 (Primary Account Number [PAN])	M	•	M	The real card number
DE 48 (Additional Data—Private Use), Subelement 33 (PAN Mapping File Information)	•	X	C	The virtual account data
DE 48, Subelement 71	•	X	C	The on-behalf service performed on the transaction

### **Exception Processing**

This message flow describes the Dual Message System processing for an inControl Virtual Card Mapping and Spend Control service authorization transaction that was declined by inControl processing.

## **Program and Service Format Requirements**

### **MasterCard *MoneySend***

---

1. The acquirer sends an Authorization Request/0100 message to the MasterCard Worldwide Network containing the inControl virtual card number in DE 2 (Primary Account Number [PAN]).
2. The Authorization Platform applies unique controls for the inControl virtual card number and performs mapping to the cardholder's primary account number.
3. If the transaction fails mapping, the Authorization Platform declines the request and sends the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130—System-generated, or a Reversal Request Response/0410 message.  
If the transaction fails spend controls, the Authorization Platform declines the request and sends the acquirer an Authorization Request Response/0110 message.
4. If the transaction fails spend controls but PAN mapping is successful, the Authorization Platform sends an Authorization Advice/0120—System-generated message to the issuer containing:
  - DE 2 (Primary Account Number [PAN])
  - DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information)
  - DE 48, subelement 71 (On-Behalf Services), subfield 1 (On-Behalf Services) value 17 (inControl Virtual Card Service) and subfield 2 (On-Behalf [OB] Result 1) containing the appropriate result value
  - DE 60 (Advice Reason code), subfield 1 (Advice Reason Code) = 200 (inControl Processing Advice to Issuer), subfield 2 (Advice Detail Code) = appropriate advice reason code

## **MasterCard *MoneySend***

The MasterCard *MoneySend* service enables person-to-person money transfers by allowing consumers to use their MasterCard®, Debit MasterCard®, MasterCard Electronic™, Cirrus®, or Maestro® card to send and access funds. The *MoneySend* service also allows use of multiple channels to initiate transactions such as an ATM, a bank branch, a stand-alone kiosk, mobile, or over the Internet.

Financial institutions offering the MasterCard *MoneySend* service may need to engage in two transactions to accommodate the funds transfer between the sender and the recipient:

- The first transaction, referred to as the “Funding Transaction,” moves funds within an originating financial institution (“On-Us”) to work within the MasterCard acquirer/issuer construct. The originating financial institution (OFI) is both the acquirer and issuer of a *MoneySend* transaction for the sender to enable the movement of money via the MasterCard Worldwide Network. The Funding Transaction is optional because the OFI may have

the ability to perform this function internally (for example, if the funding mechanism is a demand deposit account [DDA] instead of a card).

- The second transaction, referred to as the “Payment Transaction,” moves funds from the OFI, via the MasterCard Network, to the recipient of the funds and into a MasterCard, Debit MasterCard, Maestro, or Cirrus account (the “Receiving Account”) at the receiving financial institution (RFI).

For participation requirements or for more information about this optional service, refer to the *MasterCard MoneySend Global Platform Guide*.

### **MasterCard MoneySend Funding Transactions**

MasterCard *MoneySend* Funding Transactions are identified in Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, Reversal Request/0400 messages by the following values:

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 00 (Purchase Transaction)
- DE 18 (Merchant Type), MCC 6538 (MasterCard *MoneySend* Funding Transaction) to identify a *MoneySend* Funding Transaction
- DE 48 (Additional Data—Private Use), transaction category code (TCC), value R (Face-to-face retail) or T (Non-face-to-face retail)
- 

OFIs may optionally send DE 124 (Member-defined Data) when submitting a *MoneySend* Funding Transaction.

MasterCard requires originating financial institution (OFI) participation when submitting a *MoneySend* Funding Transaction.

### **MasterCard MoneySend Payment Transactions**

The *MoneySend* Payment Transaction provides a unique message to facilitate remittances between two parties: a sender using the services of a financial institution acting on the sender's behalf, referred to as the originating financial institution (OFI)—the Payment Transaction acquirer—and the recipient who receives the funds when they are deposited into his or her MasterCard or Maestro account at another financial institution, referred to as the receiving financial institution (RFI)—the recipient's card issuer.

The *MoneySend* service provides consumers with a fast, secure, and convenient way to transfer money domestically and internationally. The service operates on the basis of account-to-account processing, which enables funds to be transferred from any approved account held at an originating financial institution to any MasterCard or Maestro account held at a receiving financial institution. Customers can use *MoneySend* transactions only through the channels offered by their financial institutions.

OFIs must be registered with MasterCard to participate in the *MoneySend* service.

## **Program and Service Format Requirements**

### **MasterCard *MoneySend***

---

OFIs must use DE 48 (Additional Data - Private Use), subelement 77 (Payment Transaction Type Indicator), value C07 (MasterCard *MoneySend*) and the following unique MasterCard *MoneySend* card acceptor business codes to identify MasterCard *MoneySend* transactions from other types of Payment Transactions:

- MCC 6536 (MasterCard *MoneySend* Intracountry)
- MCC 6537 (MasterCard *MoneySend* Intercountry)

The OFI and RFI countries determine which card acceptor business code (MCC) is used.

The maximum amount allowed for each MasterCard *MoneySend* transaction is the maximum amount allowed for the OFI region or country. The Authorization Platform will validate the Authorization Request/0100 message against the MasterCard *MoneySend* maximum transaction amount limit (USD 2500). Currency conversion on the MasterCard *MoneySend* transaction will be completed before comparing it to the maximum transaction amount limit.

The Authorization Platform will use the value provided in DE 4 (Amount, Transaction) by the OFI when performing currency conversion to derive the value for DE 5 (Amount, Settlement Amount).

The Authorization Platform converts DE 4 (Amount, Transaction) to USD (if necessary) and compares it to the maximum transaction amount limit for the OFI region or country. If the value in DE 5 is greater than the maximum transaction amount limit, the Authorization Platform will send the OFI an Authorization Request Response/0110 message containing DE 39 (Response Code), value 13 (Invalid Amount).

The Authorization Platform will reject an Authorization Request/0100 or a Reversal Request/0400 message that does not meet the edits for a properly formatted MasterCard *MoneySend* transaction.

## **Authorization Request/0100—MasterCard *MoneySend* Funding Transactions**

Originating Financial Institutions (OFI) that are registered for the MasterCard *MoneySend* service will be required to send an Authorization Request/0100 and Reversal Request/0400 message with the required data elements in addition to the data elements that are specific to this service.

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	00 = Funding Transaction
DE 18 (Merchant Type)	M	•	M	MCC 6538 (MasterCard <i>MoneySend</i> Funding Transaction)
DE 48 (Additional Data—Private Use), TCC	M	•	M	R = Face-to-face retail or T = Non-face-to-face retail
DE 124 (MasterCard <i>MoneySend</i> , Sender Identification Data)	O	X	C	<p>Acquirers may optionally send DE 124, subfields 1–4 containing sender identification data when the Authorization Request/0100 message is a MasterCard <i>MoneySend</i> Funding Transaction.</p> <p>In DE 124 of the response message, issuers must echo—<b>unedited</b>—the information sent by the originator/acquirer.</p> <p>DE 124 should not be used for any other purpose if the transaction is a MasterCard <i>MoneySend</i> transaction.</p>

## Reversal Request/0400—MasterCard *MoneySend* Funding Transaction

Following is a list of the data elements and values applicable to this message type. All mandatory Reversal Request/0400 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	00 = Funding Transaction
DE 18 (Merchant Type)	M	•	M	MCC 6538 (MasterCard <i>MoneySend</i> Funding Transaction)
DE 48 (Additional Data—Private Use), TCC	M	•	M	R = Face-to-face retail or T = Non-face-to-face retail
DE 124 (MasterCard <i>MoneySend</i> , Sender Identification Data)	O	X	C	<p>Acquirers may optionally send DE 124, subfields 1–4 containing sender identification data when the Authorization Request/0100 message is a MasterCard <i>MoneySend</i> Funding Transaction.</p> <p>In DE 124 of the response message, issuers must echo—<b>unedited</b>—the information sent by the originator/acquirer.</p>

## Program and Service Format Requirements

### MasterCard *MoneySend*

---

## Authorization Platform Edits

The Authorization Platform will perform the following edits on the Authorization Request/0100 and Reversal Request/0400 messages for *MoneySend* Funding Transactions.

WHEN...	THEN the Authorization Platform will...
DE 3 (Processing Code), value 00 (Purchase Transaction) is present And DE 18 (Merchant Type), value 6538 (MasterCard <i>MoneySend</i> Funding Transaction) is present And The OFI identified by the ICA provided in DE 32 (Acquiring Institution ID Code) has not registered to process transactions via the MasterCard <i>MoneySend</i> platform	Reject the transaction and send the OFI an Authorization Request Response/0110 or Reversal Request Response/0410 message containing DE 39 (Response Code), value 58 (Transaction not permitted to acquirer/terminal).

## Authorization Request/0100—MasterCard *MoneySend* Payment Transactions

Originating Financial Institutions (OFI) that are registered for the MasterCard *MoneySend* service will be required to send an Authorization Request/0100 and Reversal Request/0400 message with the required data elements in addition to the data elements that are specific to this service.

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	28 = Payment Transaction
DE 18 (Merchant Type)	M	•	M	Must be one of the following values: MCC 6536 (MasterCard <i>MoneySend</i> Intracountry) MCC 6537 (MasterCard <i>MoneySend</i> Intercountry)
DE 48 (Additional Data—Private Use), TCC	M	•	M	P = Payment Transaction
DE 48, subelement 77, (Payment Transaction Type Indicator)	C	•	C	C07 = MasterCard <i>MoneySend</i>

Data Element	Org	Sys	Dst	Values/Comments			
DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level)	M	•	M	The Authorization Platform validates the POI to ensure DE 61, subfield 10 is one of the following values:  <b>IF...</b> <b>THEN...</b>  At a bank branch 0 = Not a CAT transaction  At an ATM 1 = Authorized Level 1 CAT: Automated dispensing machine with PIN  At an unmanned kiosk 2 = Authorized Level 2 CAT: Self-service terminal kiosk  On the Internet 6 = Authorized Level 6 CAT: Electronic commerce			
DE 124 (MasterCard <i>MoneySend</i> , Sender Identification Data)	M	•	M	Acquirers must send DE 124, subfields 1-4 containing sender identification data when the Authorization Request/0100 message is a MasterCard <i>MoneySend</i> Payment Transaction. In DE 124 of the response message, issuers must echo— <b>unedited</b> —the information sent by the originator/acquirer. DE 124 should not be used for any other purpose if the transaction is a MasterCard <i>MoneySend</i> transaction.			

## Reversal Request/0400—MasterCard *MoneySend* Payment Transaction

Following is a list of the data elements and values applicable to this message type. All mandatory Reversal Request/0400 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	28 = Payment Transaction
DE 18 (Merchant Type)	M	•	M	Must be one of the following values: MCC 6536 (MasterCard <i>MoneySend</i> Intracountry) MCC 6537 (MasterCard <i>MoneySend</i> Intercountry)
DE 48 (Additional Data—Private Use), TCC	M	•	M	P = Payment Transaction

## Program and Service Format Requirements

### MasterCard *MoneySend*

Data Element	Org	Sys	Dst	Values/Comments										
DE 48, subelement 77, (Payment Transaction Type Indicator)	C	•	C	C07 = MasterCard <i>MoneySend</i>										
DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level)	M	•	M	The Authorization Platform will validate the POI to ensure DE 61, subfield 10 is one of the following values:  <table border="1"> <thead> <tr> <th>IF...</th> <th>THEN...</th> </tr> </thead> <tbody> <tr> <td>At a bank branch</td> <td>0 = Not a CAT transaction</td> </tr> <tr> <td>At an ATM</td> <td>1 = Authorized Level 1 CAT: Automated dispensing machine with PIN</td> </tr> <tr> <td>At an unmanned kiosk</td> <td>2 = Authorized Level 2 CAT: Self-service terminal</td> </tr> <tr> <td>On the Internet</td> <td>6 = Authorized Level 6 CAT: Electronic commerce</td> </tr> </tbody> </table>	IF...	THEN...	At a bank branch	0 = Not a CAT transaction	At an ATM	1 = Authorized Level 1 CAT: Automated dispensing machine with PIN	At an unmanned kiosk	2 = Authorized Level 2 CAT: Self-service terminal	On the Internet	6 = Authorized Level 6 CAT: Electronic commerce
IF...	THEN...													
At a bank branch	0 = Not a CAT transaction													
At an ATM	1 = Authorized Level 1 CAT: Automated dispensing machine with PIN													
At an unmanned kiosk	2 = Authorized Level 2 CAT: Self-service terminal													
On the Internet	6 = Authorized Level 6 CAT: Electronic commerce													
DE 124 (MasterCard <i>MoneySend</i> , Sender Identification Data)	M	•	M	Acquirers must send DE 124, subfields 1-4 containing sender identification data when the Authorization Request/0100 message is a MasterCard <i>MoneySend</i> payment transaction.  In DE 124 of the response message, issuers must echo— <b>unedited</b> —the information sent by the originator/acquirer.										

## Authorization Platform Edits

The Authorization Platform will perform the following edits on the Authorization Request/0100 and Reversal Request/0400 messages for *MoneySend* Payment Transactions.

WHEN...	THEN the Authorization Platform...
When an OFI identified by the ICA number provided in DE 32 (Acquiring Institution ID Code) attempts to submit a MasterCard <i>MoneySend</i> Payment Transaction but has not registered for the MasterCard <i>MoneySend</i> service	Rejects the transactions and sends the OFI an Authorization Request Response/0110 or Reversal Request Response/0410 message containing DE 39 (Response Code), value 58 (Transaction not permitted to acquirer/terminal).
The OFI is registered for the MasterCard <i>MoneySend</i> service and is submitting a <i>MoneySend</i> Payment Transaction where:	<ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 is not MCC 6536 or MCC 6537</li> </ul> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> </ul>

WHEN...	THEN the Authorization Platform...
<ul style="list-style-type: none"> <li>• DE 48, subelement 77 contains value C07</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 is present</li> </ul>	<ul style="list-style-type: none"> <li>• DE 44 = 018 (Merchant Type)</li> </ul>
<p>The OFI is registered for the MasterCard <i>MoneySend</i> service and is submitting a <i>MoneySend</i> Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains value MCC 6536 or MCC 6537</li> <li>• DE 48, subelement 77 contains value C07</li> <li>• DE 61, subfield 10 criteria is not met</li> <li>• DE 124 is present</li> </ul>	<p>Sends the OFI an Authorization Request Response/0110 or Reversal Request Response/0410 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 061 (Point-of-Service [POS] Data)</li> </ul>
<p>The OFI is registered for the MasterCard <i>MoneySend</i> service and is submitting a <i>MoneySend</i> Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC 6536 or MCC 6537</li> <li>• DE 48, subelement 77 contains value C07</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 is not present</li> </ul>	<p>Sends the OFI an Authorization Request Response/0110 or Reversal Request Response/0410 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 124 (Merchant-defined Data)</li> </ul>
<ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 48, subelement 77 contains value C07</li> <li>• DE 124, subfield 2 or subfield 3 is not present or contains all zeros or spaces</li> </ul>	<p>Sends the OFI an Authorization Request Response/0110 or Reversal Request Response/0410 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 124 (Merchant-defined Data)</li> </ul>
DE 3, subfield 1 contains value 28 and DE 61, subfield 10 contains value 1 and DE 52 and DE 55 are <b>not</b> present	Forwards the Authorization Request/0100 message to the issuer.
An acquiring country is not supported by the MasterCard <i>MoneySend</i> platform	Declines the request and sends the OFI an Authorization Request Response/0110 message where DE 39 = 58 (Transaction not permitted to acquirer/terminal)

## Program and Service Format Requirements

### Merchant Advice Codes

WHEN...	THEN the Authorization Platform...
An issuing country, RFI, or RFI's account range is not able to offer the MasterCard <i>MoneySend</i> service	Declines the request and sends the OFI an Authorization Request Response/0110 message where DE 39 = 57 (Transaction not permitted to issuer/cardholder)
Note: MasterCard Electronic consumer e-commerce <i>MoneySend</i> Payment Transactions do not require UCAF data (DE 48, subelement 43).	

## Merchant Advice Codes

MasterCard supports the use of Merchant Advice codes for issuers to communicate clearly with merchants.

- The reason for approving or declining a transaction
- The actions merchants can take to continue to serve their customers

Issuers can use Merchant Advice codes to provide specific direction to acquirers.

### Merchant Advice Codes Used with Response Codes

Issuers can use the Merchant Advice Codes in conjunction or association with Response Codes to indicate to merchants how to respond to various transaction scenarios.

#### DE 48, Subelement 84 (Merchant Advice Codes)

Issuers can use the following values to indicate Merchant Advice codes in Authorization Request Response/0110 messages, DE 48, subelement 84:

Value	Description
01	New Account Information Available
02	Try Again Later
03	Do Not Try Again
21	Recurring Payment Cancellation Service

#### Authorization Request Response/0110, DE 39 Response Codes

The following table lists the most common DE 39 values that issuers send in conjunction with Merchant Advice codes in DE 48, subelement 84.

Value	Description
00	Approved
05	Do not honor

Value	Description
14	Invalid card number
51	Insufficient funds/over credit limit
54	Expired card

### Examples of Combined DE 48, Subelement 84 and DE 39 Values

The following table provides examples of how issuers and acquirers should use the combination of DE 48, subelement 84, and DE 39.

DE 39	DE 48, subelement 84	Merchant Advice Description	Examples of Reason for Decline	Suggested Merchant Action
00	01	New account information available	<ul style="list-style-type: none"> <li>• Expired card</li> <li>• Account upgrade</li> <li>• Portfolio sale</li> <li>• Conversion</li> </ul>	Obtain new account information before next billing cycle
05				
14				
51				
54				
51	02	Try again later	<ul style="list-style-type: none"> <li>• Over credit limit</li> <li>• Insufficient funds</li> </ul>	Recycle transaction 72 hours later
05				
14				
51				
54				
05	03	Do not try again	<ul style="list-style-type: none"> <li>• Account closed</li> <li>• Fraudulent</li> </ul>	Obtain another type of payment from customer
14				
51				
54				
05	21	Recurring Payment Cancellation Service	Cardholder cancelled recurring agreement	Do not resubmit transaction

## M/Chip Processing Services

MasterCard provides M/Chip Processing services to assist issuers that choose to migrate to MasterCard M/Chip technology while minimizing changes to their host systems. The Stand-In System provides chip security features for customers currently using M/Chip technology. The security features provide additional verification for chip transactions when the issuer's host is unavailable.

The MasterCard M/Chip Processing services include:

- Chip to Magnetic Stripe Conversion
- M/Chip Cryptogram Pre-validation
- M/Chip Cryptogram Validation in Stand-In processing
- Combined Service Option

## **Program and Service Format Requirements**

### **M/Chip Processing Services**

---

Please refer to the *Authorization Manual* for M/Chip Processing service programs and service information.

The MasterCard M/Chip Processing services support issuers using M/Chip technology in their authorization processing by performing all, or part of the M/Chip-related authorization processing on-behalf of the issuer in a designated account range.

The Chip to Magnetic Stripe Conversion and the M/Chip Cryptogram Pre-validation services are provided on a permanent basis. The M/Chip Cryptogram Validation in Stand-In processing service is provided on a dynamic basis if and when the issuer is not able to respond to an authorization request.

MasterCard provides the following DE 48 (Additional Data–Private Use) subelements that support M/Chip Processing services:

- Subelement 71 (On-behalf Services)
- Subelement 72 (Issuer Chip Authentication Data)
- Subelement 79 (Chip CVR/TVR Bit Error Results)

## **Program use of M/Chip Processing Service Data Elements**

The following table defines the M/Chip Processing Services use of DE 48, subelement 71, subelement 72, subelement 74, and subelement 79.

<b>DE 48 Subelement:</b>	<b>Description</b>
Subelement 71 (On-behalf Services)	<p>Subelement 71 notifies the issuer of the M/Chip Processing service performed on the transaction. Transactions that meet the criteria for the service contain subelement 71 data in DE 48 of the Authorization Request/0100 to notify the issuer of the service performed and the results.</p> <p>Issuers must return subelement 71 in the Authorization Request Response/0110 message when subelement 71 is present in the Authorization Request/0100 message.</p> <p>The acquiring MIP removes subelement 71 before sending the Authorization Request Response/0110 message to the acquirer host.</p>
Subelement 72 (Issuer Chip Authentication)	<p>MasterCard uses subelement 72 to carry data used during cryptogram processing.</p> <p>Issuers subscribing to the M/Chip Cryptogram Pre-validation service will have subelement 72 in the Authorization Request/0100 message when the ARQC is valid as determined by MasterCard.</p> <p>Issuers that use the M/Chip Cryptogram Validation in Stand-In processing service or the M/Chip Cryptogram Pre-validation service will have subelement 72 in the Authorization Advice/0120</p>

DE 48 Subelement:	Description
	message. In this situation, subelement 72 contains the ARPC (Authorization Response Cryptogram) present in DE 55, subelement ID 91 (Issuer Authentication Data) in the Authorization Request Response/0110 based on the approval or decline decision.
	The Authorization Platform returns subelement 72 in the Authorization Request Response/0110 message when subelement 72 is present in the Authorization Request/0100 message.
	The acquiring MIP removes subelement 72 before sending the Authorization Request Response/0110 message to the acquirer host.
Subelement 74 (Additional Processing Information)	For M/Chip Processing services, subelement 74 notifies the acquirer that there was an issue with the cryptogram validation.
	MasterCard provides the acquirer an Authorization Request Response/0110 message containing subelement 74 when there is an issue with cryptogram validation during M/Chip Processing service processing.
	Issuers may provide the acquirer an Authorization Request Response/0110 message containing subelement 74 when there is an issue with cryptogram validation when they perform their own validation.
Subelement 79 (Chip CVR/TVR Bit Error Results)	Issuers that participate in the M/Chip Cryptogram Pre-validation Service or the M/Chip Cryptogram Validation in Stand-In Processing Service receive subelement 79 in the Authorization Request/0100 and the Authorization Advice/0120—System-generated when errors are detected in the CVR/TVR within the Issuer Application data during M/Chip Cryptogram Validation processing. Subelement 79 is present when subelement 71, subfield 2 (OB Result 1) contains the value T (TVR/CVR was invalid). Subelement 79 should not be returned in the Authorization Request Response/0110.

## Chip To Magnetic Stripe Conversion

The Chip to Magnetic Stripe Conversion service is an optional service that removes M/Chip-related data element (DE) 55 (Integrated Circuit Card [ICC] System-related Data), if present and DE 23 (Card Sequence Number), if present and changes the value in DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) before sending the Authorization Request/0100 message to the issuer for processing.

## **Program and Service Format Requirements**

### **M/Chip Processing Services**

---

Chip to Magnetic Stripe Conversion affects issuers only. Acquirers are not affected by this service. Issuers subscribing to the Chip to Magnetic Stripe Conversion service must ensure that the cards are not personalized to expect Issuer Authentication Data in DE 55 in the Authorization Request Response/0110 message.

Authorization Advice/0120 messages contain the converted magnetic stripe transaction and include DE 48, subelement 71.

Issuers should be aware that the acquirer submits the original M/Chip transaction into clearing.

The Global Clearing Management System (GCMS) offers the Chip to Magnetic Stripe Conversion service. Issuers should refer to the *GCMS Reference Manual* for information about this optional service.

To request this service, issuers must contact MasterCard and identify the account range that the service supports.

## **Authorization and Stand-In Processing**

The following Dual Message System and Stand-In processing applies for M/Chip Processing Services.

### **Dual Message System Processing**

The issuer receives the Authorization Request/0100 message containing DE 48, subelement 71 with the value 01C, 01M, or 01S indicating that the Chip to Magnetic Stripe Conversion On-behalf service was performed on the transaction.

---

<b>IF the transaction is Full-Grade and...</b>	<b>THEN the Authorization Platform will...</b>
DE 55 is present, and	Remove DE 55
DE 23 is present, and	Remove DE 23
DE 22, subfield 1 contains:  05 PAN auto-entry via chip	Change DE 22, subfield 1 to 90 = PAN auto-entry via magnetic stripe and DE 48, subelement 71, subfield 2, value C (Conversion of the M/Chip transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 05 [PAN auto-entry via chip] or 79 [Chip card/PAN entry via manual entry])

---

<b>IF the transaction is Full-Grade and...</b>		<b>THEN the Authorization Platform will...</b>
07	PAN auto-entry via contactless M/Chip	<p>Change DE 22, subfield 1 to 90 = PAN auto-entry via magnetic stripe and</p> <p>DE 48, subelement 71, subfield 2, value S (Conversion of the M/Chip transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 07 [PAN auto-entry via contactless M/Chip])</p>
79	Chip card/PAN entry via manual entry	<p>Change DE 22, subfield 1 to 01 = PAN manual entry and</p> <p>DE 48, subelement 71, subfield 2, value C (Conversion of the M/Chip transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 05 [PAN auto-entry via chip] or 79 [Chip card/PAN entry via manual entry])</p>
80	Chip card/PAN via magnetic stripe	<p>Change DE 22, subfield 1 to 90 = PAN auto-entry via magnetic stripe and</p> <p>DE 48, subelement 71, subfield 2, value M (Conversion of the M/Chip fallback transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 80 [PAN auto-entry with magnetic stripe])</p>
<b>IF the transaction is Partial-Grade and...</b>		<b>THEN the Authorization Platform will...</b>
DE 55 is not present, and DE 23 is present		Remove DE 23
DE 22, subfield 1 contains:		
05	PAN auto-entry via chip	<p>Change DE 22, subfield 1 to 90 = PAN auto-entry via magnetic stripe and</p> <p>DE 48, subelement 71, subfield 2, value C (Conversion of the M/Chip transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 05 [PAN auto-entry via chip] or 79 [Chip card/PAN entry via manual entry])</p>

## Program and Service Format Requirements

### M/Chip Processing Services

IF the transaction is Partial-Grade and...		THEN the Authorization Platform will...
07	PAN auto-entry via contactless M/Chip	Change DE 22, subfield 1 to 90 = PAN auto-entry via magnetic stripe and DE 48, subelement 71, subfield 2, value S (Conversion of the M/Chip transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 07 [PAN auto-entry via contactless M/Chip])
79	Chip card/PAN entry via manual entry	Change DE 22, subfield 1 to 01 = PAN manual entry and DE 48, subelement 71, subfield 2, value C (Conversion of the M/Chip transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 05 [PAN auto-entry via chip] or 79 [Chip card/PAN entry via manual entry])
80	Chip card/PAN via magnetic stripe	Change DE 22, subfield 1 to 90 = PAN auto-entry via magnetic stripe and DE 48, subelement 71, subfield 2, value M (Conversion of the M/Chip fallback transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 80 [PAN auto-entry with magnetic stripe])
IF DE 55 is present and...		THEN the Authorization Platform will...
DE 22 is not 05, 07, 79, or 80		Reject the transaction for a format error: DE 39 = 30 DE 44 = 055

### Stand-In and X-Code Processing

Stand-In processes the Authorization Request/0100 message as a magnetic stripe transaction if the issuer is not available. X-Code processes the Authorization Request/0100 message as a magnetic stripe transaction if Stand-In processing is not available.

The Authorization Advice/0120 message contains the converted magnetic stripe transaction and includes DE 48, subelement 71.

<b>Subelement 71 (On-behalf Services)...</b>	<b>Contains...</b>		
Subfield 1 (OB Service)	01	=	Chip to Magnetic Strip Conversion
Subfield 2 (OB Result 1)	C	=	Conversion of the M/Chip transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 05 [PAN auto-entry via chip] or 79 [Chip card/PAN entry via manual entry]
	M	=	Conversion of the M/Chip fallback transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 80 [PAN auto-entry with magnetic stripe]
	S	=	Conversion of the M/Chip transaction to a magnetic stripe transaction was completed from an original POS PAN Entry Mode value of 07 [PAN auto-entry via contactless M/Chip]
Subfield 3 (OB Result 2)	Blank	=	No value present

## M/Chip Cryptogram Pre-validation

The M/Chip Cryptogram Pre-validation service validates the Authorization Request Cryptogram (ARQC) and generates the Authorization Response Cryptogram (ARPC) for issuers subscribing to this service. MasterCard supports cryptogram validation for M/Chip Select 2.0, M/Chip Lite 2.1, M/Chip 4.0 (EMV96 and EMV2000), or Common Core Definition (EMV-CCD) session key derivations.

Transactions that qualify for this service contain the following data elements:

- DE 55 (Integrated Circuit Card [ICC] System Related Data)
- DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) must be one of the following values:
  - 05 = PAN auto-entry via chip
  - 07 = PAN auto-entry via contactless M/Chip

The Authorization Platform performs the following edits:

## Program and Service Format Requirements

### M/Chip Processing Services

IF...	THEN the Authorization Platform will...
DE 55 format is not valid or the required subfields are not present	Reject the transaction for a format error with: DE 39 = 30 DE 44 = 055
DE 48, subelement 71 or subelement 72 are present in the Authorization Request/0100 message from the acquirer host	Reject the transaction for a format error with: DE 39 = 30 DE 44 = 048

### Validation of the Application Cryptogram

Validation of the ARQC in the Application Cryptogram subfield supports parameters linked to each key, based on the PAN (account range), Floor Expiry date, and DMK index (also known as the Key Derivation Index–KDI).

Issuers must provide MasterCard with the keys and parameters according to the On-behalf key management (OBKM) documentation set. MasterCard generates the ARPC unless there was a technical failure. The session key derivations supported include:

- M/Chip2 (Lite and Select) for the ARQC and the ARPC
- M/Chip4 (EMV96 for Lite and Select) for the ARQC and the ARPC
- M/Chip4 (EMV2000 for Lite and Select) for the ARQC and the ARPC
- Common Core Definition (EMV-CCD) for the ARQC and ARPC

Subelement 71—On-behalf Service notifies the issuer that the M/Chip Cryptogram Pre-validation service was performed on the transaction. This service is indicated in subfield 1 OB Service with the value 02. Subfield 2 OB Result 1 provides information that can be used by the issuer in the authorization decision process.

Several tests are performed on DE 55 during the ARQC validation process. The following identifies the tests and the values in subfield 2 (OB Result 1). If a test produces a negative result, no additional tests are performed.

IF starting with the application cryptogram validation...	THEN the value in subelement 71, subfield 2 (OB Result 1) is...
The Application Cryptogram could not be validated due to a technical error	U
A format error is detected in DE 55	F
The Application Cryptogram is invalid	I

<b>IF starting with the application cryptogram validation...</b>	<b>THEN the value in subelement 71, subfield 2 (OB Result 1) is...</b>
The cryptogram in the Application Cryptogram is valid but the AC is not an ARQC	G
The Application Cryptogram was a valid ARQC but the TVR/CVR was invalid	T
No errors were detected in the previous tests, the ARQC is valid	V

Issuers will receive additional detail on the specific Card Verification Results (CVR) and Terminal Verification Results (TVR) found to be in error during the cryptogram validation process. Information about the specific bits in error submitted in the transaction is forwarded to the issuer in DE 48, subelement 79 (Chip CVR/TVR Bit Error Results) of the Authorization Request/0100 message and the Authorization Advice/0120—System-generated message.

The Authorization Request Response/0110 message is returned to the acquirer when a format error occurs. The issuer receives the Authorization Request/0100 message in all other transactions.

When DE 48, subelement 71, subfield 2 contains U, F, I, G, or T, MasterCard sends the acquirer an Authorization Request Response/0110 message where DE 48, subelement 74, subfield 1 is value 02 and subfield 2 is subelement 71, subfield 2 value.

### **Generation of the Issuer Chip Authentication Data**

MasterCard generates the ARPC assuming an approval response from the issuer (DE 39 = 00). This ARPC is placed in DE 48, subelement 72 based on key information provided by the issuer. The ARPC is generated when the ARQC is valid.

MasterCard uses subelement 72 to carry data used during cryptogram processing. The issuer must return this data in the Authorization Request Response/0110 message. If the issuer declines the transaction, MasterCard re-generates the ARPC before sending the Authorization Request Response/0110 message to the acquirer host. MasterCard removes subelements 71 and 72 from the Authorization Request Response/0110 message before sending the message to the acquirer host.

If Stand-In responds to the Authorization Request/0100 message, subelement 72 is also present in the Authorization Advice/0120 message sent by Stand-In processing.

Stand-In processing provides authorization support when the issuer is not available. Normal Stand-In processing occurs when the Application Cryptogram is determined to be valid based on the value in subelement 71, subfield 2 (OB Result 1).

## **Program and Service Format Requirements**

### **M/Chip Processing Services**

---

Stand-In processing uses the decision matrix values from the OBKM interface when subelement 71, subfield 2 (OB Result 1) contains a value of G, I, T, or U indicating the Application Cryptogram is invalid.

The Authorization Response Cryptogram is generated based on the Stand-In response. The Authorization Request Response/0110 message created includes DE 55, subfield ID 91 Issuer Authentication Data.

The Authorization Advice/0120 message includes:

- DE 48, subelement 71 that identifies the service performed on the transaction
- DE 48, subelement 72 that contains the Authorization Response Cryptogram generated based on the approved or declined response
- DE 48, subelement 79 that identifies the CVR/TVR bits found to be in error
- DE 55 containing the ARQC from the Authorization Request/0100 message

### **DE 60 (Advice Reason Code)**

DE 60, subfield 2 contains values depending on values contained in DE 48, subelement 71, subfield 2 as shown below:

<b>IF subfield 2 (OB Result 1) contains...</b>	<b>THEN DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code) contains...</b>	
F	0033	= Incorrect chip data
G	0039	= Cryptogram not ARQC
I	0034	= Chip validation failed
T	0035	= TVR/CVR validation failed
U	0032	= Chip technical failure -Or- Another valid advice reason code
V	0000	= Accept -Or- Another valid advice reason code

Acquirers and issuers are both affected by M/Chip Cryptogram Pre-validation service.

Acquirers should be aware that Issuer Chip Authentication Data may not be present in the Authorization Request Response/0110 message if the ARPC was not generated. The card may decline the transaction.

The M/Chip Cryptogram Pre-validation service is optional. Issuers must contact MasterCard and identify the account range that the service supports. Issuers are also required to provide the keys and parameters according to the OBKM documentation set.

MasterCard notifies the issuer that the M/Chip Cryptogram Pre-validation service was performed on the transaction by the presence of DE 48, subelement 71.

The Authorization Advice/0120 message provides the ARQC from the Authorization Request/0100 message in DE 55. The ARPC generated based on an approved or declined response is in DE 48, subelement 72.

MasterCard does not perform Limit-1 processing for transactions qualifying for the M/Chip Cryptogram Pre-validation service.

If Stand-In is not available, the Authorization Request/0100 message is processed by X-Code. No ARQC validation/ARPC generation occurs on X-Code processing.

Issuers should contact their Customer Implementation Services specialist to sign-up and test the M/Chip Processing services.

## **Combined Service Option**

Issuers can choose an option that combines the Chip to Magnetic Stripe Conversion and M/Chip Cryptogram Pre-validation services.

This option allows two M/Chip processing services to be performed on a single transaction, providing issuers with a bridge to maximize the benefits of chip card processing capabilities while minimizing impacts on their authorization systems. These two services also are available individually.

The Combined Service Option is optional.

## **M/Chip Cryptogram Validation in Stand-In Processing**

The M/Chip Cryptogram Validation in Stand-In processing service supports issuers that process chip transactions on an on-going basis. M/Chip Cryptogram Validation in Stand-In processing supports chip cryptogram validation and generation of the ARPC when the issuer is signed-out, the transaction cannot be delivered to the issuer, or the issuer timed-out.

MasterCard performs the cryptographic support and provides Dual Message System processing for issuers using the M/Chip Select 2.0, M/Chip Lite 2.1, M/Chip 4.0 (EMV 96 and EMV 2000), and Common Core Definition (EMV-CCD) session key derivations.

### **Transaction Qualifiers**

The processing performed by MasterCard for the M/Chip Cryptogram Validation in Stand-In processing service is very similar to the processing performed for the M/Chip Cryptogram Pre-validation service.

## **Program and Service Format Requirements**

### **M/Chip Processing Services**

---

Transactions containing the following data elements qualify for this service:

- DE 55 must be present
- DE 22, subfield 1 containing one of the following values:
  - 05 = PAN auto-entry via chip
  - 07 = PAN auto-entry via contactless M/Chip

For transactions that qualify for this service:

- The ARQC is validated and the TVR/CVR fields are validated according to a default pattern
- Stand-In processing approves or declines the transaction
- The ARPC is generated
- The Authorization Request Response/0110 message is created
- The Authorization Advice/0120 message is created

### **Authorization Platform Edits**

The Authorization Platform performs the following edits:

<b>IF....</b>	<b>THEN the Authorization Platform will...</b>
DE 55 format is not valid or the required subfields are not present	Reject the transaction with format error in DE 39 = 30 DE 44 = 055
DE 48 subelement 71 or subelement 72 are present in the Authorization Request/0100 from the acquirer	Reject the transaction with format error in DE 39 = 30 DE 44 = 048

### **Validation of the Application Cryptogram**

Validation of the ARQC in the Application Cryptogram subfield supports parameters linked to each key, based on the PAN (account range), Floor Expiry date, and DMK index (also known as the Key Derivation Index - KDI).

MasterCard generates the ARPC unless there was a technical failure or the ARQC was invalid.

The session key derivations supported include:

- M/Chip2 (Lite and Select) for the ARQC and the ARPC
- M/Chip4 (EMV 96 for Lite and Select) for the ARQC and the ARPC
- M/Chip4 (EMV 2000 for Lite and Select) for the ARQC and the ARPC
- Common Core Definition (EMV-CCD) for the ARQC and ARPC

Subelement 71 notifies the issuer that the Dynamic M/Chip Stand-In service was performed on the transaction. This is indicated in subfield 1 (OB Service) with the value 03. Subfield 2 (OB Result 1) provides information regarding the results of the ARQC validation.

Several tests are performed on DE 55 during the ARQC validation process. The following identifies the tests and the values in subfield 2. If a test produces a negative result, no additional tests are performed.

<b>IF starting with the application cryptogram validation...</b>	<b>THEN the value in subelement 71, subfield 2 (OB Result 1) is...</b>
The Application Cryptogram could not be validated due to a technical error	U
A format error is detected in DE 55	F (MasterCard Internal only)
The Application Cryptogram is invalid	I
The cryptogram in the Application Cryptogram is valid but the AC is not an ARQC	G
The Application Cryptogram was a valid ARQC but the TVR/CVR was invalid	T
No errors were detected in the previous tests, the ARQC is valid	V

Issuers will receive additional detail on the specific Card Verification Results (CVR) and Terminal Verification Results (TVR) found to be in error during the cryptogram validation process. Information regarding the specific bits in error submitted in the transaction will be forwarded to the issuer in DE 48, subelement 79 (Chip CVR/TVR Bit Error Results) of the Authorization Request/0100 message and the Authorization Advice/0120—System-generated message.

The Authorization Request Response/0110 message is returned to the acquirer when a format error occurs. Stand-In processing will use the issuer defined values from the OBKM interface in all other transactions.

When DE 48, subelement 71, subfield 2 contains U, F, I, G, or T, MasterCard will return an Authorization Request Response/0110 message where DE 48, subelement 74, subfield 1 is value 03 and subfield 2 is subelement 71, subfield 2 value.

## Generation of the Issuer Chip Authentication Data

MasterCard generates the ARPC in DE 48, subelement 72 based on key information provided by the issuer.

MasterCard uses subelement 72 to carry data used during cryptogram processing. Subelement 72 will be present in the Authorization Advice/0120 message sent by Stand-In.

## **Program and Service Format Requirements**

### **M/Chip Processing Services**

---

Stand-In processing provides the authorization support when the issuer is signed out, the transaction cannot be delivered to the issuer, or the issuer timed out. Normal Stand-In processing occurs when the ARQC was determined to be valid based on the value in subelement 71, subfield 2.

Stand-In uses the decision matrix values from the OBKM interface when subelement 71, subfield 2 contains the value G, I, T, or U.

The Authorization Response Cryptogram is generated based on the Stand-In response. The Authorization Request Response/0110 message created includes DE 55, subfield ID 91 Issuer Authentication Data.

The Authorization Advice/0120 message includes:

- DE 48, subelement 71 that identifies the service performed and results
- DE 48, subelement 72 that contains the Authorization Response Cryptogram generated based on approved or declined response.
- DE 48, subelement 79 that identifies the CVR/TVR bits found to be in error
- DE 55 containing the ARQC from the Authorization Request/0100 message

### **DE 60—Advice Reason Code**

DE 60, subfield 2 contains values depending on values contained in DE 48, subelement 71, subfield 2 as shown below:

<b>IF subfield 2 (OB Result 1) contains...</b>	<b>THEN DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code) contains...</b>		
F	0033	=	Incorrect chip data
G	0039	=	Cryptogram not ARQC
I	0034	=	Chip validation failed
T	0035	=	TVR/CVR validation failed
U	0032	=	Chip technical failure
		-Or-	
			Another valid advice reason code
V	0000	=	Accept
		-Or-	
			Another valid advice reason code

Acquirers and issuers are both affected by M/Chip Cryptogram Validation in Stand-In processing service.

Acquirers should be aware that Issuer Chip Authentication Data may not be present in the Authorization Request Response/0110 message if the ARPC was not generated. The card may decline the transaction.

The Authorization Advice/0120 message provides the ARQC from the Authorization Request/0100 in DE 55. The ARPC generated is in DE 48, subelement 72 when the transaction was approved.

If Stand-In processing is not available, the Authorization Request/0100 message is processed by X-Code processing. No ARQC validation/ARPC generation occurs in X-Code processing.

The M/Chip Cryptogram Validation in Stand-In processing service is optional.

Issuers should contact their Customer Implementation Services specialist for information regarding signing up and testing for the M/Chip Processing services.

Issuers must contact MasterCard and identify the account range that the service will support.

## Mobile Remote Payments

Mobile Remote Payments is a payment functionality that is initiated by an enrolled cardholder from the cardholder's mobile device to facilitate a transaction through a service manager.

### NOTE

**Applies only in countries where Mobile Remote Payments transactions are supported. The applicability in a country to support this functionality will be announced in a regional bulletin, a country-specific bulletin, or both.**

A cardholder may choose to enroll in a remote payment service that is accessed using a mobile device, which is a cardholder-controlled mobile phone that has been registered with the cardholder's issuer and which is used for entry of the cardholder's PIN or mobile-specific credentials.

### Acquirer and Issuer Domains

The Mobile Remote Payments program is structured into two primary domains, the acquirer domain and the issuer domain. For both domains, the service manager role is central to the delivery of the Mobile Remote Payments program. The following information describes the business functions related to the service manager role.

- **Acquirer Domain**—In the acquirer domain, the service manager acts on behalf of acquirers. The role of service manager may be filled by an acquirer or by an external Member Service Provider (MSP) approved by MasterCard. Liability does not shift from merchants to issuers under the acquirer domain as cardholder verification is performed either by the acquirer or by the service manager acting on behalf of the acquirer.

## **Program and Service Format Requirements**

### **Mobile Remote Payments**

---

- **Issuer Domain**—In the issuer domain, the service manager acts on behalf of the issuers. The role of service manager may be filled by an issuer or by an external Member Service Provider (MSP) approved by MasterCard. Liability shifts from merchants to issuers under the issuer domain as cardholder verification is performed either by the issuer or by the Service Manager acting on behalf of the issuer.

### **Customer Requirements**

To process Mobile Remote Payments transactions:

- Issuers may use a service manager to provide the Mobile Remote Payments program services.
- Acquirers may use a service manager to provide the Mobile Remote Payments program services.
- All issuers must be able to receive and process all Mobile Remote Payments data present in Authorization Request/0100 messages.
- All acquirers must properly identify Mobile Remote Payments transactions in Authorization Request/0100 messages, and receive and process Mobile Remote Payment transaction Authorization Request Response/0110 messages.
- Mobile Remote Payments transactions have a zero floor limit and must be authorized by the issuer or its agent.

### **To Participate**

Issuers and acquirers must register with MasterCard to participate in the Mobile Remote Payments program, as described in the *Mobile Remote Payments Program Guide*.

### **For More Information**

For more information about:

- Operational processes, security requirements, and guidelines for the Mobile Remote Payments program, see the *Mobile Remote Payments Program Guide*.
- Supporting data requirements, see the *Customer Interface Specification* manual.

## **Authorization Platform Edits**

The following edits are performed on Authorization Request/0100 and Authorization Advice/0120 messages for Mobile Remote Payment transactions.

WHEN...	THEN the Authorization Platform...
DE 48 (Additional Data—Private Use), subelement 48 (Mobile Program Indicators), subfield 1 (Remote Payments Program Type Identifier) contains a value other than 1 (Issuer domain) or 2 (Acquirer Domain)	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 048</li> </ul>
The Authorization Request/0100 or Authorization Request Response/0120—Acquirer-generated message contains: <ul style="list-style-type: none"> <li>• DE 48, subelement 48, subfield 1, value of 1 or 2, and</li> <li>• DE 22 (Point-of-Service [POS] EntryMode), subfield 1 (POS Terminal PAN Entry Mode), is not value 82 (PAN Auto Entry via Server [issuer, acquirer, or third party vendor system])</li> </ul>	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 022</li> </ul>

## Partial Approvals

The Authorization Platform allows acquirers to indicate whether the merchant terminal supports receipt of partial approvals in an authorization request message.

If the acquirer has indicated that the merchant terminal supports receipt of partial approvals, issuers can approve a portion of the requested transaction amount by responding with the approved amount and a partial approval response code in the authorization message. All Debit MasterCard® card issuers in the U.S. region must support partial approvals and updates to the cardholder's open-to-buy balance upon receipt of a reversal (full or partial).

### Authorization Request/0100—Partial Approval

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data Private Use), subelement 61 (POS Data, Extended Condition Codes), subfield 1 (Partial Approval Terminal Indicator)	C	•	C	1 = (Merchant terminal supports receipt of partial approvals)

## Program and Service Format Requirements

### Partial Approvals

---

## Authorization Request Response/0110—Partial Approval

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 4 (Amount, Transaction)	•	X	M	Partial approval amount in acquirer transaction currency.
DE 5 (Amount, Settlement)	•	X	C	Partial approval amount in the settlement currency.
DE 6 (Amount, Cardholder Billing)	M	•	M	Partial approval amount in issuer cardholder billing currency. This amount can be less than or equal to the original amount present in the Authorization Request/0100 message in the amount data element that corresponds to the issuer cardholder billing currency.  This amount may be less than, greater than, or equal to the amount present in the Authorization Request/0100 message when the DE 18 (Merchant Type) is value 5542 (Fuel Dispenser, Automated)
DE 38 (Authorization ID Response)	M	•	M	Authorization Code.
DE 39 (Response Code)	M	•	M	10 = Partial Approval
DE 51 (Currency Code, Cardholder Billing)	M	•	M	Issuer cardholder billing currency code.
DE 54 (Additional Amounts), subfield 2 (Amount Type)	•	X	M	57 = (Original Amount)
DE 54, subfield 4 (Amount)	•	X	M	D = (debit amount) plus 12 digits

### NOTE

**Issuers responding with DE 39, value 10 will not be required to echo DE 4 (Amount, Transaction) in the Authorization Request Response/0110 message. Likewise, if DE 5 (Amount, Settlement) was present in the Authorization Request/0100 message to the issuer, the issuer will not be required to echo DE 5 in the Authorization Request Response/0110 message when responding with DE 39, value 10. The issuer will provide the partial approval amount in DE 6 (Amount, Cardholder Billing).**

The Authorization Platform additionally provides the partial approval amount to the acquirer in the following data elements of the Authorization Request Response/0110 message:

- DE 4 in acquirer's transaction currency
- DE 5 in U.S. dollars if the acquirer receives settlement amount-related data elements

- DE 6 in the issuer's cardholder billing currency

The Authorization Platform will provide two additional occurrences of the original amount in DE 54 of the Authorization Request Response/0110 message to the acquirer; one in the acquirer's currency and one in the issuer cardholder billing currency.

## Reversal Request/0400—Partial Approval

In some cases, the cardholder or merchant may elect not to complete the transaction after receiving the partial approval response from the issuer. MasterCard supports full acquirer-generated reversal messages to allow the merchant to cancel the partial approval.

In addition to all other applicable data elements for the Reversal Request/0400 message, acquirers should submit Reversal Request/0400 messages with the following data elements for a partial approval:

- The partial approval amount in DE 4 that was present in the Authorization Request Response/0110 message to the acquirer, not the original amount present in DE 4 of the Authorization Request/0100 message from the acquirer
- DE 39, value 10

When processing a Reversal Request/0400 message for a partial approval (DE 39, value 10), the issuer should increase the cardholder open-to-buy using the partial approval amount present in the amount data element of the Reversal Request/0400 message that corresponds to the issuer cardholder billing currency.

The Reversal Request/0400 message will not contain DE 48, subelement 61 or DE 54, subelement 2, value 57.

## Reversal Advice/0420—Partial Approval

Following are data elements applicable to this message in addition to the required data elements.

If the Authorization Platform generates a Reversal Advice/0420 message after the issuer has responded to the Authorization Request Response/0110 message with DE 39, value 10, the Authorization Platform will provide the following data elements:

- Partial approval amount in DE 4 in the acquirer transaction currency
- Partial approval amount in DE 5 if the issuer has opted to receive amounts in the settlement currency (U.S. dollars)
- Partial approval amount in DE 6 in the issuer cardholder billing currency
- DE 39, value 10

## **Program and Service Format Requirements**

### **Partial Approvals**

---

- Original amount in DE 54 in the issuer cardholder billing currency (and acquirer transaction currency if different from issuer cardholder billing currency)

When processing an Reversal Advice/0420 message for a partial approval (DE 39, value 10), the issuer should increase the cardholder open-to-buy using the partial approval amount present in the amount data element of the Reversal Advice/0420 message that corresponds to the issuer's cardholder billing currency.

### **Authorization Advice/0120—Issuer-generated (to RiskFinder)**

The following data elements apply to this message in addition to the required data elements.

In addition to the standard data elements that are part of the Authorization Advice/0120—Issuer-generated message to RiskFinder, issuers that choose to initiate Authorization Advice/0120—Issuer-generated messages to RiskFinder for partial approvals should send the following:

- Partial approval amount using the same amount data elements in the same currencies that were present in the Authorization Request/0100 message to the issuer. The issuer may need to perform currency conversion on the partial approval amount to convert it from the issuer cardholder billing currency to the appropriate acquirer transaction currency or U.S. dollars or both.
- DE 39, value 10 as provided by the issuer in the Authorization Request Response/0110 message.

### **Authorization Advice/0120—Acquirer-generated**

The following data elements apply to this message in addition to the required data elements.

When an acquirer creates an Authorization Advice/0120—Acquirer-generated message to advise the issuer of an approved authorization performed by the acquirer, it may include DE 48, subelement 61 in the Authorization Advice/0120—Acquirer-generated message if it was present in the original Authorization Request/0100 message.

DE 39, value 10 is not a valid value for Authorization Advice/0120—Acquirer-generated messages. If an Authorization Advice/0120—Acquirer-generated message contains DE 39, value 10 and the advice is not for an Automated Fuel Dispenser Completion (DE 18 = 5542), the Authorization Platform will generate an Authorization Advice Response/0130 message containing DE 39, value 30 and DE 44 (Additional Data), value 039.

If an Authorization Advice/0120—Acquirer-generated message contains DE 39, value 10 and the advice is for an Automated Fuel Dispenser Completion, the Authorization Platform will change the DE 39 value to 00 (Approved or completed successfully) before forwarding the advice to the issuer.

## Alternate Processing

The Stand-In System and the X-Code System will not provide a partial approval response to an authorization request because these systems do not maintain card balances.

However, if an Authorization Request/0100 message containing DE 48, subelement 61 is processed by the Stand-In System or the X-Code System, the corresponding Authorization Advice/0120—System-generated message will contain DE 48, subelement 61.

## Authorization Platform Edits

The Authorization Platform will perform the following edits.

### Authorization Request/0100 Edits

The Authorization Platform performs the following edits on the Authorization Request/0100 message.

WHEN...	THEN the Authorization Platform...
DE 48, subelement 61, subfield 1 contains a value other than 0 or 1	Generates an Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 048
DE 48, subelement 61, subfields 4–5 contain values other than 0	Generates an Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 048
DE 54 is present in the Authorization Request/0100 message where DE 54, subfield 2 contains value 57 (Original Amount)	Generates an Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 054

### Authorization Request Response/0110 Edits

The Authorization Platform performs the following edits on the Authorization Request Response/0110 message when the issuer has provided DE 39 with value 10.

## Program and Service Format Requirements

### Partial Approvals

---

WHEN...	THEN the Authorization Platform...
DE 48, subelement 61 is not present or DE 48, subelement 61, subfield 1 does not contain value 1 in the Authorization Request/0100 message sent to the issuer	Generates an Authorization Response Negative Acknowledgement/0190 message to the issuer where: DE 39 = 30 DE 44 = 039
DE 38 is not present	Generates an Authorization Response Negative Acknowledgement/0190 message to the issuer where: DE 39 = 30 DE 44 = 038
DE 6 is not present	Generates an Authorization Response Negative Acknowledgement/0190 message to the issuer where: DE 39 = 30 DE 44 = 006
The issuer responds with DE 39, value 10 (Partial Approval) and DE 6 is a partial approval amount equal to the original requested amount in the Authorization Request/0100 message	Allows the partial approval amount to be equal to the requested amount.
DE 6 (Amount, Cardholder Billing) is an amount greater than or equal to the original amount provided in the Authorization Request/0100 message And DE 39 (Response Code) is 10 (Partial Approval) And DE 18 (Merchant Type) is not 5542 (Fuel Dispenser, Automated)	Rejects the Authorization Request Response/0110 message with an Authorization Response Negative Acknowledgement/0190 where: DE 39 = 30 DE 44 = 006
DE 51 is not present or is not the issuer's correct cardholder billing currency code	Generates an Authorization Response Negative Acknowledgement/0190 message to the issuer where: DE 39 = 30 DE 44 = 051

### Authorization Advice (Acquirer-generated)/0120 Edits

The Authorization Platform performs the following edit on the Authorization Advice/0120—Acquirer-generated message.

WHEN...	THEN the Authorization Platform...
DE 39 contains value 10 (Partial Approval) and the advice message is <b>not</b> for an Automated Fuel Dispenser Completion message (DE 18 = 5542)	Generates an Authorization Advice Response (System-generated)/0130 message containing: DE 39 = 30 DE 44 = 039

## Payment Transactions

A Payment Transaction facilitates the movement of funds between two parties—a payer (sender) and a payee (recipient). This transaction can be used to support several business opportunities, such as person-to-person payments, merchant rebates and rewards, loading value to a debit or prepaid account, issuer rebates and rewards.

A Payment Transaction also may be used to initiate a Private Label prepaid card activation request. For card activation requests there is no movement of funds. Refer to the Private Label Processing section in this chapter for more information.

Payment Transactions are identified in the following messages:

- Authorization Request/0100
- Authorization Advice/0120—System-generated
- Reversal Request/0400
- Reversal Advice/0420

### Authorization Request/0100—Payment Transaction Message

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) (Cardholder account credits)	M	•	M	28 = Payment Transaction
DE 3, subfield 2 (Cardholder “From Account” Type Code)	M	•	M	00 = Default account (account not specified or not applicable)
DE 3, subfield 3 (Cardholder “To Account” Type Code)	M	•	M	Any valid value for subfield 3.
DE 18 (Merchant Type)	M	•	M	Valid merchant type value for Payment Transaction.

## Program and Service Format Requirements

### Payment Transactions

---

Data Element	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	P = Payment Transaction
DE 48, subelement 77 (Payment Transaction Type Indicator)	M	•	M	<p>Must be one of the following values:</p> <ul style="list-style-type: none"><li>• C01 = Person-to-Person</li><li>• C02 = Rebate</li><li>• C03 = Load Value</li><li>• C04 = Gaming Re-pay (usage is limited to eligible acquirers and issuers in eligible countries)</li><li>• C05 = Payment Transaction (for a reason other than those defined in values C01–C04)</li><li>• C06 = Payment of a credit card balance with cash or check</li><li>• C07 = MasterCard <i>MoneySend</i></li><li>• C09 = Card Activation (Currently only applicable for Private Label Prepaid Cards issued in Europe)</li></ul>

## Authorization Request Response/0110—Payment Transaction

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code)	ME	•	ME	Processing Code value in the original Authorization Request/0100 message.
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	CE	•	CE	P = Payment Transaction

## Authorization Platform Edits

Issuers must process transaction amounts in a Payment Transaction as a credit to the cardholder account. Following are Authorization Request/0100 and Reversal Request/0400 Edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 3, subfield 1, value 28 and TCC value P are not both present	Sends the acquirer a response where: DE 39 = 30 (Format error) DE 44 = 048
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) does not contain value 28 (Payment Transaction) and DE 48, subelement 77 is present	Removes DE 48, subelement 77 from the following messages: <ul style="list-style-type: none"><li>• Authorization Request/0100</li><li>• Reversal Request/0400</li><li>• Reversal Advice/0420</li></ul>
DE 3, subelement 1 is value 28 and DE 48, subelement 77 is not included	Sends the acquirer a response where: DE 39 = 30 (Format error) DE 44 = 048
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) contains value 28 (Payment Transaction), and DE 48 (Additional Data—Private Use), subelement 77 (Payment Transaction Type Indicator), contains value C09 (Card Activation) and DE 61 (Point of Sale [POS] Data) subfields does not contain the following values: <ul style="list-style-type: none"><li>• Subfield 1 (POS Terminal Attendance) = 0 (Attended Terminal)</li><li>• Subfield 3 (POS Terminal Location) = 0 (On premises of card acceptor facility)</li><li>• Subfield 4 (POS Cardholder Presence) = 0 (Cardholder present)</li><li>• Subfield 5 (POS Card Presence) = 0 (Card present)</li><li>• Subfield 10 (Cardholder-Activated Terminal [CAT] Level) = 0 (Not a CAT transaction)</li></ul>	The Authorization Platform declines the request with a format error response where: DE 39 (Response Code) = 30 DE 44 (Response Data) = 061
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) contains value 28 (Payment	The Authorization Platform declines the request with a format error response where: DE 39 (Response Code) = 30

## Program and Service Format Requirements

### Payment Transactions

---

WHEN...	THEN the Authorization Platform...
<p>Transaction), and DE 48 (Additional Data—Private Use), subelement 77 (Payment Transaction Type Indicator), contains value C09 (Card Activation) and</p> <p>DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) does not contain one of the following values:</p> <ul style="list-style-type: none"><li>• 02 = PAN entry mode unknown</li><li>• 05 = PAN auto-entry via chip07 = PAN auto-entry via contactless M/Chip</li><li>• 80 = Chip card at chip-capable terminal was unable to process transaction using data on the chip; therefore, the terminal defaulted to the magnetic stripe-read PAN. The full track data has been read from the data encoded on the card and transmitted within the Authorization Request/0100 in DE 45 (Track 1 Data) or DE 35 (Track 2 Data) without alteration or truncation. To use this value, the acquirer must be qualified to use value 90.</li><li>• 90 = PAN auto-entry via magnetic stripe—the full track data has been read from the data encoded on the card and transmitted within the authorization request in DE 35 (Track 2 Data) or DE 45 (Track 1 Data) without alteration or truncation.</li><li>• 91 = PAN auto-entry via contactless magnetic stripe—the full track data has been read from the data on the card and transmitted within the authorization request in DE 35 (Track 2 Data) or DE 45 (Track 1 Data) without alteration or truncation.</li></ul>	DE 44 (Response Data) = 022

#### NOTE

**The Authorization Platform will reject the transaction with a format error on DE 3 if the acquirer sends an Authorization Advice/0120—Acquirer-generated message where DE 3, subfield 1 contains value 28.**

## PayPass CVC 3 Processing Service

MasterCard provides *PayPass* processing services to assist issuers processing *PayPass* transactions with the validation of the Card Validation Code 3 (CVC 3) to ensure the values provided by the acquirer match the issuer's expected values.

MasterCard offers the following on-behalf services:

- **Static CVC 3 Pre-validation Service**—The Static CVC 3 Pre-validation service is an optional, stand-alone service for issuers with authorization systems that do not support static CVC 3 validation. The Static CVC 3 Pre-validation Service uses the CVC 1 algorithm and key type. The *PayPass* Mapping Service may be used with the Static CVC 3 Pre-validation Service.
- **Static CVC 3 Validation in Stand-In Processing Service**—This is an optional service for issuers with *PayPass*-enabled authorization systems that support static CVC 3 validation using the CVC 1 algorithm and key type that would like MasterCard to provide static CVC 3 validation when the issuer is not available and the transaction is processed by the Stand-In System.

MasterCard will perform the static CVC 3 validation on behalf of the issuer before forwarding the Authorization Request/0100 message. If the issuer is unavailable, MasterCard will consider the results of the static CVC 3 validation when the transaction is processed by the Stand-In System.

- **Dynamic CVC 3 Pre-validation Service**—This is an optional stand-alone service for issuers with *PayPass*-enabled authorization systems that do not support dynamic CVC 3 validation. The *PayPass* Mapping Service may be used with the Dynamic CVC 3 Pre-validation Service.

MasterCard will perform the dynamic CVC 3 validation on behalf of the issuer before forwarding the Authorization Request/0100 message. If the issuer is unavailable, MasterCard will consider the results of the dynamic CVC 3 validation when the transaction is processed by the Stand-In System.

- **Dynamic CVC 3 Validation in Stand-In Processing Service**—This is an optional service for issuers with *PayPass*-enabled authorization systems that support dynamic CVC 3 validation in-house that would like MasterCard to provide dynamic CVC 3 validation when the issuer is not available and the transaction is processed by the Stand-In System.

### NOTE

**In conjunction with the revised standards for PayPass, effective 1 July 2007  
MasterCard no longer offers the Static CVC 3 Pre-validation Service, but  
continues to support the Static CVC 3 Validation in Stand-In Service.**

The *PayPass* Mapping Service is for issuers with non-*PayPass*-enabled authorization systems that are not able to support the processing of a separate *PayPass* account number and the validation of dynamic CVC 3 value.

## Program and Service Format Requirements

### PayPass CVC 3 Processing Service

---

Participation in any CVC 3 on-behalf service or services is defined by account range. Validation will be facilitated by information the issuer provides to MasterCard. Issuers will be requested to provide confidential key data to MasterCard that will be critical in the validation process (unless MasterCard arranges for devices to be sent to cardholders on behalf of issuers). For information about the CVC 3 on-behalf services and how to participate, see the *Authorization Manual*.

## Authorization Request/0100—CVC 3

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

The Authorization Request/0100 message will contain CVC 3 values in DE 45 (Track 1 Data) or DE 35 (Track 2 Data) following the configuration provided by the issuer. The MasterCard branded *PayPass* account number is entered via contactless magnetic stripe where DE 22 (Point of Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) is 91.

MasterCard will apply the appropriate algorithm to DE 45 or DE 35 using the parameter data provided by the issuer to determine the validity of the CVC 3.

Data Element	Org	Sys	Dst	Values/Comments
DE 22 (Point of Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	91 = PAN auto-entry via contactless magnetic stripe—the full track data has 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. The MasterCard branded <i>PayPass</i> account number is entered via contactless magnetic stripe
DE 35 (Track 2 Data)	C	•	C	Contains CVC 3 values following the configuration by the issuer.
DE 45 (Track 1 Data)	C	•	C	Contains CVC 3 values following the configuration by the issuer.
DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 1 (On-behalf [OB] Service)	M	•	M	12 = Static CVC 3 Pre-validation Service 13 = Static CVC 3 Validation in Stand-In Processing 15 = Dynamic CVC 3 Pre-validation (with or without PayPass Mapping Service) 16 = Dynamic CVC 3 Validation in Stand-In Processing
DE 48, subelement 71, subfield 2 (On-behalf [OB] Result 1) when subfield 1 contains value 12 or 13	M	•	M	I = Invalid U = Unable to process V = Valid

Data Element	Org	Sys	Dst	Values/Comments
DE 48, subelement 71, subfield 2 when subfield 1 contains value 15 or 16	M	•	M	A = ATC outside allowed range (applicable when ATC value is dynamic [varying value]) E = CVC 3 ATC Replay I = Invalid N = Unpredictable Number Mismatch (applicable when the UN is dynamic [varying value]). (Indicates that the number/length in the discretionary data in DE 45 or DE 35 does not match the number/length provided by the issuer during personalization). U = Unable to process V = Valid
DE 48, subelement 71, subfield 3 (On-behalf [OB] Result 2)	M	•	M	This subfield is for MasterCard use only.

## Dynamic CVC 3 Application Transaction Counter (ATC) Processing

The ATC is used in the calculation of the dynamic CVC 3 cryptogram. The ATC counter value is managed by the chip on a *PayPass* card that increments with every authorization that occurs at a *PayPass*-enabled terminal.

The Authorization Platform supports DE 48, subelement 71 (On-behalf Service), subfield 2 (On-behalf [OB] Result 1), value E (CVC 3 ATC Replay) in the Authorization Request/0100 message to indicate to the issuer that the ATC value has been used in a previous transaction.

When the result of Dynamic CVC 3 validation in DE 48, subelement 71, subfield 2 is V (Valid) or A (ATC outside allowed range), the Authorization Platform compares the transaction's ATC value to the stored list of ATC values for each *PayPass* account number/sequence number/expiration date combination.

If the ATC used in validating the CVC 3 value is not in the stored list of ATC values, the Authorization Platform adds the transaction's five-digit ATC value to the stored list of ATC values.

If the ATC used in validating the CVC 3 value is in the stored list of ATC values, the Authorization Platform replaces DE 48, subelement 71, subfield 2, value V or A with value E in the Authorization Request/0100 message to the issuer. The Authorization Platform does not add the transaction's ATC again to the stored list of ATC values.

Replacing the DE 48, subelement 71, subfield 2 value V or A, with value E does not affect any data contained in the message that supports value V or A. For example, DE 48, subelement 34 supports value A, but remains unchanged if value E replaces DE 48, subelement 71, subfield 2, value A.

The Authorization Platform populates DE 48, subelement 87 (Card Validation Code Result) value Y (Invalid) in the Authorization Request Response/0110 message to the acquirer.

**NOTE**

**The Authorization Platform only adds to the list of stored ATC values for transactions that have been processed online through the MasterCard Authorization Platform. ATC values for transactions processed offline are not available for the Authorization Platform to use in CVC 3 ATC replay processing.**

## **Dynamic CVC 3 Application Transaction Counter (ATC) Information**

DE 48, subelement 34 (Dynamic CVC 3 ATC Information) provides issuers with information about the ATC value derived for use in dynamic CVC 3 validation processing.

DE 48, subelement 34 will be conditionally present in Authorization Request/0100 messages and Authorization Advice/0120—System-generated messages when the issuer participates in the Dynamic CVC 3 Pre-validation service or the Dynamic CVC 3 Validation in Stand-In Processing service.

The Authorization Platform will provide DE 48, subelement 34 when the Dynamic CVC Pre-validation service or the Dynamic CVC 3 Validation in Stand-In Processing service is performed and validation results in DE 48, subelement 71 (On-behalf Services, subfield 2 (On-behalf [OB] Result 1) contain the value A (ATC outside allowed range), E (CVC 3 ATC Replay), or V (Valid). DE 48, subelement 34 also may be sent as part of the PayPass Mapping service if implemented with Dynamic CVC 3 Pre-validation.

When responding to the Authorization Request/0100 message, issuers should consider the results of the CVC 3 validation in DE 48, subelement 71, subfield 2 and DE 48, subelement 34 (if present).

## **MCC109 (PayPass Application Transaction Counter File)**

The MCC109 (Application Transaction Counter [ATC] file) contains a range of ATC values for a *PayPass* account number/card sequence number/expiration date combination for *PayPass* cards that were personalized using dynamic values in the ATC and unpredictable number (UN). Issuers participating in the Dynamic CVC 3 Pre-validation service or the Dynamic CVC 3 Validation in Stand-In Processing service may provide this file to MasterCard. Issuers may only add to or inquire about this file.

MasterCard supports entry of the ATC data in DE 101 (File Name), value (MCC109) via the following methods:

- Issuer File Update/0302 messages
- Bulk file request (R311)

- MasterCard eService

MCC109 (*PayPass* Application Transaction Counter [ATC] File) maintenance requests submitted via the Issuer File Update Request/0302 message or MasterCard eService are applied immediately. Maintenance requests submitted by bulk file are applied one time per day at 18:00 St. Louis, MO USA time.

#### **NOTE**

**This functionality does not apply to *PayPass* cards and devices that were personalized to send zeros in the ATC and UN.**

### **Authorization Platform Edits**

The Authorization Platform performs the following edits on Issuer File Update Request/0302 messages when DE 101 (File Name) contains value MCC109 and DE 120 (Record File Layout) contains the layout for the *PayPass* ATC File.

Field ID and Name	Authorization Edit
1 PayPass Account Number	<ul style="list-style-type: none"> <li>• <i>PayPass</i> account number must be present</li> <li>• <i>PayPass</i> account number is numeric</li> <li>• <i>PayPass</i> account number prefix is valid</li> <li>• <i>PayPass</i> account number check digit is correct</li> <li>• <i>PayPass</i> account number required in the <i>PayPass</i> ATC File (MCC109) for additions and inquiries</li> </ul>
2 Card Sequence Number	<ul style="list-style-type: none"> <li>• Card sequence number must be present</li> <li>• Card sequence number is numeric</li> <li>• Value may be zero</li> <li>• Card sequence number is required in the <i>PayPass</i> ATC File (MCC109) for additions and inquiries</li> </ul>
3 PayPass Account Expiration Date	<ul style="list-style-type: none"> <li>• <i>PayPass</i> Account Expiration Date is valid YYMM format</li> <li>• <i>PayPass</i> Account Expiration Date is required in the <i>PayPass</i> ATC File (MCC109) for additions and inquiries</li> </ul>
4 PayPass Application Transaction Counter (ATC) Value	<ul style="list-style-type: none"> <li>• <i>PayPass</i> ATC is numeric (may be zero)</li> <li>• <i>PayPass</i> ATC is required in the <i>PayPass</i> ATC File (MCC109) for a additions and inquiries</li> </ul>

#### **NOTE**

**Fields 1 through 3 are mandatory for an inquiry. Fields 1 through 4 are mandatory for an add.**

## **Card Validation Code Result**

The acquirer will receive DE 48, subelement 87 when the CVC 3 validation result was not valid.

Acquirers may receive the following:

- Y = Indicates the ATC was determined to be outside the allowed range specified by the issuer, the ATC was determined to be a replay, or the CVC 3 value was determined to be invalid.
- E = Indicates the length of the unpredictable number was not a valid length resulting in an Unpredictable Number (UN) that was not valid.
- P = Indicates MasterCard was unable to process the CVC 3 validation.

If the CVC 3 data is valid, the Authorization Platform will not include DE 48, subelement 87 in the Authorization Request Response/0110 message to the acquirer.

The issuer will receive the Authorization Advice/0120 message, DE 48, subelement 87 when CVC 3 was invalid in the Authorization Request/0100 message.

## **Optional Non-valid CVC 3 Processing**

Issuers may elect to have the Authorization Platform respond to Authorization Request/0100 messages on their behalf when the CVC 3 value is not valid. The issuer will receive an Authorization Advice/0120—System-generated message when the Authorization Platform responds.

For information about how to participate, see the *PayPass On-behalf Services Guide*.

The following table describes the process that occurs when the issuer wants the Authorization Platform to respond to Authorization Request/0100 messages on its behalf during CVC 3 validation.

---

<b>WHEN the CVC 3 validation results contain a value of...</b>	<b>THEN the Authorization Platform...</b>
A, E, I, N, or U	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"><li>• DE 39 = 05 (Do not honor)</li><li>• DE 48, subelement 87 = E, P, or Y</li></ul> <p>Generates an Authorization Advice/0120 message to the issuer containing:</p> <ul style="list-style-type: none"><li>• DE 39, value 05 (Do not honor)</li><li>• DE 48, subelement 34 (if created)</li></ul>

**WHEN the CVC 3 validation results contain a value of...**

**THEN the Authorization Platform...**

- DE 48, subelement 71 with the appropriate values
- DE 48, subelement 87, value E, P, or Y
- DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code), value 115 (Transaction processed via MIP On-behalf Service Decision)
- DE 60, subfield 2 (Advice Detail Code), one of the following values:
  - 0042 (CVC 3 Unable to process)
  - 0043 (CVC 3 ATC outside allowed range)
  - 0044 (CVC 3 Invalid)
  - 0045 (CVC 3 Unpredictable number mismatch)
  - 0046 (CVC 3 ATC Replay)

V

Forwards the Authorization Request/0100 to the issuer for processing

---

## ATC Data Extract File

MasterCard provides the ability for issuers participating in the Dynamic CVC 3 On-behalf services to optionally request a file containing all ATCs that MasterCard is currently storing for each PayPass account number/card sequence number/expiration date combination within a requested account range(s). Issuers that want to perform their own dynamic CVC 3 validation processing can use this ATC information to provide the foundation for an initial repository of ATCs. Issuers can request the ATC data by individual account range(s) or for all account ranges within an ICA.

Issuers that want to obtain this information must contact their Customer Operations Services representative for a one time initial setup for this file. Then, each time the issuer wants to receive the current list of ATCs on file, the issuer must submit an ATC Data File Request for this information using bulk type RH51 (test bulk type RH53). The ATC Data File Outbound delivered to the issuer will be bulk type TM44 (test bulk type TM46).

Reference the *Account Management System User Manual* for the layout of this file.

## **Alternate Processing**

MasterCard supports issuers subscribing to the CVC 3 Pre-validation services (12, 15) that are not available to respond to the Authorization Request/0100 message and issuers subscribing to the CVC 3 Validation in Stand-In Processing service (13, 16) by responding to the authorization message on behalf of the issuer. MasterCard will consider the results of the CVC 3 validation in DE 48, subelement 71 when responding to the Authorization Request/0100.

The values in DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code) are dependant upon the values contained in DE 48, subelement 71, subfield 2 (OB Result 1) as described below.

<b>IF DE 48, subelement 71, subfield 2 contains the value...</b>	<b>THEN DE 60, subfield 2 will contain...</b>
U	0042 (CVC 3 [Unable to process])
A	0043 (CVC 3 [ATC outside allowed range])
E	0046 (CVC 3 ATC Replay)
I	0044 (CVC 3 [Invalid])
N	0045 (CVC 3 [Unpredictable number mismatch])

MIP X-Code processing does not perform CVC 3 validation. MIP X-Code processing will respond based on the type of transaction and the MIP X-Code limits defined.

## **PayPass Mapping Service for PayPass M/Chip and Contact M/Chip Transactions**

The *PayPass* Mapping Service will be performed for participating account ranges when DE 22, subfield 1 contains value 05 (PAN auto-entry via chip) or value 07 (PAN auto-entry via contactless M/Chip). The *PayPass* Mapping service will replace values 05 and 07 with values 06 and 08, respectively, before forwarding the message to the issuer.

Issuers that participate in the *PayPass* Mapping Service and that issue *PayPass* M/Chip or Contact M/Chip cards must be prepared to receive transactions containing new values 06 and 08 in DE 22, subfield 1.

Issuers will not return these new values in the corresponding response messages to acquirers.

## **PayPass Mapping Service Processing of PayPass M/Chip and Contact M/Chip Transactions**

The following process describes how the Authorization Platform processes Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, and Reversal Request/0400 messages for *PayPass* Mapping Service transactions.

<b>WHEN the message contains...</b>	<b>THEN the Authorization Platform...</b>
DE 22, subfield 1, value 05 (PAN auto-entry via chip) and The <i>PayPass</i> Mapping Service was performed on the transaction	Changes the value in DE 22, subfield 1 from 05 to 06, indicating that the <i>PayPass</i> Mapping Service occurred.
DE 22, subfield 1, value 07 (PAN auto-entry via contactless M/Chip) and The <i>PayPass</i> Mapping Service was performed on the transaction	Changes the value in DE 22, subfield 1 from 07 to 08, indicating that the <i>PayPass</i> Mapping Service occurred.

The *PayPass* Mapping Service occurs on Authorization 0100, Authorization Advice/0120—acquirer-generated, and Reversal Request/0400 messages. The following example describes the *PayPass* Mapping Service being performed on an Authorization Request/0100 message.

Stages describing the process that occurs when an Authorization Request/0100 transaction is generated from a *PayPass* M/Chip or Contact M/Chip card eligible for the *PayPass* Mapping Service.

1. When a cardholder initiates an eligible *PayPass* M/Chip or Contact M/Chip transaction on a *PayPass* M/Chip or Contact M/Chip terminal, the *PayPass* M/Chip PAN or Contact M/Chip PAN is passed to the terminal.
2. The acquirer sends an Authorization Request/0100 message containing the *PayPass* M/Chip PAN or Contact M/Chip account number to the Authorization Platform.
3. The Authorization Platform maps the *PayPass* M/Chip or Contact M/Chip account number to the cardholder's PAN (or funding account), and then forwards the authorization message containing the following values to the issuer:
  - DE 2 (Primary Account Number [PAN]) containing the cardholder's PAN
  - DE 14 (Date, Expiration) containing the cardholder's expiry date, if provided
  - DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), value 08 (Contactless M/Chip *PayPass* Mapping Service applied) or 06 (PAN auto-entry via chip *PayPass* Mapping Service applied)

## **Program and Service Format Requirements**

### **PayPass Mapping Service for PayPass M/Chip and Contact M/Chip Transactions**

---

- DE 23 (Card Sequence Number) containing the *PayPass* M/Chip or Contact M/Chip card sequence number, if provided
  - DE 35 (Track 2 Data), if provided, is removed
  - DE 45 (Track 1 Data), if provided, is removed
  - DE 48 (Additional Data—Private Use), subelement 33 (*PayPass* Mapping Information) containing *PayPass* M/Chip or Contact M/Chip PAN information
  - DE 48, subelement 71 (On-behalf Services), identifying the *PayPass* Mapping Service and any other on-behalf services performed
  - DE 55 (Integrated Circuit Card [ICC] System-related Data), as originally sent by the terminal
4. The issuer responds with an Authorization Request Response/0110 message containing the cardholder's PAN in DE 2.
  5. The Authorization Platform maps the PAN back to the *PayPass* M/Chip or Contact M/Chip account number and places the cardholder's PAN in DE 48, subelement 33, and then sends the *PayPass* M/Chip or Contact M/Chip account number in DE 2 to the acquirer.
  6. The acquirer forwards the *PayPass* M/Chip or Contact M/Chip account number and other authorization response information to the *PayPass* terminal.

The *PayPass* Mapping Service for *PayPass* M/Chip and Contact M/Chip transactions (DE 22, subfield 1, value 05 or 07) requires participation in the Dynamic CVC 3 Pre-validation Service unless the account range comprises M/Chip cards that have not had the magnetic stripe profile programmed.

For more information about the MasterCard *PayPass* Mapping Service, refer to the *PayPass On-behalf Services Guide*.

## **Authorization Platform Edits**

The following edit will be performed on Authorization Request/0100, Authorization Advice/0120, and Reversal Request/0400 messages to enforce the current valid expiration date edit that exists for both *PayPass* M/Chip and Contact M/Chip transactions that are eligible for the *PayPass* Mapping Service.

WHEN...	THEN the Authorization Platform...
<p>The expiration date in DE 14, DE 35, or DE 45 (whichever data element is first to contain the expiration date) is expired and DE 22, subfield 1 is value 05 or 07 and The account is part of an account range that participates in the PayPass Mapping Service</p>	Rejects the transaction and sends the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 message where DE 39 (Response Code) is 54 (Expired card).

## Pay with Rewards Service

The MasterCard Pay with Rewards service provides cardholders with the ability to redeem their loyalty points as currency to pay for purchases at any merchant where MasterCard-branded payment cards are accepted. The cardholder will use a separately issued “redemption card,” which will be a MasterCard debit product, to initiate points redemption transactions at the POS.

The cardholder can initiate a points redemption transaction by presenting the Pay with Rewards card as a mode of payment. The acquirer will route the corresponding Authorization Request/0100 message to the Authorization Platform.

The Authorization Platform will determine that the account range of Primary Account Number (PAN) in DE 2 participates in the MasterCard Pay with Rewards service. If the account range is for the MasterCard Pay with Rewards service, the Authorization Platform will route such Authorization Request/0100 transaction to the MasterCard Rewards System (MRS).

The Authorization Platform supports Authorization Request/0100 and full and partial Reversal Request/0400 processing for the Pay with Rewards service.

## Authorization Request/0100—Pay with Rewards

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number [(PAN)])	M	•	M	Contains the issuer's or LPO's corporate funding account.
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	Contains values 00 = Purchase

## Program and Service Format Requirements

### Pay with Rewards Service

Data Element	Org	Sys	Dst	Values/Comments
DE 14 (Date, Expiration)	C	•	C	Contains the expiration date associated to the funding card.
DE 48 (Additional Data—Private Use), TCC	M	•	M	PWR can be used for purchases only. No ATM, no Cash Disbursements, no Payments.
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 1 (Account Number Indicator)	•	X	C	R = Pay with Rewards card, indicating the Pay with Rewards card follows
DE 48, subelement 33, subfield 2 (Account Number)	•	X	C	Contains Pay with Rewards card PAN.
DE 48, subelement 33, subfield 3 (Expiration Date)	•	X	C	May contain actual expiration date only if issuer provided in MCC106 (PAN Mapping File).
DE 48, subelement 33, subfield 4 (Product Code)	•	X	C	Contains Pay with Rewards card product code, if provided.
DE 48, subelement 71 (On-behalf Services), subfield 1 (On-behalf [OB] Service)	•	X	C	Contains value 27 (Pay with Rewards Service) to indicate the Pay with Rewards card was presented at the POS.
DE 48, subelement 71, subfield 2 (On-behalf [OB] Result 1)	•	X	C	Indicates the results of the Pay with Rewards service processing.

### Authorization Request Response/0110—Pay With Rewards

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number [(PAN)]	ME	•	ME	Contains the Pay with Rewards card presented at the POS for the transaction
DE 63 (Network Data), subfield 1 (Financial Network Code)	ME	•	ME	Represents the product code of the Pay with Rewards card.
DE 63, subfield 2, (Financial Network Code)	ME	•	ME	Contains Banknet Reference Number.
DE 121 (Authorizing Agent ID Code)	C	•	C	000004 = MasterCard Rewards System

**NOTE**

As with other dynamic mapping services, DE 35 (Track Data) on the Authorization Request/0100 message to the issuer will continue to represent the Pay with Rewards card presented at the POS. The issuer should continue to recognize the transaction as having a mapping service performed and associate the track data to DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information) instead of DE 2 (Primary Account Number [PAN]).

## Authorization Platform Edits

The Authorization Platform performs the following edits on Pay With Rewards transactions.

<b>WHEN the acquirer...</b>	<b>THEN the Authorization Platform...</b>
Sends an Authorization Request/0100 message containing a value other than 00 (Purchase) in DE 3 (Processing Code) for a Pay with Rewards PAN	Sends the acquirer an Authorization Request Response/0110 containing DE 39 (Response Code), value 57 (Transaction not permitted to issuer/cardholder).
Sends an Authorization Advice/0120 message for a Pay with Rewards PAN	Sends the acquirer an Authorization Advice Response/0130 message containing DE 39, value 57.
<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
One or more rules, restrictions, or controls fail	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) = Pay with Rewards card presented at the POS</li> <li>• DE 39 (Response Code) = 05 (Do not honor)</li> <li>• DE 121 (Authorizing Agent ID Code) = 000004 (MasterCard Rewards System)</li> </ul> <p>Sends the issuer an Authorization Advice/0120 message where:</p> <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) = Pay with Rewards card presented at the POS</li> <li>• DE 39 (Response Code) = 05 (Do not honor)</li> <li>• DE 48 (Additional Data—Private Use, Subelements), subelement 71 (On-behalf Services), subfield 1 (On-behalf [OB] Service) = 27 (Pay with Rewards Service)</li> <li>• DE 48, subelement 71, subfield 2 (On-behalf [OB] Result 1) = value R (Pay with Rewards transaction)</li> </ul>

## Program and Service Format Requirements

### Pay with Rewards Service

---

WHEN...	THEN the Authorization Platform...
	<p>declined on issuer's behalf for failing rules/restrictions)</p> <ul style="list-style-type: none"><li>• DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) = 126 (Pay with Rewards processing advice to issuer)</li><li>• DE 60, subfield 2 (Advice Detail Code) = 0121 (Reject: Pay with Rewards—Redemption rule(s) failed)</li><li>• DE 121 = 000004 (MasterCard Rewards System)</li></ul>
DE 2 contains a PAN that is not registered for the MasterCard Pay with Rewards service	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"><li>• DE 2 (Primary Account Number [PAN]) = Pay with Rewards card presented at the POS</li><li>• DE 39 (Response Code) = 05 (Do not honor)</li><li>• DE 121 = 000004 (MasterCard Rewards System)</li></ul> <p>Sends the issuer an Authorization Advice/0120 message where:</p> <ul style="list-style-type: none"><li>• DE 2 = Pay with Rewards card presented at the POS</li><li>• DE 39 (Response Code) = 05 (Do not honor)</li><li>• DE 48, subelement 71, subfield 1 = 27</li><li>• DE 48, subelement 71, subfield 2 = N (Pay with Rewards transaction declined—Card not registered for service)</li><li>• DE 60, subfield 1 = 126</li><li>• DE 60, subfield 2 = 0123 (Reject: Pay with Rewards—Account not registered)</li><li>• DE 121 = 000004 (MasterCard Rewards System)</li></ul>

WHEN...	THEN the Authorization Platform...
Points balance is insufficient	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) = Pay with Rewards card presented at the POS</li> <li>• DE 39 (Response Code) = 05 (Do not honor)</li> <li>• DE 121 = 000004 (MasterCard Rewards System)</li> </ul> <p>Sends the issuer an Authorization Advice/0120 message where:</p> <ul style="list-style-type: none"> <li>• DE 2 = Pay with Rewards card presented at the POS</li> <li>• DE 39 (Response Code) = 05 (Do not honor)</li> <li>• DE 48, subelement 71, subfield 1 = 27</li> <li>• DE 48, subelement 71, subfield 2 = I (Pay with Rewards transaction declined on issuer's behalf for insufficient points balance)</li> <li>• DE 60, subfield 1 = 126</li> <li>• DE 60, subfield 2 = 0120 (Reject: Pay with Rewards—Insufficient points balance)</li> <li>• DE 121 = 000004 (MasterCard Rewards System)</li> </ul>
Unable to perform the Pay with Rewards service	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) = Pay with Rewards card presented at the POS</li> <li>• DE 39 (Response Code) = 96 (System error)</li> </ul> <p>Sends the issuer an Authorization Advice/0120 message where:</p> <ul style="list-style-type: none"> <li>• DE 2 = Pay with Rewards card presented at the POS</li> <li>• DE 39 = 96 (System error)</li> <li>• DE 48, subelement 71, subfield 1 = 27</li> <li>• DE 48, subelement 71, subfield 2 = U (Pay with Rewards service was not performed successfully)</li> </ul>

## **Program and Service Format Requirements**

### **PIN Management Service**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
	<ul style="list-style-type: none"><li>• DE 60, subfield 1 = 126</li><li>• DE 60, subfield 2 = 0122 (Decline: Pay with Rewards service was not performed successfully)</li></ul>
System Error Occurred after Pay with Rewards service processed the request	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"><li>• DE 2 = Pay with Rewards card presented at the POS</li><li>• DE 39 = 96 (System error)</li></ul>
	<p>Sends the issuer an Authorization Advice/0120 message where:</p> <ul style="list-style-type: none"><li>• DE 2 = Pay with Rewards card presented at the POS</li><li>• DE 48, subelement 71, subfield 1 = 27</li><li>• DE 48, subelement 71, subfield 2 = L (Pay with Rewards transaction funded using consumer loyalty points)</li><li>• DE 60, subfield 1 = 126</li><li>• DE 60, subfield 2 = 0124 (Decline: Systems error)</li></ul>
<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The MasterCard Rewards Service (MRS) successfully processes a MasterCard Pay with Rewards redemption transaction and the Authorization Request/0100 message is delivered to the issuer, but the issuer returns a partial approval response code in the Authorization Request Response/0110 message	<p>Creates and sends the issuer an Authorization Response Negative Acknowledgement/0190 message containing:</p> <p>DE 39 = 30 (Format Error) DE 44 = 039</p>

## **PIN Management Service**

### **Chip PIN Management Service**

The Chip PIN Management Service is an optional service that enables cardholders to perform the transactions at ATMs that support MasterCard, Maestro®, or Cirrus® chip cards.

Transactions supported are:

- PIN change—Allows cardholders to change the PIN code on their chip card.

- PIN unblock—Allows cardholders to unblock the PIN code on their chip card by resetting the PIN try counter.

The Chip PIN Management Service is available only to full grade acquirers and chip grade issuers. For example, the Chip PIN Management Service is *not* available for:

- Transactions initiated with a chip card using magnetic stripe technology
- Issuers that use the Chip to Magnetic Stripe Conversion on-behalf service
- Issuers that use the M/Chip Cryptogram Pre-validation

### **Authorization Request/0100—PIN Change (Chip Card)**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number [PAN])	M	•	M	
DE 3 (Processing Code), subfield 1	M	•	M	92 = PIN Change
DE 3, subfield 2 (Cardholder Transaction Type Code)	M	•	M	00 = Default Account
DE 3, subfield 3 (Cardholder “To Account” Type Code)	M	•	M	00 = Default Account
DE 4 (Amount, Transaction)	M	•	M	Must be zero unless an ATM transaction fee has been applied by an acquirer for an ATM transaction in a country where application of an ATM transaction fee is allowed.
DE 18 (Merchant Type)	M	•	M	6011 = Member Financial Institution-Automated Cash Disbursement
DE 22 (Point-of-Service (POS) Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	05 = PAN auto-entry via chip
DE 22, subfield 2 (POS Terminal PIN Entry Mode)	M	•	M	1 = Terminal has PIN entry capability
DE 28, (Amount, Transaction Fee)	C	•	C	May contain an ATM transaction fee, if applicable for transactions in a country where application of an ATM transaction fee is allowed.
DE 32 (Acquiring Institution ID Code)	M	•	M	

## Program and Service Format Requirements

### PIN Management Service

---

Data Element	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	Space or Z = ATM Cash Disbursement
DE 52 (Personal ID Number [PIN] Data)	C	X	C	Required for ATM transactions
DE 55 (Integrated Circuit Card (ICC) System-Related Data)	C	•	C	Conditional data for chip-based transactions
DE 125 (New PIN Data)	C	X	C	Must be present for all online chip card PIN change transactions; otherwise not present  DE 125 contains the new PIN, which is formatted into one of the supported PIN block formats and is then encrypted. The PIN block format and encryption method used must be the same as the one used for the existing PIN that is stored in DE 52.

### Authorization Request Response/0110—PIN Change (Chip Card)

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 39 (Response Code)	M	•	M	00 = Successful PIN change 71 = PIN Not Changed 85 = Successful PIN change (recommended for chip cards) 89 = Unacceptable PIN—Transaction Declined—Retry
DE 55 (Integrated Circuit Card [ICC] System-Related Data)	C	•	C	Contains system-generated Authorization Response Cryptogram (APRC).  Depending on the card application, DE 55 may contain an issuer script. The issuer script message contains instructions to the chip card: <ul style="list-style-type: none"><li>• If the issuer approves the PIN unblock request, the script message instructs the chip card to unblock the PIN on the card.</li><li>• If the issuer declines the PIN unblock request, the issuer may optionally provide additional instructions to block the chip card (for example, block the card or the card application) using the related issuer script.</li></ul>

**Reversal Request/0400—PIN Change (Chip Card)**

Following is a list of the data elements and values applicable to this message type. All mandatory Reversal Request/0400 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 2 (Primary Account Number [PAN])	M	•	M	
DE 3 (Processing Code), subfield 1	M	•	M	92 = PIN Change
DE 3, subfield 2 (Cardholder Transaction Type Code)	M	•	M	00 = Default Account
DE 3, subfield 3 (Cardholder "To Account" Type Code)	M	•	M	00 = Default Account
DE 4 (Amount, Transaction)	M	•	M	Must be zero unless an ATM transaction fee has been applied by an acquirer for an ATM transaction in a country where application of an ATM transaction fee is allowed.
DE 18 (Merchant Type)	M	•	M	6011 = Member Financial Institution-Automated Cash Disbursement
DE 22 (Point-of-Service (POS) Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	05 = PAN auto-entry via chip
DE 22, subfield 2 (POS Terminal PIN Entry Mode)	M	•	M	1 = Terminal has PIN entry capability
DE 28, (Amount, Transaction Fee)	C	•	C	May contain an ATM transaction fee, if applicable for transactions in a country where application of an ATM transaction fee is allowed.
DE 32 (Acquiring Institution ID Code)	M	•	M	
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	X	M	Space or Z = ATM Cash Disbursement
DE 48, subelement 20 (Cardholder Verification Method)	M	X	M	P = Online PIN Verification

**Magnetic Stripe PIN Management Service**

MasterCard has expanded the optional Chip PIN Management service to allow cardholders to change the PIN associated with their non-chip (magnetic stripe) MasterCard® credit, Debit MasterCard®, Maestro®, or Cirrus® card at any ATM that supports this functionality.

## Program and Service Format Requirements

### PIN Management Service

---

This expansion allows issuers globally to provide their cardholders with additional conveniences for their magnetic stripe cards.

Participating acquirers in the Europe region that process transactions through the Dual Message System can indicate a PIN change transaction performed on a magnetic stripe card in the Authorization Request/0100—PIN Change (Magnetic Stripe Card) message.

### Authorization Request/0100—PIN Change (Magnetic Stripe Card)

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number [PAN])	M	•	M	
DE 3 (Processing Code), subfield 1	M	•	M	92 = PIN Change
DE 3, subfield 2 (Cardholder Transaction Type Code)	M	•	M	00 = Default Account
DE 3, subfield 3 (Cardholder “To Account” Type Code)	M	•	M	00 = Default Account
DE 4 (Amount, Transaction)	M	•	M	Must be zero unless an ATM transaction fee has been applied by an acquirer for an ATM transaction in a country where application of an ATM transaction fee is allowed.
DE 18 (Merchant Type)	M	•	M	6011 = Member Financial Institution-Automated Cash Disbursement
DE 22 (Point-of-Service (POS) Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	02 = PAN auto-entry via magnetic stripe—track data is not required) or 90 PAN auto-entry via magnetic stripe—the full track data has been read)
DE 22, subfield 2 (POS Terminal PIN Entry Mode)	M	•	M	1 = Terminal has PIN entry capability
DE 28, (Amount, Transaction Fee)	C	•	C	May contain an ATM transaction fee, if applicable for transactions in a country where application of an ATM transaction fee is allowed.
DE 32 (Acquiring Institution ID Code)	M	•	M	
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	Space or Z = ATM Cash Disbursement

Data Element	Org	Sys	Dst	Values/Comments
DE 52 (Personal ID Number [PIN] Data)	C	X	C	Required for ATM transactions
DE 125 (New PIN Data)	C	X	C	Must be present for all online chip card PIN change transactions; otherwise not present  DE 125 contains the new PIN, which is formatted into one of the supported PIN block formats and is then encrypted. The PIN block format and encryption method used must be the same as the one used for the existing PIN that is stored in DE 52.

**NOTE**

**In the event of a transaction failure or time out, the acquirer must reverse the PIN change transaction so that the issuer is aware that the PIN change was not completed at the ATM. Consequently, the new PIN should not be considered active.**

**Authorization Request Response/0110—PIN Change (Magnetic Stripe Card)**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 39 (Response Code)	M	•	M	00 = Successful PIN change 71 = PIN Not Changed 85 = Successful PIN change (recommended for chip cards) 89 = Unacceptable PIN—Transaction Declined—Retry

**Reversal Request/0400—PIN Change (Magnetic Stripe Card)**

Following is a list of the data elements and values applicable to this message type. All mandatory Reversal Request/0400 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1	M	•	M	92 = PIN Change
DE 3, subfield 2 (Cardholder Transaction Type Code)	M	•	M	00 = Default Account
DE 3, subfield 3 (Cardholder “To Account” Type Code)	M	•	M	00 = Default Account

## Program and Service Format Requirements

### PIN Management Service

Data Element	Org	Sys	Dst	Values/Comments
DE 4 (Amount, Transaction)	M	•	M	Must be zero unless an ATM transaction fee has been applied by an acquirer for an ATM transaction in a country where application of an ATM transaction fee is allowed.
DE 18 (Merchant Type)	M	•	M	6011 = Member Financial Institution-Automated Cash Disbursement
DE 22 (Point-of-Service (POS) Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	02 = PAN auto-entry via magnetic stripe—track data is not required) or 90 PAN auto-entry via magnetic stripe—the full track data has been read)
DE 22, subfield 2 (POS Terminal PIN Entry Mode)	M	•	M	1 = Terminal has PIN entry capability
DE 28, (Amount, Transaction Fee)	C	•	C	May contain an ATM transaction fee, if applicable for transactions in a country where application of an ATM transaction fee is allowed.
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	X	M	Space or Z = ATM Cash Disbursement
DE 48, subelement 20 (Cardholder Verification Method)	M	X	M	P = Online PIN Verification

### Authorization Request/0100 Edits (Magnetic Stripe Card)

The following edits apply for PIN Management magnetic stripe transactions.

WHEN...	THEN the Authorization Platform...
DE 3, subfield 1 contains value 91 (PIN Unblock) and DE 22, subfield 1 does not contain value 05 (PAN auto-entry via chip)	Sends the acquirer an Authorization Request Response/0110 message where DE 39 (Response Code) = 57 (Transaction not permitted to issuer/cardholder).
DE 3, subfield 1 contains value 92 (PIN Change) and DE 125 is not present	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 30 (Format error) DE 44 (Additional Response Data) = 125 (indicating the data element in error)

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 3, subfield 1 contains value 92 and DE 22, subfield 1, does not contain one of the following values: <ul style="list-style-type: none"><li>• 02 (PAN auto-entry via magnetic stripe—track data is not required)</li><li>• 90 (PAN auto-entry via magnetic stripe—the full track data has been read)</li></ul>	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 30 DE 44 = 022
DE 3, subfield 1 contains value 92 and DE 22, subfield 2 does not contain value 1 (Terminal has PIN entry capability)	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 30 DE 44 = 022
DE 3, subfield 1 contains value 92 and DE 52 is not present	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 30 DE 44 = 052
DE 3, subfield 1 contains value 92 and DE 4 does not contain a value of all zeros, indicating a zero-amount transaction and DE 28 is not present	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 30 DE 44 = 004
DE 3, subfield 1 contains value 92 and DE 48, TCC contains a value other than Z (ATM Cash Disbursement) or space	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 30 DE 44 = 048
The acquirer does not participate in the PIN Management service	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 58 (Transaction not permitted to acquirer/terminal)
The issuer does not participate in the PIN Management service	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 57 (Transaction not permitted to issuer/cardholder)
The issuer is not able to respond to the PIN Management transaction on time	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 91 (Authorization Platform or issuer system inoperative)

## **Program and Service Format Requirements**

### **PIN Management Service**

---

#### **Authorization Advice/0120—Acquirer-generated Edits (Magnetic Stripe Card)**

The following edits apply to PIN Management magnetic stripe card transactions.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 3, subfield 1 contains value 92	Sends the acquirer an Authorization Advice Response/0130 message where: DE 39 = 30 DE 44 = 003

#### **Reversal Request/0400 Edits (Magnetic Stripe Card)**

The following edits apply to PIN Management, magnetic stripe card transactions.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 3, subfield 1 contains value 92 and DE 22, subfield 1, does not contain one of the following values: <ul style="list-style-type: none"><li>• 02</li><li>• 90</li></ul>	Sends the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 022
DE 3, subfield 1 contains value 92 and DE 22, subfield 2 does not contain value 1	Sends the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 022
DE 3, subfield 1 contains value 92 and DE 4 does not contain a value of all zeros, indicating a zero-amount transaction and DE 28 is not present	Sends the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 004
DE 3, subfield 1 contains value 92 and DE 48, TCC contains a value other than Z or space	Sends the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 048

WHEN...	THEN the Authorization Platform...
The acquirer does not participate in the PIN Management service	Sends the acquirer a Reversal Request Response/0410 message where DE 39 = 58 (Transaction not permitted to acquirer/terminal)
The issuer does not participate in the PIN Management service	Sends the acquirer a Reversal Request Response/0410 message where DE 39 = 57 (Transaction not permitted to issuer/cardholder)

## Issuer Response Options to a Magnetic Stripe PIN Change Request

For PIN change transactions, the issuer may respond using one of the following methods:

- If the card is a non-chip (magnetic stripe) card or if the card is a chip card **not** supporting offline PIN and the issuer approves, the issuer sends an Authorization Request Response/0110 message containing DE 39 (Response Code), value 00 (Approved or completed successfully) or DE 39, value 85 (Not declined).

### NOTE

**When approving a PIN change transaction, MasterCard recommends that issuers of chip cards send DE 39, value 85 in the Authorization Request Response/0110 message.**

- If the card is a non-chip (magnetic stripe) card or if the card is a chip card **not** supporting offline PIN and the issuer declines, the issuer sends an Authorization Request Response/0110 message containing DE 39, value 70 (Contact Card Issuer), DE 39, value 71 (PIN Not Changed), or DE 39, value 89 (Unacceptable PIN—Transaction Declined—Retry).
- If the card is a chip card supporting offline PIN, the issuer must decline and send an Authorization Request Response/0110 message containing DE 39, value 57 (Transaction not permitted to issuer/cardholder).

Issuers that have chip cards personalized with both online and offline PIN must not approve PIN change transactions when DE 22 (Point of Service [POS] Entry Mode, subfield 1 (POS Terminal PAN Entry Mode) contains value 02 or value 90. If these transactions are approved, the offline PIN will be out-of-sync with the online PIN, and subsequent offline transactions may be declined due to invalid PIN.

If an issuer's account range participates in Chip to Magnetic Stripe Conversion or M/Chip Cryptogram Pre-validation on-behalf services, that account range cannot participate in the Chip PIN Management service, even if the account range also contains magnetic stripe cards.

## **PIN Processing for Europe Region Members**

MasterCard supports PIN translation for acquirers and issuers and issuer PIN validation for Track 1 and Track 2 on the Banknet telecommunications network for customers in the Europe Region.

### **PIN Translation**

The Authorization Platform performs PIN translation on DE 52 (Personal ID Number [PIN] Data) and DE 125 (New PIN Data) for issuers and acquirers that use the MasterCard Worldwide Network.

When issuers perform PIN processing in-house or when they participate in the Online PIN Validation in Stand-In service, issuers must specify DE 53, subfield 4 (PIN key index number) in the Network Management Request/0800—Sign-On/Sign-off message, all remaining DE 53, subfields may be zero filled.

Issuers participating in the Online PIN Pre-validation Service are not required to send DE 53 in the Network Management Request/0800—Sign-On/Sign-off message.

Acquirers specify the key used to encrypt the PIN using the Authorization Request/0100 message.

The Key Management Services (KMS) group provides members a Member Key ID (MKID) for each service. The MKID is used to notify the KMS group of new security keys. Each customer will associate the PIN key index number to identify a specific security key. Customers may define a maximum of 99 security keys for use during PIN translation.

### **DE 53 (Security-related Control Information)**

Acquirers will specify DE 53, subfield 3 (PIN Block Format Code) when sending the Authorization Request/0100 message.

Issuers that use the PIN translation service to translate DE 52 and DE 125 (New PIN Data) will receive DE 53, subfield 4 (PIN Key Index Number) that identifies the PIN key used for translation.

PIN translation also will be performed on DE 125, if present, when the PIN translation was successfully completed for DE 52.

## **PIN Translation Edits**

The following edits apply to Authorization Request/0100 messages (for acquirers only).

WHEN...	THEN the Authorization Platform...
The acquirer uses the Authorization Platform for PIN translation and DE 52 (Personal ID Number [PIN] Data) is present and DE 53 (Security-related Control Information) is not present	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30 (Format error)</li> <li>• DE 44 = 053 (DE 53 is the data element in error)</li> </ul>
The acquirer uses the Authorization Platform for PIN translation and DE 52 is present and DE 53, subfield 3 (PIN Block Format Code) is not valid. (Valid values are 01, 02, 03, 10, 11, and 19.)	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 053</li> </ul>
The acquirer uses the Authorization Platform for PIN translation and DE 52 is present and DE 53, subfield 4 (PIN Key Index Number) contains a PIN Key Index Number not known to MasterCard	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"> <li>• DE 39 = 88 (Cryptographic failure)</li> <li>• DE 48 (Additional Data—Private Use), subelement 80 (PIN Service Code) = TI (The Authorization Platform was unable to translate the PIN)</li> </ul>
The acquirer does not use the Authorization Platform for PIN translation and DE 53 is present	Removes DE 53 and forwards the Authorization Request/0100 message to the MasterCard Debit Switch (MDS)
An Authorization Platform Security Translation Platform fails	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"> <li>• DE 39 = 88</li> <li>• DE 48, subelement 80 = TI</li> </ul>

The following edits apply to Network Management Request/0800 sign-on messages.

WHEN...	THEN the Authorization Platform...
The issuer uses the Authorization Platform for PIN translation and DE 53, subfield 4 (PIN Key Index Number) contains a PIN Key Index Number not known to MasterCard	Sends the issuer a Network Management Request Response/0810 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 053</li> </ul>

## PIN Validation

The Authorization Platform supports the following PIN validation methods:

- IBM3624 (variable length)
- ABA (MasterCard/VISA PVV)

## **Program and Service Format Requirements**

### **PIN Processing for Europe Region Members**

---

PIN validation results will be provided in DE 48, subelement 71 (On-behalf Services) in Authorization Request/0100 and Authorization Advice/0120—System-generated messages when PIN validation has been performed on behalf of the issuer. DE 48, subelement 71 will contain the following values related to PIN validation:

- Subfield 1 (On-behalf [OB] Service) will contain the following values:
  - 08 (Online PIN Pre-validation)
  - 09 (PIN Validation in Stand-In)
- Subfield 2 (On-behalf [OB] Result 1) when subfield 1 is value 08 or 09:
  - I (Invalid)
  - P (Mandatory PVV not on file)
  - R (PIN retry exceeded)
  - U (Unable to process)
  - V (Valid)
- Subfield 3 (On-behalf [OB] Result 2) is blank when it is sent to the issuer

The Authorization Platform will manage tracking the number of PIN failed attempts at the card level (for example, PAN, card sequence number from the track and expiration date).

DE 52 (Personal ID Number [PIN] Data) is not included in the Authorization Request/0100 message when PIN validation is performed.

---

<b>WHEN the issuer subscribes to the...</b>	<b>THEN the issuer...</b>
PIN Validation in Stand-In service	<p>Chooses the PIN Failed Attempts limit, which must be less than or equal to five.</p> <p>The Stand-In System will reset the PIN Failed Attempts counter to zero when a valid PIN is entered and the count has not exceeded the issuer defined maximum.</p> <p>The Stand-In System will reset the PIN Failed Attempts counter to zero after the Stand-In System maintenance.</p>
Online PIN Pre-validation	<p>Does not choose the PIN Failed Attempts. MasterCard will allow five PIN Failed Attempts. The Authorization Platform will reset the PIN Failed Attempts counter to zero when a valid PIN is entered and the count has not exceeded five. The Authorization Platform will reset the PIN Failed Attempts counter to zero after 24 hours has passed.</p>

---

## PIN Validation Edits

The following edits apply to Authorization Request/0100 messages (for issuers only).

WHEN...	THEN the Authorization Platform...
The issuer uses the Authorization Platform for PIN pre-validation and the PIN is valid and the number of PIN failed attempts were not yet exceeded	Forwards the Authorization Request/0100 message where: <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 08 (Online PIN Pre-validation)</li> <li>• DE 48, subelement 71, subfield 2 = V (Valid)</li> </ul>
The issuer uses the Authorization Platform for PIN pre-validation and the PIN validation cannot be performed	Forwards the Authorization Request/0100 message where: <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 08</li> <li>• DE 48, subelement 71, subfield 2 = U (Unable to process)</li> </ul>
The issuer uses the Authorization Platform for PIN pre-validation and the number of PIN retries were exceeded	Forwards the Authorization Request/0100 message where: <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 08</li> <li>• DE 48, subelement 71, subfield 2 = R (PIN retry exceeded)</li> </ul>
The issuer uses the Authorization Platform for PIN pre-validation and the PIN validation fails	Forwards the Authorization Request/0100 message where: <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 08</li> <li>• DE 48, subelement 71, subfield 2 = I (Invalid)</li> </ul>
The issuer uses the Authorization Platform for PIN pre-validation and has specified Mandatory PVV On File and the PVV was not found	Forwards the Authorization Request/0100 message where: <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 08</li> <li>• DE 48, subelement 71, subfield 2 = P (Mandatory PVV not on file)</li> </ul>

**Program and Service Format Requirements**  
**PIN Processing for Europe Region Members**

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The issuer uses the Authorization Platform for PIN Validation in Stand-In, PIN validation fails, and the number of PIN retries were not yet exceeded	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = issuer defined</li> <li>• DE 48, subelement 80 = PI (Authorization Platform unable to process PIN)</li> </ul> <p>Sends the issuer an Authorization Advice/0120—System-generated message where:</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 09 (PIN Validation in Stand-In)</li> <li>• DE 48, subelement 71, subfield 2 = I (Invalid)</li> <li>• DE 60, subfield 2 = 0051 (invalid PIN)</li> </ul>
The issuer uses the Authorization Platform for PIN Validation in Stand-In and the PIN validation fails	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = issuer defined</li> <li>• DE 48, subelement 80 = PI</li> </ul> <p>Sends the issuer an Authorization Advice/0120 (System-generated) message where:</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 09</li> <li>• DE 48, subelement 71, subfield 2 = U (Unable to process)</li> <li>• DE 60, subfield 2 = 0050 (Unable to process)</li> </ul>
The issuer uses the Authorization Platform for PIN Validation in Stand-In and the PIN is valid and the number of PIN retries were not yet exceeded	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = determined by remaining Stand-In processing tests</li> <li>• DE 48, subelement 80 = PV (Valid PIN)</li> </ul> <p>Sends the issuer an Authorization Advice/0120 (System-generated) message where:</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 09</li> <li>• DE 48, subelement 71, subfield 2 = V (Valid)</li> </ul>

WHEN...	THEN the Authorization Platform...
The issuer uses the Authorization Platform for PIN Validation in Stand-In and the number of PIN retries were exceeded	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = issuer defined response code</li> <li>• DE 48, subelement 80 = PI</li> </ul> <p>Sends the issuer an Authorization Advice/0120—System-generated message where:</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 09</li> <li>• DE 48, subelement 71, subfield 2 = R (PIN retry exceeded)</li> <li>• DE 60, subfield 2 = 0052 (PIN Retry Exceeded-invalid PIN)</li> </ul>
The issuer uses the Authorization Platform for PIN Validation in Stand-In and has specified Mandatory PVV On File and the PVV was not found	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = issuer defined value</li> <li>• DE 48, subelement 80 = PI</li> </ul> <p>Sends the issuer an Authorization Advice/0120—System-generated message where:</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 09</li> <li>• DE 48, subelement 71, subfield 2 = P (Mandatory PVV not on file)</li> <li>• DE 60, subfield 2 = 0052 (Mandatory PVV not on file)</li> </ul>
The issuer uses the Authorization Platform for PIN Validation in Stand-In and the PIN translation fails	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 88</li> <li>• DE 48, subelement 80 = TI</li> </ul> <p>Sends the issuer an Authorization Advice/0120—System-generated message where:</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1 = 09</li> <li>• DE 48, subelement 71, subfield 2 = U (Unable to process)</li> <li>• DE 60, subfield 2 = 0050 (Unable to process)</li> </ul>

## **PIN Key Management**

The Key Management Services (KMS) group will manage the security keys for customers using the PIN translation and PIN validation services supported by the Authorization Platform on the MasterCard Worldwide Network.

## **PIN Verification Value (PVV)/PIN Offset on File Service**

The PVV/PIN Offset used in PIN validation is usually located on Track 1 or Track 2 of a cards magnetic stripe. MasterCard offers a service by which the issuer may optionally send the PVV/PIN offsets, in a file to MasterCard in order to override the information encoded in the track of a cards magnetic stripe.

MasterCard activates the PVV/PIN Offset data from an issuer upon receipt of the PVV/PIN Offset File. Issuers may send a full file replacements weekly.

### **Processing Transactions Using PVV/PIN Offset**

Issuers that use the optional PVV/PIN Offset on File processing must request participation in the service for each card range and (optionally) expiry date range.

To process a transaction, the Authorization Platform checks that PVV/PIN Offset details are held on file for the relevant card range and expiry date range. If details are on file for the card range and expiry date range, the Authorization Platform checks for the individual card's details within the issuer's stored file.

The Authorization Platform checks the entry in the PVV/PIN Offset file to ensure that the card's PAN, card sequence number, and expiry date match. If they do match, the Authorization Platform can use the PVV value on file. If the PAN, card sequence number, and expiry date do not match, the Authorization Platform processes the transaction according to the processing parameters that the issuer specifies for the relevant card range and expiry date.

### **Processing Parameters**

MasterCard stores the issuer PVV/PIN Offset files for use in the Online PIN Pre-validation and the Online PIN Validation in Stand-In on-behalf services. When the Authorization Platform cannot find a matching entry (with the correct PAN, card sequence number, and expiry date values) in the issuer PVV/PIN Offset file, it needs further instructions to process the transaction properly.

The issuer must select one of the following processing options for each card range and expiry date:

- **Optional on file**—With this option, if no matching PVV/PIN Offset entry is found in the PVV/PIN Offset file, the Authorization Platform retrieves the PVV value from Track 1 or Track 2 of the relevant card.
- **Mandatory on file**—With this option, the Authorization Platform, having checked the Track 1 or Track 2 information for the issuer card against the

entries held in the issuer PVV/PIN Offset file, performs one of the following actions:

- For Stand-In services, the Authorization Platform returns an Authorization Request Response/0110 message to the acquirer and an Authorization Advice/0120—System-generated message to the issuer with the appropriate response code, detailing the result of the processing.
- For Pre-validation services, the Authorization Platform forwards the results of the PIN validation to the issuer in an Authorization Request/0100 message and to the acquirer in an Authorization Request Response/0110 message.

The Global Parameters section of the Authorization Parameter Summary Report provides an indicator to identify issuer participation.

## PVV/PIN Offset File Format

Following is the PVV/PIN Offset File format that has a fixed length of 64 characters. Issuers may use Bulk ID RA85 or CONNECT:Direct to send the PVV/PIN Offset file to MasterCard.

### PVV/PIN Offset File Header Record

Field Name	Attribute	Length	Comments/Values
Record type ID	Alphanumeric	3	HDR—header record
File version number	Numeric	3	100 (initial version)
Customer ID	Alphanumeric	11	First six digits must contain the issuers ICA with leading zeros Seventh digit and beyond contains trailing spaces
Transmission code	Alphanumeric	10	Member assigned transmission code. May contain all spaces or zeros.
Transmission sequence	Numeric	4	0000-9999 Wraps at 9999
Transmission date	Numeric	6	YYMMDD in UTC
Transmission time	Numeric	6	hhmmss in UTC
Input file type	Alphanumeric	1	F: Full file replace
Filler	Alphanumeric	20	Spaces

**Program and Service Format Requirements**  
**PIN Processing for Europe Region Members**

---

**PVV/PIN Offset File Detail Record**

<b>Field Name</b>	<b>Attribute</b>	<b>Length</b>	<b>Comments/Values</b>
Record type ID	Alphanumeric	3	DTL—detail record
Update code	Alphanumeric	1	A = add/update
PAN	Numeric	19	With trailing spaces
Card expiry date	Numeric	4	YYMM (must contain a valid year and month)
Card sequence number	Numeric	1	Must contain the Sequence Number associated with the PAN or 0. A value of 0 indicates that the card sequence number should not be used as criteria when matching to the PVV file.
PVV/PIN Offset	Numeric	6	Trailing spaces
Filler	Alphanumeric	30	Spaces

**PVV/PIN Offset File Trailer Record**

<b>Field Name</b>	<b>Attribute</b>	<b>Length</b>	<b>Comments/Values</b>
Record type ID	Alphanumeric	3	TRL—trailer record
Number of detail records	Numeric	11	Detail record count
Filler	Alphanumeric	50	Spaces

**Alternate Processing**

MasterCard will support issuers subscribing to the Online PIN Pre-validation service (OB service code value 08) that are not available to respond to the Authorization Request/0100 message and issuers subscribing to the PIN Validation in Stand-In service (OB service code value 09) by responding to the Authorization Request/0100 message on behalf of the issuer. MasterCard will consider the results of the PIN validation in DE 48, subelement 71 when responding to the Authorization Request/0100 message.

The values contained in DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code) are dependant on the values contained in DE 48, subelement 71, subfield 2 (OB Result 1) as described in the following table.

<b>WHEN DE 48, subelement 71, subfield 2 contains the value...</b>	<b>THEN DE 60, subfield 2 will contain...</b>
U (Unable to Process)	0050
I (Invalid)	0051
P (Mandatory PVV not on file)	0052
R (PIN Retry Exceeded [invalid PIN])	0052

## PIN Processing for non-Europe Members

Personal identification number (PIN) is a proven technology that is not easily circumvented. It is secure within actual market conditions. MasterCard permits acquirers to use PIN technology at the point of sale that prompts MasterCard cardholders for a PIN.

This section contains PIN processing procedures for non-Europe customers. For information about PIN processing procedures for Europe Region acquirers and issuers that process through the MasterCard Worldwide Network, see the PIN Processing for Europe Region Members section.

### Acquirer Requirements

Acquirers must comply with the following before processing MasterCard purchase transactions that contain a PIN (such as CAT Level 1 transactions) in Authorization/01xx messages:

- Support either static or dynamic PIN Encryption Key (PEK) exchanges
- Comply with the MasterCard Magnetic Stripe Compliance Program
- Correctly format Authorization Request/0100—PIN messages
- Correctly format Authorization Request Response/0110—PIN messages

### Support either Static or Dynamic PIN Encryption Key (PEK) Exchanges

The Authorization Platform and members' system use PEK to encrypt or decrypt PINs. PEKs provide a secure means of passing PIN information in Authorization/01x messages. Acquirers must support **either** static **or** dynamic PEK exchanges.

**For increased security, MasterCard strongly recommends using dynamic PEK exchanges.**

Following are the differences between the two options:

## **Program and Service Format Requirements**

### **PIN Processing for non-Europe Members**

<b>PEK</b>	<b>Description</b>
Static	<ul style="list-style-type: none"> <li>• Members and the Authorization Platform establish these keys offline.</li> <li>• Members and the Authorization Platform must establish a single PEK. This PEK must be associated with the acquirer's customer ID.</li> </ul>
Dynamic	<ul style="list-style-type: none"> <li>• Members and the Authorization Platform exchange these keys automatically online every 24 hours or every 2,500 transactions, whichever occurs first.</li> <li>• Members and the Authorization Platform use Key Encryption Keys (KEKs) to encrypt and decrypt the PEKs during PEK exchanges between the acquirer and the Authorization Platform. Each acquirer must establish a KEK with MasterCard to exchange the PEKs dynamically with the Authorization Platform. This KEK must be associated with the acquirer's customer ID.</li> </ul>

### **MasterCard Magnetic Stripe Compliance Program Compliance**

PIN verification requires valid track data, only acquirers that comply with the MasterCard magnetic stripe compliance program and provide complete and unaltered track data in their Authorization Request/0100 messages are able to support PIN processing.

### **Authorization Request/0100—PIN Transactions**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	<p>Must contain one of the following values:</p> <ul style="list-style-type: none"> <li>• 05 = (PAN auto entry via chip)</li> <li>• 07 = (PAN auto entry via contactless M/Chip)</li> <li>• 80 = (PAN auto entry via magnetic stripe, unable to process a chip card at chip-capable terminal)</li> <li>• 90 = (PAN auto entry via magnetic stripe)</li> </ul>
DE 26 (POS PIN Capture Code)	C	•	C	Must be present when DE 52 (PIN Data) is present and the maximum PIN characters that the terminal accepts is something other (more or less) than 12 characters.

## Program and Service Format Requirements

### PIN Processing for non-Europe Members

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 32 (Acquiring Institution ID Code)	M	•	M	If present, must be the same ID as the Member Group ID for the Authorization Platform to translate the PIN data that the acquirer provides.
DE 33 (Forwarding Institution ID Code)	C	•	C	If present, must be the same ID as the Member Group ID for the Authorization Platform to translate the PIN data that the acquirer provides
DE 35 (Track-2 Data)	C	•	C	Must be present and represent the information as encoded on the magnetic stripe of the card (or the equivalent data if a chip card and chip-capable terminal are used at the point of interaction) OR
DE 45 (Track-1 Data)	C	•	C	Must be present and represent the information as encoded on the magnetic stripe of the card (or the equivalent data if a chip card and chip-capable terminal are used at the point of interaction)
DE 52 (PIN Data)	C	X	C	The 16-digit number Data Encryption Standard (DES) hexadecimal number in the ANSI PIN block format (also referred to as “ISO Format-0” or “Eurocheque Format-1”)

## **Authorization Request Response/0110—PIN Transactions**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 39 (Response Code)	M	•	M	Contains response code indicating the Authorization Platform or the issuer could or could not verify the PIN entered at the point of interaction. Refer to table below that identifies possible responses based on PIN processing conditions.
DE 48 (Additional Data—Private Use), TCC	C	•	C	Must contain the appropriate TCC code.
DE 48, subelement 80 (PIN Service Code)	C	•	C	Identifies whether the Authorization Platform attempted to verify or translate the PIN. Valid values: • PV = (The Authorization Platform verified the PIN)

## Program and Service Format Requirements

### PIN Processing for non-Europe Members

Data Element	Org	Sys	Dst	Values/Comments
				<ul style="list-style-type: none"><li>• TV = (The Authorization Platform translated the PIN for issuer verification)</li><li>• PI = (The Authorization Platform was unable to verify the PIN)</li><li>• TI = (The Authorization Platform was unable to translate the PIN)</li></ul>

Acquirer-related PIN processing errors, indicated by DE 39 (Response Code), value 30 (Format Error) and DE 44 (Additional Response Data) value 052 (DE 52 PIN Data), occur if the Authorization Platform is unable to decrypt the PIN data. Possible causes are:

- The PEK that the Authorization Platform and customer share is not synchronized. It should be the same key.
- The Authorization Platform is unable to determine the proper PEK because DE 32 or DE 33 is incorrect.
- The acquirer is not qualified to be in the MasterCard Magnetic Stripe Compliance Program.
- The acquirer did not correctly establish the static PEK or KEK with MasterCard.
- The DE 22, subfield 1 value is not valid for transactions that contain a PIN.

Following are possible Authorization Request Response/0110 message responses:

IF...	THEN...
The Authorization Platform on behalf of the issuer was unable to verify the PIN.	DE 39 = 55 (Invalid PIN) DE 48, subelement 80 (PIN Service Code) = PI
The Authorization Platform translated the PIN, but the issuer was unable to verify the PIN.	DE 39 = 55 DE 48, subelement 80 = TV
The Authorization Platform was unable to decrypt the PIN for the acquirer.	DE 39 = 30 (Format Error) DE 44 = 52DE 48, subelement 80 = TI
PIN processing was successful (verification or translation).	DE 39 = any valid code DE 48, subelement 80 = TV or PV
The Authorization Platform was unable to decrypt the PIN for the issuer.	DE 39 = 91 (Authorization Platform or issuer system inoperative) DE 48, subelement 80 = TI

## Issuer Requirements

Issuers must comply with the following to process MasterCard transactions that contain a PIN in Authorization Request/0100 messages:

- Receive purchase or ATM transactions that contain a PIN
- Support Static or Dynamic PEK Exchanges
- Process applicable data elements in Authorization Request/0100 Messages
- Process applicable data elements in Authorization Request Response/0110 Messages
- Process applicable data elements in Authorization Advice/0120-System Generated messages
- Process applicable data elements in Reversal Advice/0420-System Generated messages

### Receive Purchase Transactions that Contain a PIN

Issuers must be able to receive purchase transactions that contain a PIN using one of the following network options:

- Through a MasterCard Worldwide Network connection using Authorization Request/0100 messages
- The default method for issuers that currently receive their MasterCard ATM cash disbursement and ATM balance inquiry activity using this interface. Static PEKs that are already active and operational at the MDS will be used for each of the issuer's bank identification number (BIN)/card ranges.  
Issuers may choose to support dynamic PEK exchanges instead.
- Through a Single Message System connection using Financial Transaction Request/0200 messages.

The default method for issuers that currently receive their Debit MasterCard activity, ATM activity, or both using this interface. These transactions will be identified as "preauthorization requests" with a value 4 in position 7 of DE 61 because they must be cleared through the MasterCard Global Clearing Management System, with all other purchase activity. PEKs that already are active and operational at the MDS will be used for each of the issuer's BIN/card ranges.

### Support Static or Dynamic PEK Exchanges

For dynamic PEK exchanges, the Authorization Platform and the issuer must establish a new single KEK for all BINs that the issuer will process. This new KEK must be associated with the issuer's Member Group ID that the issuer uses for sign-on, sign-off and store-and-forward (SAF) sessions for the associated BINs. The issuer must complete the Customer-Initiated Key Part Exchange Form (536).

## Program and Service Format Requirements

### PIN Processing for non-Europe Members

---

Refer to the *Authorization Manual* for this form. **For increased security, MasterCard strongly recommends using dynamic PEKs.**

#### Authorization Request/0100—PIN Messages

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data—Private Use), TCC	M	•	M	Must contain the appropriate TCC code.
DE 48, subelement 80 (PIN Service Code)				This subelement contains the results of PIN processing as follows:  IF the issuer chooses to... THEN the Authorization Platform...  Use the MasterCard PIN Verification Service
				<ul style="list-style-type: none"><li>• Omits DE 52 from the Authorization Request/0100 message sent to the issuer.</li><li>• Sends DE 48, subelement 80, value PV (The Authorization Platform verified the PIN).</li><li>• If the PIN is invalid, the Authorization Platform sends the acquirer an Authorization Request Response/0110 message where DE 39 contains the value 55.</li></ul>
DE 52 (Personal ID Number (PIN) Data)	C	X	C	Will be present if the Authorization Platform does not perform PIN verification. The issuer verifies the PIN data in DE 52.  Either DE 45 or DE 35 will be present in the message to provide the PIN verification value (PVV) or offset, depending on the issuer's verification method.

IF...	THEN...
DE 52 is present	DE 48, subelement 80 is value TV
DE 52 is not present	DE 48, subelement 80 is value PV

### Authorization Advice/0120—PIN Messages

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Advice/0120 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data—Private Use), TCC	•	M	M	Must contain the appropriate TCC code.
DE 48, subelement 80 (PIN Service Code)				This subelement contains the results of PIN processing as follows:  IF the issuer chooses to... THEN the Authorization Platform...
				Have the Authorization Platform verify the PIN
				<ul style="list-style-type: none"> <li>• Omits DE 52 from the Authorization Advice/0120 message sent to the issuer.</li> <li>• Sends DE 48, subelement 80, value TI (The Authorization Platform was unable to translate the PIN).</li> </ul>
DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code)	•	M	M	107 (PIN Processing Error)
DE 60, subfield 2 (Advice Detail Code)	•	M	M	Provides additional details as follows: 0030 = (Reject: Unable to verify PIN data) 0031 = (Reject: Unable to decrypt/encrypt PIN data)

### Reversal Advice/0420—PIN Messages

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

The issuer must be able to receive Reversal Advice/0420 messages with DE 60 values in addition to all other applicable data elements.

## **Program and Service Format Requirements**

### **PIN Processing for non-Europe Members**

---

The Reversal Advice/0420 message identifies the corresponding Authorization Request Response/0110 message being reversed that contained PIN data.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code)	•	M	M	400 = (Banknet advice: APS error; unable to deliver response)
DE 60, subfield 2 (Advice Detail Code)	•	M	M	2000 = (Reject: PIN data present in Authorization Request/0100 message)

### **Alternate Processing**

The issuer may choose to have the Authorization Platform verify PIN data on their behalf. If the Authorization Platform performs PIN verification, it will perform Stand-In, Limit-1, and X-Code processing using the issuer or MasterCard existing authorization-qualifying criteria, when applicable.

If the Authorization Platform does not verify the PIN data and the issuer is unavailable or unable to process the Authorization Request/0100 message, the Authorization Platform will respond to the acquirer with an Authorization Request Response/0110 message indicating the issuer could not process the Authorization Request/0100 message, except in situations where an issuer chooses to allow transactions with unverified PINs in Stand-in processing.

### **Support for Both Acquiring and Issuing Processing**

Customers that support both acquiring and issuing authorization processing may use the same PEK for all purchase transactions that contain a PIN. To accomplish this, the customer must use the same member ID as follows:

- As the Member Group ID for establishing the static PEK or the KEK.
- In DE 32 or DE 33 in all acquired transactions.
- In DE 2 and DE 33 of the Network Management Request/0800—PEK Exchange—On Demand message.
- In DE 2 of the Network Management Request/0800—Group Sign-on message.

### **Cleartext Use Prohibited**

If there is a major problem with security equipment (for example, a faulty TRSM or DES circuit board), the Authorization Platform suspends all transaction processing with that customer. The customer must not send unencrypted (cleartext) PIN data.

#### **NOTE**

**MasterCard Operating Rules expressly prohibit use of cleartext processing of transactions.**

## Emergency Static PEK or Emergency KEK Process

Following are the stages of the emergency static PEK or KEK process.

1. MasterCard considers the faulty customer as “down.”
2. Authorized MasterCard personnel randomly generate both parts of an emergency static PEK or KEK.
3. MasterCard personnel call the security or operations staff of the customer. MasterCard gives the emergency static PEK or KEK verbally to the customer.
4. Both the MasterCard personnel and the customer insert the new emergency static PEK or KEK in their TRSMs.
5. The Authorization Platform initiates dynamic PEK exchange with a Network Management Request/0800—PEK Exchange, using the new emergency static PEK or KEK.

MasterCard and the customer are to use the emergency static PEK or KEK process only as an interim measure to get the customer up as quickly as possible following a key exchange failure. MasterCard limits the use of the emergency static PEK or KEK in any one occurrence to six business days. The customer must notify their security officers responsible for key management immediately of the security failure situation and must conduct a secure key exchange at the earliest possible time. For static PEK and KEK set-up process please refer to the *Authorization Manual*.

### Previous PEKs

After exchanging new PEKs statically or dynamically, the Authorization Platform and the customer are responsible for preserving the previous PEK for five minutes. They do this in the event that the current PEK becomes inoperative. If the current PEK has a Sanity Check error during this five-minute interval, the Authorization Platform or the customer should attempt to use the previous PEK. If the previous PEK is also inoperative, then refer to the steps previously discussed to determine action.

### PIN Verification Value on File Service

For issuers that use MDS for PIN-processing services and elect to use the PIN Validation in Stand-In service, MDS will perform the PIN validation service using the PVV for a card based on the PVV value provided in a file by the issuer.

Issuers that choose to register for this service must send a PVV/PIN Offset file to MDS to update cardholder PINs and must use MDS-managed security keys. A Customer Implementation Services specialist will assist issuers with setting up a file or adding new files for testing and production.

## **Program and Service Format Requirements**

### **PIN Processing for non-Europe Members**

---

Participating issuers must send a PVV/PIN Offset file to MDS to provide and update cardholder PIN information. This file must be sent using the secure Global File Transfer (GFT) methods approved by MasterCard. The following bulk file IDs have been established for use when submitting PVV/PIN Offset files: RM29 (Production), RM31 (MTF).

Issuers also must ensure that they have exchanged the PIN verification keys (PVKs) with MDS before using this service.

### **PVV/PIN Offset File Format**

The PVV/PIN Offset file has a fixed length of 64 characters. Issuers may use Bulk ID RM29 (Production), RM31 (MTF) or CONNECT:Direct to send the PVV/PIN Offset file to MasterCard. Refer to the following tables for information about the files header, detail, and trailer records.

#### **PVV/PIN Offset File Header Record**

<b>Field Name</b>	<b>Attribute</b>	<b>Length</b>	<b>Comments and Values</b>
Record Type ID	Alphanumeric	3	HDR—header record
File Version Number	Numeric	3	100 (initial version)
Customer ID	Alphanumeric	11	The first six digits must contain the issuers ICA with leading zeros. The seventh digit and beyond contains trailing spaces.
Transmission code	Alphanumeric	10	Member-assigned transmission code. May contain all spaces or zeros.
Transmission sequence	Numeric	4	0000–9999 Wraps at 9999
Transmission date	Numeric	6	YYMMDD in UTC
Transmission time	Numeric	6	hhmmss in UTC
Input file type	Alphanumeric	1	F = Full file replacement
Filler	Alphanumeric	20	Spaces

#### **PVV/PIN Offset File Detail Record**

<b>Field Name</b>	<b>Attribute</b>	<b>Length</b>	<b>Comments and Values</b>
Record Type ID	Alphanumeric	3	DTL = detail record
Update code	Alphanumeric	1	A = add/update
PAN	Alphanumeric	19	With trailing spaces

## Program and Service Format Requirements

### PIN Processing for non-Europe Members

---

Field Name	Attribute	Length	Comments and Values
Card expiry date	Numeric	4	YYMM (must contain a valid year and month)
Card sequence number	Numeric	1	Values can be in the range of 0-9 Must contain the Sequence Number associated with the PAN or 0. A value of 0 indicates that the card sequence number should not be used as criteria when matching to the PVV file.
PVV/PIN Offset	Numeric	6	Trailing spaces
Filler	Alphanumeric	30	Spaces

### **PVV/PIN Offset File Trailer Record**

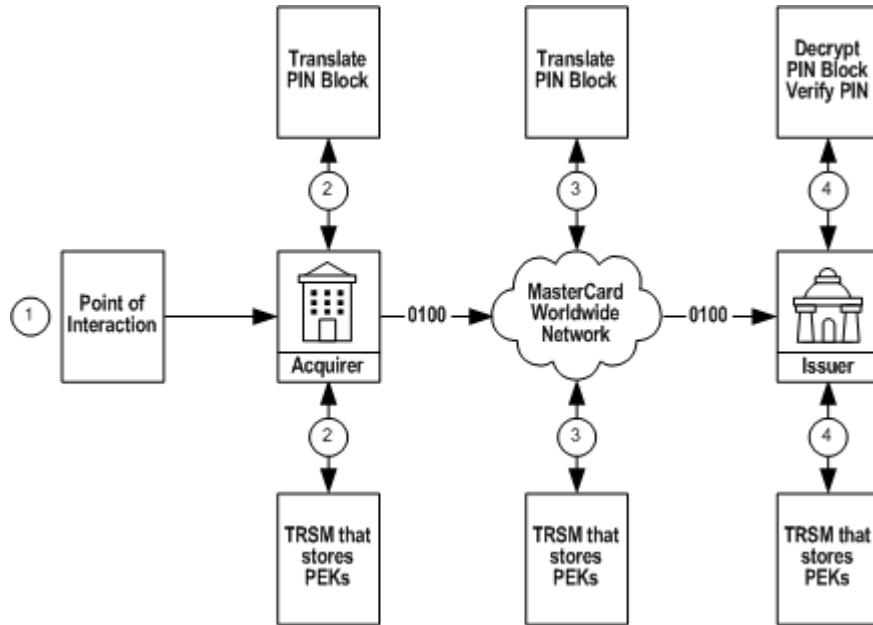
Field Name	Attribute	Length	Comments and Values
Record type ID	Alphanumeric	3	TRL = trailer record
Number of detail records	Numeric	11	Detail record count
Filler	Alphanumeric	50	Spaces

### **Alternate Processing**

In instances where Stand-In processing is not accessible, X-Code processing is initiated. X-code processing does not perform PIN verification. Therefore, authorization requests received with an unverified PIN will be declined.

## PIN Translation and Verification Process

This message flow describes the key exchanges during the PIN translation and verification process.



1. The cardholder enters the PIN at the point of interaction. The PIN is encrypted by the terminal's hardware under a PIN encryption key and is then sent to the acquirer.
2. The acquirer receives the encrypted PIN, which the acquirer then decrypts using the terminal PEK stored in a TRSM. The acquirer then creates the ANSI PIN block and encrypts it using the DES algorithm as follows:

**First Block—PIN Data:** The first digit of this block contains the control character 0, followed by a number representing the PIN length (maximum 12), and then the PIN itself. The acquirer then fills the remaining digits of the block on the right with hexadecimal F's to complete the 16-digit account number.

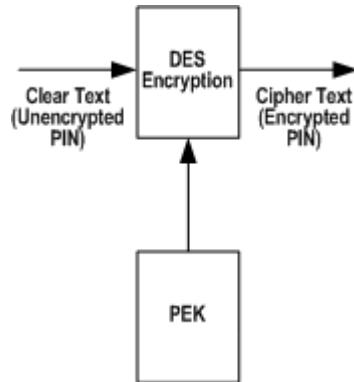
**Second Block—PAN Data:** The first four digits of the second block contain 0000, followed by the 12 right-most digits of the PAN, excluding the check digit. The acquirer then pads zeros to the left to complete the 16-digit data element.

In formatting an ANSI block, the acquirer performs an XOR function on the two 16-digit blocks.

After creating the PIN block, the acquirer sends it through the DES algorithm along with the 16-digit PEK that the acquirer and the Authorization Platform share, producing the translated PIN block as follows. The acquirer may encrypt the PIN using:

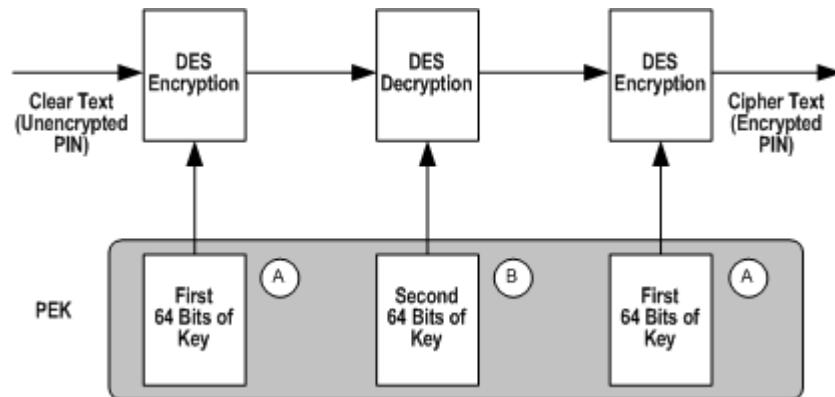
- a. Single DES algorithm

Encrypt PIN information using a single DES key algorithm with single-length PEKs as follows:



- b. Triple DES algorithm with double length PEKs

Encrypt PIN information using a triple DES key algorithm with double-length PEKs as follows:<sup>5</sup>



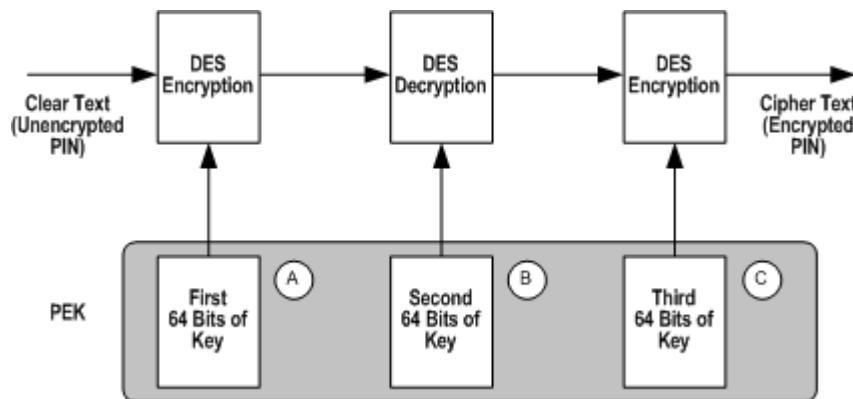
- c. Triple DES algorithm with triple length PEKs

Encrypt PIN information using a triple DES key algorithm with triple-length PEKs as follows:<sup>6</sup>

- 
- 5. When a customer chooses to support triple DES, the customer must support both sending and receiving double-length (16-byte) PEKs.
  - 6. When a customer chooses to support triple DES, the customer must support both sending and receiving double-length (16-byte) PEKs.

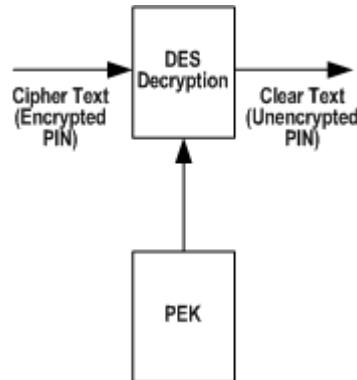
## Program and Service Format Requirements

### PIN Processing for non-Europe Members



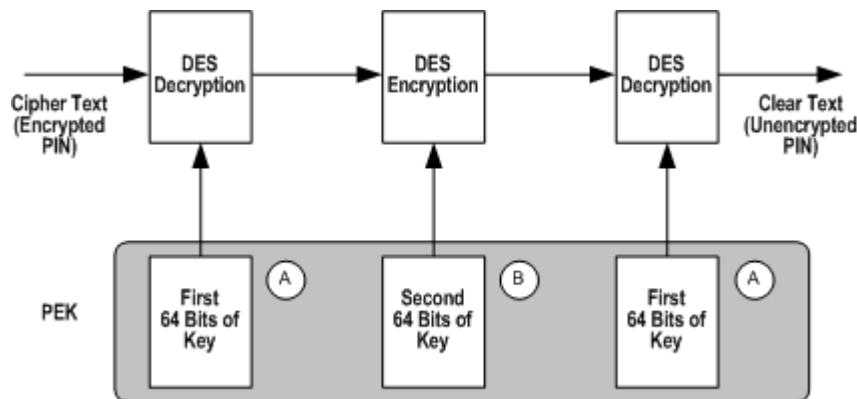
3. The acquirer sends the translated PIN block to the Authorization Platform. The Authorization Platform translates it from the acquirer PEK to the issuer PEK using the procedures described in step 2. The Authorization Platform then sends the translated PIN block to the issuer for verification.<sup>7</sup>
4. The issuer then translates the PIN block and verifies the PIN using:
  - a. Single DES algorithm

Decrypt PIN information using a single DES key algorithm with single-length PEKs as follows:



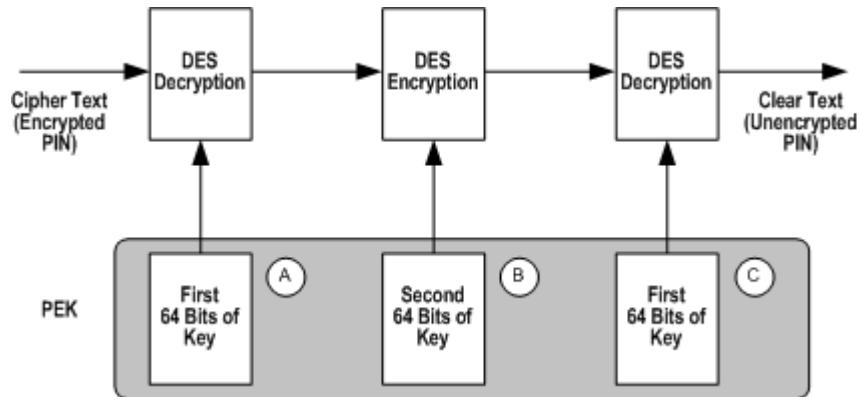
- b. Triple DES algorithm with double length PEKs
- Decrypt PIN information using a triple DES key algorithm with double- or triple-length PEKs as follows:

7. DE 52 (PIN Data) is not in the Authorization Request/0100 message going to the issuer if the Authorization Platform is performing PIN verification on the issuer's behalf.



- c. Triple DES algorithm with triple length PEKs

Decrypt PIN information using a triple DES key algorithm with triple-length PEKs as follows:



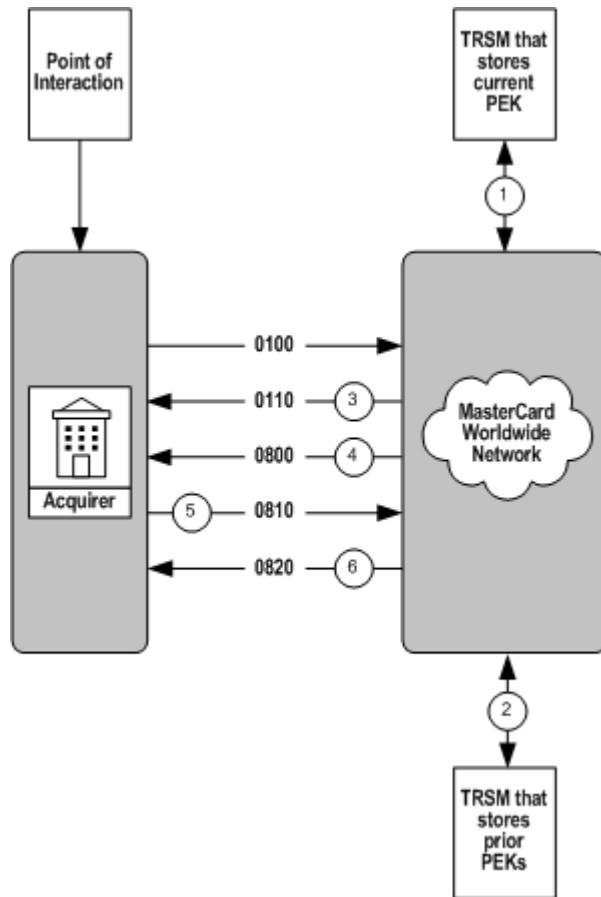
### **Detection of PEK Corruption Using Sanity Checks**

Issuers and the Authorization Platform perform Sanity Checks on PIN blocks as part of the PIN encryption/decryption process. This subsection describes Sanity Check errors that indicate PEK out-of-synchronization conditions that may occur during PIN decryption. It also explains ensuing steps that the Authorization Platform and customer take.

All Tamper Resistant Security Modules (TRSMs) must be able to detect possible corruption of PEKs by performing Sanity Checks on the PIN block as part of decryption. When Sanity Check errors occur, customers should use the following procedures to resolve the problem.

## Authorization Platform Sanity Check Error

This flow describes the process when the Authorization Platform TRSM discovers a PEK or KEK error.



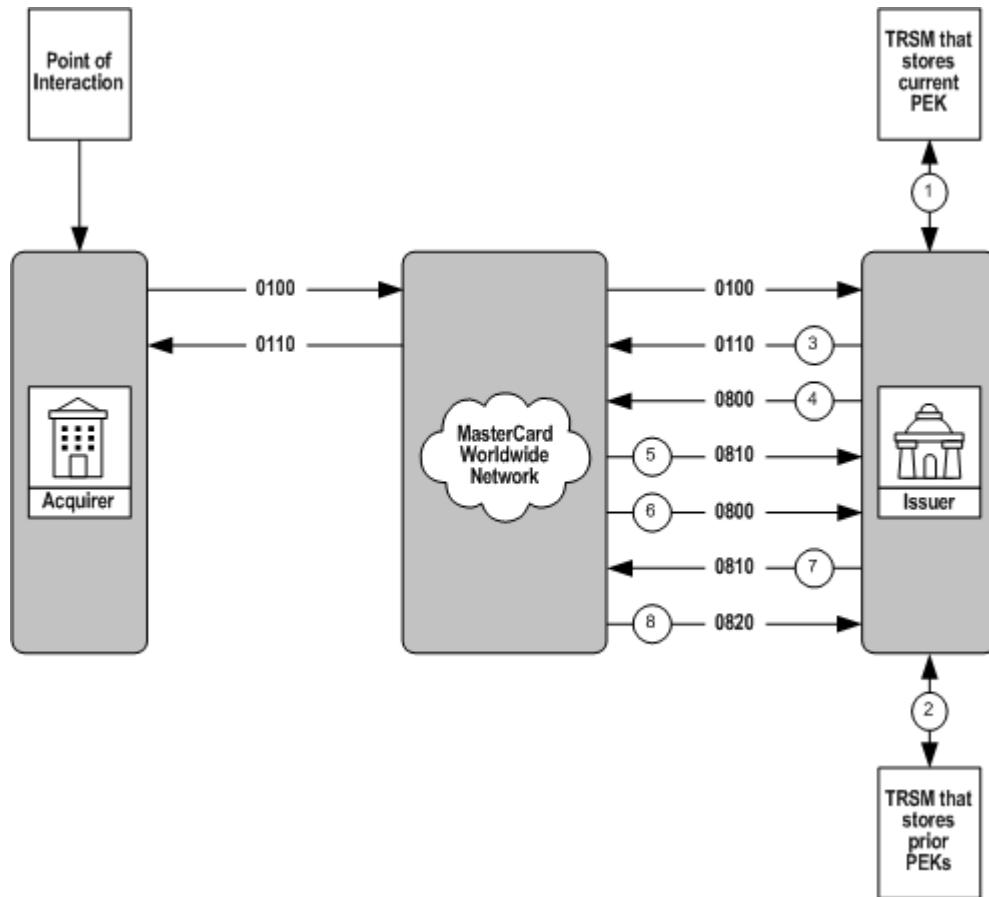
1. The Authorization Platform's Sanity Check reveals an out-of-synchronization condition with the PEK that it shares with the acquirer.
2. If five consecutive transactions fail the Sanity Check, and the Authorization Platform has performed steps 1–3 with each of the previous five transactions from the acquirer, the Authorization Platform takes the following action:
  - For a **static PEK**, MasterCard starts emergency procedures to create a new static PEK.
  - For a **dynamic PEK**, the Authorization Platform sends the acquirer a Network Management Request/0800—PEK Exchange message with a new PEK. If there are problems with the new PEK, the Authorization Platform will initiate procedures to establish a new KEK.
3. For a **dynamic PEK**, the acquirer sends a Network Management Request Response/0810—PEK Exchange to the Authorization Platform acknowledging receipt of the Network Management Request/0800—PEK Exchange message exchanging the PEK. If the message does not contain

a DE 39 value of 00—completed successfully—the Authorization Platform sends another Network Management Request/0800—PEK Exchange message.

4. For a **dynamic PEK**, the Authorization Platform sends a Network Management Advice/0820—PEK Exchange message to the acquirer that notifies the customer that the new PEK is active and operational. Subsequent Authorization Request/0100 messages must use the new PEK to encrypt the PIN in DE 52.

### Issuer Sanity Check Error

The Issuer TRSMs must be able to detect possible corruption of PEKs. This process flow describes the process when the issuer TRSM discovers a PEK error using a Sanity Check.



1. The issuer's Sanity Check reveals an out-of-synchronization condition with the PEK that it shares with the Authorization Platform.
2. The issuer attempts to decrypt the PIN block using the **prior** PEK, if available.
3. If the Sanity Check fails using the **prior** PEK, the issuer sends an Authorization Request Response/0110 message.
4. If five consecutive transactions fail the Sanity Check, and the issuer has performed steps 1–3 with each of the five transactions, the issuer takes the following appropriate action:
  - For a **static PEK**, the issuer contacts MasterCard to start emergency procedures to create a new static PEK.
  - For a **dynamic PEK**, the issuer sends the Authorization Platform a Network Management Request/0800—PEK Exchange—On Demand

message to create a new PEK. If there are problems with the new PEK, the issuer contacts MasterCard to start emergency procedures to establish a new KEK.

5. For a **dynamic PEK**, the Authorization Platform acknowledges receipt of the request by sending a Network Management Request Response/0810—PEK Exchange message.
6. For a **dynamic PEK**, the Authorization Platform sends to the issuer a Network Management Request/0800—PEK Exchange message with a new PEK.
7. For a **dynamic PEK**, the issuer sends a Network Management Request Response/0810—PEK Exchange message to the Authorization Platform acknowledging receipt of the Network Management Request/0800—PEK Exchange message exchanging the PEK. If the message does not contain a DE 39 value of 00—completed successfully—the Authorization Platform sends another Network Management Request/0800—PEK Exchange message.
8. For a **dynamic PEK**, the issuer receives a Network Management Advice/0820—PEK Exchange message from the Authorization Platform that notifies the customer that the new PEK is active and operational. Subsequent Authorization Request/0100 messages must use the new PEK to encrypt the PIN in DE 52.

## Private Label Processing

Under the MasterCard Private Label Program, private label issuers use MasterCard account ranges. The use of a MasterCard account range on an approved private label program facilitates the seamless switching of private label transactions via the four-party model (issuer, acquirer, merchant, MasterCard). To make sure that only participating private label merchants are allowed to accept these private label cards, transaction verification may optionally be enabled so that non-participating merchants' transactions are not approved.

MasterCard Private Label card programs will use MasterCard or Maestro BIN ranges.

## Authorization Request/0100—Private Label Processing

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 63 (Network Data), subfield 1 (Financial Network Code)	•	X	M	A valid private label financial network code.

## Program and Service Format Requirements

### Private Label Processing

---

#### Authorization Platform Edits

The Authorization Platform will perform the following edit.

WHEN DE 48, subelement 32 is present and...	THEN the Authorization Platform...
The length of the MasterCard Assigned ID is less than six digits in the Authorization Request/0100, Authorization Advice/0120—System-generated, and Reversal Request/0400 message	Sends the acquirer an Authorization Request/0110, Authorization Advice Response/0130 or Reversal Response/0410 message where: DE 39 = 30 (Format Error) DE 44 = 048

#### Private Label with Balance Inquiry

MasterCard provides private label issuers to allow their cardholders the ability to request a balance inquiry on their private label card at the point of sale (POS).

Private label issuers that want to offer Private Label balance inquiry at the POS must support balance inquiries at the POS as described in [Balance Inquiry—Point-of-Sale](#).

For information about participation in the balance inquiry service, see the *Authorization Manual*.

#### Authorization Request/0100—Private Label with Balance Inquiry

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code)	M	•	M	30 = Balance Inquiry
DE 63 (Network Data), subfield 1 (Financial Network Code)	•	X	M	A valid private label financial network code.

#### Merchant Verification Service

Private Label Merchant Verification is an optional service available to issuers for their private label programs. However, this is a mandatory service for issuers that participate in the MasterCard Co-Brand Proprietary Transaction Management Service and that process under the MasterCard Private Label program.

The Authorization Platform evaluates each Authorization Request/0100 message to determine whether the account participates in the Private Label Merchant Verification services. If the account participates in Private Label Merchant Verification, the Authorization Platform validates whether the transaction occurred at a participating merchant location.

The Authorization Platform validates the merchant in DE 42 (Card Acceptor ID Code) or DE 48 (Additional Data—Private Use), subelement 32 (MasterCard Assigned ID) to ensure that the transaction occurred at a participating private label merchant location.

- If the participating private label merchant is validated against the merchant registration database, the Authorization Platform populates DE 63, subfield 1 with the Private Label product code and forwards the Authorization Request/0100 message to the issuer for approval.
- If the participating merchant cannot be validated, the Authorization Platform rejects the transaction and sends the acquirer an Authorization Request Response/0110 message where DE 39 (Response Code) = 58 (Transaction not permitted to acquirer/terminal). Also, if the Authorization Platform declines the private label transaction because the transaction did not occur at the participating private label merchant location, the Authorization Platform sends the issuer an Authorization Advice/0120 message. DE 60 (Advice Reason Code) contains new value in Subfield 1 (Advice Reason Code = 116) and subfield 2 (Advice Detail Code = 0116)

**NOTE**

**The Private Label Merchant Verification service is not performed on Authorization Advice/0120 and Reversal Request/0400 messages.**

Issuers will use the information provided in the Reversal Request/0400 message to reverse the original Authorization Request/0100 message. The product code provided in DE 63, subfield 1 may be different in the Reversal Request/0400 message than in the Authorization Request/0100 message.

### **Authorization Platform Edits**

The Authorization Platform will perform the following edits on Private Label Merchant Verification Service.

---

<b>WHEN the issuer is set up for Private Label Merchant Verification Service and...</b>	<b>THEN the Authorization Platform...</b>
The account range is set up as private label, but DE 42 (Card Acceptor ID Code) or DE 48 (Additional Data—Private Use) subelement 32 (MasterCard Assigned ID) in Authorization Request/0100 message does not find a match	Rejects the transaction and sends the Authorization Request Response/0110 to the acquirer where: DE 39 = 58 (Transaction not permitted to acquirer or terminal) DE 44 = 042

---

### **Co-brand Proprietary Transaction Management Service**

The Co-brand Proprietary card program allows customers to use account ranges for the card product that can be both private label and MasterCard brand.

## **Program and Service Format Requirements**

### **Private Label Processing**

---

#### **NOTE**

**Europe private label issuers are not eligible for this service.**

For transactions originating from co-brand proprietary cards, the Co-brand Proprietary Transaction Management Service seamlessly determines whether the transaction occurred at the co-brand partner's merchant location and, if so, places the appropriate private label product code in the Authorization Request/0100 message before routing the transaction to the issuer for approval. The transaction must adhere to MasterCard Private Label product standards. If the transaction did not occur at the participating merchant location, the Authorization Platform populates the MasterCard brand product in the Authorization Request/0100 message before routing the transaction to the issuer for approval. The transaction must adhere to all applicable MasterCard standards.

The co-brand proprietary account range participating in the Co-brand Proprietary Transaction Management Service must also participate in the Private Label Merchant Verification Service. Cardholder accounts within the co-brand card program may optionally participate in Account Level Management. Issuers must adhere to the current Account Level Management processing rules and must register individual accounts according to Account Level Management guidelines. To learn more about participating in Account Level Management, customers should contact their Technical Account Manager.

Co-Brand Proprietary Transaction Management Service leverages the existing Account Level Management functionality. Issuers that participate in the Co-brand Proprietary card program or Account Level Management must be prepared to receive the account category value in DE 48 (Additional Data—Private Use), subelement 38 (Account Category) of the Authorization Request/0100 message.

- The account category value P indicates that the cardholder account participates in either Account Level Management Product Graduation or the Co-brand card program.
- Account category values B and M are associated only with Account Level Management.

Issuers must look at the DE 48 (Additional Data—Private Use) subelement 38 (Account Category Code) in Authorization Request/0100 message and, if approved, must move the value to DE 38 position 6 of the Authorization Response/0110 message.

Acquirers must look at DE 38 (Authorization ID Response), position 6 for the account category code value and DE 63 (Network Data), subfield 1 (Financial Network Code) in the Authorization Request Response/0110 message to determine how to submit the transaction to clearing.

The Authorization Platform validates the merchant in DE 42 (Card Acceptor ID Code) or DE 48 (Additional Data—Private Use), subelement 32 (MasterCard Assigned ID) to ensure that the transaction occurred at a participating private label merchant location or not in the following order:

- If the participating private label merchant is validated against the merchant registration database, the Authorization Platform populates DE 63, subfield 1 with the Private Label product code and DE 48, subelement 38 (Account Category) with the value P (Account qualifies for MasterCard Product Graduation or Co-brand Proprietary card program).
- If the transaction cannot be validated as originating from the co-brand partner's merchant location, the Authorization Platform determines whether the cardholder account participates in Account Level Management. If yes, the Authorization Platform populates DE 63, subfield 1 and DE 48, subelement 38 according to Account Level Management processing.
- If the transaction does not occur at a private label merchant location and the cardholder account does not participate in Account Level Management, the Authorization Platform forwards the transaction to the issuer with DE 63, subfield 1 = MasterCard brand product code associated with the account range and DE 48, subelement 38 = P.

Please refer to *Authorization Manual* for details about the Private Label Processing.

#### **NOTE**

**Failure to include the category code in DE 38, position 6 on the approved authorization will cause the authorization request to be routed to and processed by the Stand-In System.**

### **Alternate Processing**

Stand-In processing supports the Co-brand Proprietary Transaction Management System. Stand-In processing uses the product code in DE 63 (Network Data), subfield 1 (Financial Network Code), instead of the product code associated with the authorization account range when applying Stand-In limits at the product code level.

Stand-In processing will also ensure that DE 38 (Authorization ID Response), position 6 in the Authorization Request Response/0110 message contains the value provided by the Authorization Platform in DE 48 (Additional Data—Private Use), subelement 38 (Account Category) of the Authorization Request/0100 message.

### **Card Activation for Private Label Processing**

Private Label enables issuers to allow consumers buying their Private Label prepaid card to activate them when purchased at the merchant location. This limits risks for the merchants as their Private Label cards (on display for sale and already loaded with a predefined amount) will be activated only when purchased.

## Program and Service Format Requirements

### Private Label Processing

---

#### Authorization Request/0100 and Reversal Request/0400—Card Activation at Point of Sale

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 and Reversal Request/0400 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code, subfield 1 (Transaction Type))	M	•	M	Must be value 28 (Payment Transaction)
DE 4, (Amount, Transaction)	M	•	M	Must be zero
DE 18 (Merchant Type)	M	•	M	Must contain a value <b>other</b> than 6010 (Member Financial Institution—Manual Cash Disbursement) or 6011 (Member Financial Institution—Automated Cash Disbursements)
DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	M	•	M	<p>Must contain one of the following values:</p> <ul style="list-style-type: none"><li>• 02 = PAN entry mode unknown</li><li>• 05 = PAN auto-entry via chip</li><li>• 07 = PAN auto-entry via contactless M/Chip</li><li>• 80 = Chip card at chip-capable terminal was unable to process transaction using data on the chip; therefore, the terminal defaulted to the magnetic stripe-read PAN. The full track data has been read from the data encoded on the card and transmitted within the Authorization Request/0100 in DE 45 (Track 1 Data) or DE 35 (Track 2 Data) without alteration or truncation. To use this value, the acquirer must be qualified to use value 90.</li><li>• 90 = PAN auto-entry via magnetic stripe—The full track data has been read from the data encoded on the card and transmitted within the authorization request in DE 35 (Track 2 Data) or DE 45 (Track 1 Data) without alteration or truncation.</li><li>• 91 = PAN auto-entry via contactless magnetic stripe—The full track data has been read from the data on the card and transmitted within the authorization request in DE 35 (Track 2 Data) or DE 45 (Track 1 Data) without alteration or truncation.</li></ul>

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	Must contain value P
DE 48 (Additional Data—Private Use), subelement 77 Payment Transaction Type Indicator)	C	•	C	Must contain value C09 (Card Activation)
DE 61 (Point of Sale [POS] Data), subfield 1 (POS Terminal Attendance)	M	•	M	Must contain value 0 (Attended Terminal)
DE 61 (Point of Sale [POS] Data), subfield 3 (POS Terminal Location)	M	•	M	Must contain value 0 (On premises of card acceptor facility)
DE 61 (Point of Sale [POS] Data), subfield 4 (POS Cardholder Presence)	M	•	M	Must contain value 0 (Cardholder present)
DE 61 (Point of Sale [POS] Data), subfield 5 (POS Card Presence)	M	•	M	Must contain value 0 (Card present)
DE 61 (Point of Sale [POS] Data), subfield 10 (Cardholder-Activated Terminal [CAT] Level)	M	•	M	Must contain value 0 (Not a CAT transaction)

## Alternate Processing

Private Label prepaid card activation transactions are not eligible for alternate (Stand-In or alternate issuer host routing) or X-Code processing. If the primary issuer is not available to respond to a card activation request, an Authorization Request Response/0110 is returned to the acquirer with DE 39 (Response Code) value 91 (Authorization Platform or issuer system inoperative).

If the issuer is not available to respond to a reversal of a card activation request, a Reversal Request Response/0410 is returned to the acquirer with DE 39 (Response Code) value 00 (Approval) and the issuer receives notification of the response the Authorization Platform provided on their behalf in a Reversal Advice/0420 message.

## **Program and Service Format Requirements**

### **Private Label Processing**

---

#### **Authorization Platform Edits**

The Authorization Platform will perform the following edits for Authorization Request/0100 and Reversal Request/0400 messages.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) contains value 28 (Payment Transaction), and DE 48 (Additional Data—Private Use), subelement 77 (Payment Transaction Type Indicator), contains value C09 (Card Activation) and DE 61 (Point of Sale [POS] Data) subfields does not contain the following values:</p> <ul style="list-style-type: none"><li>• Subfield 1 (POS Terminal Attendance) = 0 (Attended Terminal)</li><li>• Subfield 3 (POS Terminal Location) = 0 (On premises of card acceptor facility)</li><li>• Subfield 4 (POS Cardholder Presence) = 0 (Cardholder present)</li><li>• Subfield 5 (POS Card Presence) = 0 (Card present)</li><li>• Subfield 10 (Cardholder-Activated Terminal [CAT] Level) = 0 (Not a CAT transaction)</li></ul>	<p>The Authorization Platform declines the request with a format error response where: DE 39 (Response Code) = 30 DE 44 (Response Data) = 061</p>
<p>DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) contains value 28 (Payment Transaction), and DE 48 (Additional Data—Private Use), subelement 77 (Payment Transaction Type Indicator), contains value C09 (Card Activation) and DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) does not contain one of the following values:</p> <ul style="list-style-type: none"><li>• 02 = PAN entry mode unknown</li><li>• 05 = PAN auto-entry via chip</li><li>• 07 = PAN auto-entry via contactless M/Chip</li></ul>	<p>The Authorization Platform declines the request with a format error response where: DE 39 (Response Code) = 30 DE 44 (Response Data) = 022</p>

WHEN...	THEN the Authorization Platform...
<ul style="list-style-type: none"><li>• 80 = Chip card at chip-capable terminal was unable to process transaction using data on the chip; therefore, the terminal defaulted to the magnetic stripe-read PAN. The full track data has been read from the data encoded on the card and transmitted within the Authorization Request/0100 in DE 45 (Track 1 Data) or DE 35 (Track 2 Data) without alteration or truncation. To use this value, the acquirer must be qualified to use value 90.</li><li>• 90 = PAN auto-entry via magnetic stripe—the full track data has been read from the data encoded on the card and transmitted within the authorization request in DE 35 (Track 2 Data) or DE 45 (Track 1 Data) without alteration or truncation.</li><li>• 91 = PAN auto-entry via contactless magnetic stripe—the full track data has been read from the data on the card and transmitted within the authorization request in DE 35 (Track 2 Data) or DE 45 (Track 1 Data) without alteration or truncation.</li></ul>	

## Card Activation Plus Initial Load for Private Label Processing

Private label acquirer and issuers can use the Card Activation Plus Initial Load service to provide their cardholders the ability to set the amount to load on their private label prepaid card at the moment of purchase and activation at the point-of-sale (POS) terminal.

For private label prepaid cards, the Authorization Platform can process one transaction for both activating and initially loading a card.

The Authorization Platform will allow a valid amount in DE 4 (Transaction Amount) for private label prepaid card activation authorization messages.

### Acquirer Processing

- Acquirers that want to offer the private label card activation plus initial load functionality must support Authorization Request/0100 and Reversal Request/0400 messages containing DE 48 (Additional Data—Private Use),

## **Program and Service Format Requirements**

### **Product Inquiry Service**

---

subelement 77 (Payment Transaction Type Indicator), value C09 (Payment Transaction Type Indicator).

- Acquirers already supporting private label card activation at POS functionality and wanting to offer card activation plus initial load must send Authorization Request/0100 and Reversal Request/0400 messages containing DE 4 (Amount, Transaction) with a valid amount and DE 48, subelement 77, value C09.
- Acquirers must submit Reversal Request/0400 messages for the full amount when reversing card activation plus initial load messages. Acquirers must ensure that DE 95 (Replacement Amounts) is not present in Reversal Request/0400 messages or, if present, that DE 95, subfield 1 (Actual Amount, Transaction) contains an amount equal to zero.

### **Issuer Processing**

- Issuers that want to offer the private label card activation plus initial load functionality must support Authorization Request/0100 and Reversal Request/0400 messages containing DE 48 (Additional Data—Private Use), subelement 77 (Payment Transaction Type Indicator), value C09 (Payment Transaction Type Indicator).
- Private label card issuers already supporting private label card activation at POS requests and wanting to offer card activation plus initial load must be able to accept Authorization Request/0100 and Reversal Request/0400 messages where DE 4 contains a valid amount, DE 6 (Amount, Cardholder Billing), and optionally DE 5 (Amount, Settlement), and DE 48, subelement 77 is C09.

## **Product Inquiry Service**

The Product Inquiry Service allows acquirers to send a product inquiry authorization request message to MasterCard.

As part of the authorization response to an acquirer, MasterCard will supply an acquirer with the product code associated with the particular MasterCard card number. Additionally, since the product codes for MasterCard® Standard Card, Gold MasterCard® Card, Platinum MasterCard® Card, or World MasterCard® Card programs potentially fall under different possible interchange rate structures, MasterCard also will populate the authorization response message with the applicable account category code as defined by the Account Level Management Service.

The information received by the acquirer through a Product Inquiry Service request, together with the published MasterCard interchange rate schedule and rate criteria, can be used by an acquirer and merchant to determine the product and associated interchange rate that may be applied to a purchase transaction for that particular card.

## Authorization Request/0100—Product Inquiry Service

Following is the list of the data elements applicable to this message. All mandatory Authorization Request/0100 data elements apply.

Data Element ID and Name	Org	Sys	Dst	Comments
4 Amount, Transaction	M	•	M	Transaction amount of zero, in the acquirer's currency, at the point of interaction.
61 Point-of-Service (POS) Data, subfield 7 (POS Transaction Status), Value 8 (Account Status Inquiry Service)	M	•	M	

## Proximity Payments

The MasterCard Proximity Payments solution, which includes *PayPass™* mag stripe and *PayPass™* M/Chip, is part of the global Proximity Payments Program and is designed to enrich the traditional card with a new contactless interface.

The contactless interface provides cardholder and merchant benefits that are particularly relevant in environments such as:

- Unattended point-of-service (POS) devices (for example, gas pumps and vending machines)
- High-traffic venues (for example, quick service and drive-through restaurants)

Proximity payments do not require cardholders holding a contactless MasterCard chip card to "swipe" or insert the card into a card reader or terminal. Instead, cardholders place the contactless card in "proximity" of a specially equipped merchant terminal to make a payment.

### For More Information

For more information about MasterCard® *PayPass™*, see [PayPass Mapping Service for PayPass M/Chip and Contact M/Chip Transactions](#) and [PayPass CVC 3 Processing Service](#).

## Authorization Request/0100—Proximity Payments

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

## **Program and Service Format Requirements**

### **Proximity Payments**

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 22 (Point-of-Service (POS) Entry Mode), subfield 1 POS Terminal PAN Entry Mode)	M	•	M	<p>Contains one of the following values:</p> <ul style="list-style-type: none"><li>• 07 = PAN auto-entry via contactless M/Chip</li><li>• 91 = PAN auto-entry via contactless magnetic stripe—the full track data has been read from the data on the card and transmitted within the Authorization Request/0100 message in DE 35 (Track 2 Data) or DE 45 (Track 1 Data) without alteration or truncation.</li></ul>
DE 61 (Point-of-Service (POS) Data), subfield 11 (POS Card Data Terminal Input)	M	•	M	<p>Contains one of the following values:</p> <ul style="list-style-type: none"><li>• 3 = Contactless M/Chip</li><li>• 4 = Contactless Magnetic Stripe</li></ul>

## Purchase of Goods or Services with Cash Back

MasterCard allows the use of Purchase of Goods or Services with Cash Back in Authorization/01xx and Reversal/04xx messages for Debit MasterCard and Maestro cards.

### Participation Mandate

All issuers of Debit MasterCard and Maestro cards are required to support the receipt of authorization and reversal requests for Purchase of Goods or Services with Cash Back transactions. The Purchase of Goods or Services with Cash Back service is automatically associated with all Debit MasterCard and Maestro account ranges.

Issuers will continue to approve or decline Purchase of Goods or Services with Cash Back transactions at their discretion.

### Terminal Support Indicator

The Authorization Platform allows acquirers to indicate whether the merchant terminal supports receipt of the purchase amount only approval response code in an authorization message.

The Authorization Request/0100 message must contain DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 09 (Purchase with Cash Back) and DE 48 (Additional Data—Private Use), subelement 61 (POS Data, Extended Condition Codes), subfield 2 (Purchase Amount Only Terminal Support Indicator), value 1 (Merchant terminal supports receipt of purchase-only approval).

## Authorization Request/0100—Purchase of Goods or Services with Cash Back

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	M	•	M	Must contain value 09 = Purchase of Goods or Services with Cash Back
DE 4 (Amount, Transaction)	M	•	M	Must contain the transaction amount, inclusive of the amount cash back.
DE 48, (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	

## Program and Service Format Requirements

### Purchase of Goods or Services with Cash Back

Data Element	Org	Sys	Dst	Values/Comments
DE 48, subelement 61 (POS Data, Extended Condition Codes), subfield 2 (Partial Approval Terminal Support Indicator)	C	•	C	1 = Merchant terminal supports receipt of purchase only approvals
DE 54 (Additional Amounts), subfield 1 (Account Type)	M	X	M	The Authorization Platform provides a second occurrence of DE 54 to the issuer if billing currency is different than transaction currency. Must contain one of the following values: 00 = Default account (not specified or not applicable) 10 = Savings Account 20 = Checking Account
DE 54, subfield 2 (Amount Type)	M	X	M	40 = Amount Cash Back
DE 54, subfield 3 (Currency Code)	M	X	M	Must contain the valid three-digit numeric value present in DE 49 (Currency Code, Transaction)
DE 54, subfield 4 (Amount)	M	X	M	D = (Debit amount) plus 12 digits right justified with leading zeros

### Issuer Response Options

Issuers have several options in how they respond to a Purchase of Goods or Services with Cash Back request.

When the issuer receives an Authorization Request 0100/message containing DE 48 (Additional Data—Private Use), subelement 61 (POS Data, Extended Condition Codes), subfield 2 (Purchase Amount Only Terminal Support Indicator), value 1 (Merchant terminal supports receipt of purchase only approvals), the issuer has the option to:

- Approve the entire transaction amount,
- Decline the entire transaction amount, or
- Respond with a purchase amount only approval. The issuer must approve the entire purchase amount, partial approval (DE 39, value 10) of the purchase amount is not allowed.

The following table describes the information that the issuer must provide in the Authorization Request Response/0110 message when responding with a purchase-only approval and the information that the acquirer will receive for a purchase-only approval.

The Issuer must provide...	The Acquirer will receive...
<p>The approved amount (purchase amount) in DE 6 (Amount, Cardholder Billing) in the issuer's cardholder billing currency. This amount must be the purchase amount as calculated by subtracting the DE 54 cash back amount from the DE 6 amount present in the Authorization Request/0100 message in the amount data element that corresponds to the issuer's cardholder billing currency.</p> <p>DE 38 (Authorization ID Response)</p> <p>DE 39 value 87 (Purchase only, no cash back allowed)</p> <p>DE 51 (Currency Code, Cardholder Billing) with the issuer's cardholder billing currency code</p>	<p>The purchase-only approval amount in the acquirer's transaction currency in DE 4</p> <p>DE 38</p> <p>DE 39, value 87</p> <p>An occurrence of the original amount of the transaction in DE 54 (Additional Amounts) in the acquirer's transaction currency. The original amount is identified by DE 54, subfield 2 (Amount Type), value 57 (Original Amount), and subfield 4 (Amount), value C plus 12-digit original amount.</p> <p>An occurrence of the original amount of the transaction in DE 54 in the issuer's cardholder billing currency. The original amount is identified by DE 54, subfield 2, value 57, and subfield 4, value C plus 12-digit original amount.</p>

**NOTE**

**Issuers responding with DE 39, value 87 will not be required to echo DE 4 (Amount, Transaction) in the Authorization Request Response/0110. Likewise, if DE 5 (Amount, Settlement) was present in the Authorization Request/0100 message to the issuer, the issuer will not be required to echo DE 5 in the Authorization Request Response/0110 when responding with DE 39, value 87. The issuer will provide the purchase-only approval amount in DE 6 and the issuer currency code in DE 51.**

## Reversal Request/0400

In some cases, the cardholder or merchant may elect not to complete the transaction after receiving the purchase-only approval response from the issuer. MasterCard supports full reversal messages to allow the merchant to cancel the transaction.

In addition to all other applicable data elements for the Reversal Request/0400 message, acquirers should submit Reversal Request/0400 messages with the following data elements for a reversal of a purchase-only approval:

- Purchase-only approval amount in DE 4 that was present in the Authorization Request Response/0110 message to the acquirer, not the original amount present in DE 4 of the Authorization Request/0100 message from the acquirer
- DE 39, value 87

The Authorization Platform will perform currency conversion if appropriate and will provide the following data elements in the Reversal Request/0400 message to the issuer:

## **Program and Service Format Requirements**

### **Purchase of Goods or Services with Cash Back**

---

- Purchase-only approval amount in DE 4 in the acquirer's transaction currency
- Purchase-only approval amount in DE 5 in U.S. dollars if the issuer has opted to receive this data element in the message
- Purchase-only approval amount in DE 6 in the issuer's cardholder billing currency
- DE 39, value 87

When processing a Reversal Request/0400 for a purchase-only approval (DE 39, value 87), the issuer should increase the cardholder's open-to-buy.

### **Reversal Advice/0420**

If the Authorization Platform generates a Reversal Advice/0420 message after the issuer has responded to the Authorization Request Response/0110 message with DE 39, value 87, the Authorization Platform will provide the following data elements.

- Purchase-only approval amount in the acquirer's transaction currency in DE 4
- Purchase-only approval amount in DE 5 in U.S. dollars, if the issuer has opted to receive this data element in the message
- Purchase-only approval amount in DE 6 in the issuer's cardholder billing currency
- DE 39, value 87
- Original amount in DE 54 in the issuer's cardholder billing currency and acquirer's transaction currency

When processing a Reversal Advice/0420 for a purchase-only approval (DE 39, value 87), the issuer should increase the cardholder's open-to-buy.

### **Authorization Advice/0120**

In addition to the standard data elements that are part of the issuer and system-generated Authorization Advice/0120 message, these messages should include the following data elements for purchase-only approvals.

- Purchase-only approval amount in DE 4 in the acquirer's transaction currency
- Purchase-only approval amount in DE 5 in the settlement currency (US dollars)
- Purchase only-approval amount in DE 6 in the issuer's cardholder billing currency
- DE 39, value 87 as provided by the issuer or Stand-In in the Authorization Request Response/0110

- Original amount in DE 54 in the issuer's cardholder billing currency and acquirer's transaction currency

## **Authorization Advice/0120—Acquirer-generated**

DE 39, value 87 is not a valid value for Authorization Advice/0120—Acquirer-generated messages. If an Authorization Advice/0120—Acquirer-generated message contains DE 39, value 87, the Authorization Platform will generate an Authorization Advice Response/0130 message where DE 39 contains value 30 and DE 44 contains value 039.

## **Alternate Processing**

MasterCard provides issuers with parameters to define whether or not a Purchase With Cash Back transaction should be forwarded to the Stand-In System for processing. For a transaction to qualify for the PIN-based category, DE 52 PIN Data will have to be present in the Authorization Request/0100 message. If DE 52 PIN Data was not present in the incoming message, the transactions will be categorized as a signature-based transaction.

If the issuer chooses to have PIN, Signature or both PIN and Signature Purchase With Cash Back transactions excluded from Stand-In processing, the Authorization Platform will provide the acquire with an Authorization Request Response/0110 message with a DE 39 Response of 91 if the issuer is not able to respond to the Authorization Request/0100 message.

If the issuer chooses to process PIN, Signature or both PIN and Signature Purchase with Cash Back transactions in Stand-in, the Stand-In System may provide the purchase-only amount response DE 39, value 87 when the Authorization Request/0100 message contains DE 3, subfield 1, value 09, and DE 48, subelement 61, subfield 2 contains value 1 and the cash back transaction limit or the cash accumulation limits have been exceeded but the purchase limits have not.

Purchase with Cash Back transactions will not be processed with the X-Code System.

## **Program and Service Format Requirements**

### **Purchase of Goods or Services with Cash Back**

---

## **Authorization Platform Edits**

The Authorization Platform will perform the following edits on Purchase of Goods or Services with Cash Back transactions.

### **Authorization Request/0100**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 3, subfield 1 with the value 09 and DE 54 is not present	DE 39 (Response Code) = 30 DE 44 (Additional Response Data) = 003
DE 3, subfield 1 with the value 09 and DE 54, subfield 1 is not a valid two-digit numeric value	DE 39 = 30 DE 44 = 054
DE 3, subfield 1 with the value 09 and DE 54, subfield 2 is not 40	DE 39 = 30 DE 44 = 003
DE 3, subfield 1 with the value 09 and DE 54, subfield 3 is not the same value as in DE 49	DE 39 = 30 DE 44 = 054
DE 3, subfield 1 with the value 09 and DE 54, subfield 4 is not D followed by 12 numeric digits	DE 39 = 30 DE 44 = 054
DE 3, subfield 1 with the value 09 and the cash back amount in DE 54 is greater than or equal to the amount in DE 4 (Amount, Transaction)	DE 39 = 30 DE 44 = 054
DE 3, subfield 1 with the value 09 and the Primary Account Number (PAN) is not within an account range that supports Purchase With Cash Back	DE 39 = 57
DE 48, subelement 61, subfield 2 contains a value other than 0 or 1	Generates an Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 048
DE 54 is present in the Authorization Request/0100 message where DE 54, subfield 2 contains value 57 (Original Amount)	Generates an Authorization Request Response/0110 message containing: DE 39 = 30 DE 44 = 054
DE 54, subfield 2 with the value 40 and DE 3, subfield 1 is not 09	DE 39 = 30 DE 44 = 003

If the Authorization Request/0100 message passes all Authorization Platform edits, the Authorization Platform will forward the Authorization Request/0100 message to the issuer.

**NOTE**

**Acquirers should send only one occurrence of DE 54, subfields 1–4 in Authorization Request/0100 and Reversal Request/0400 messages.**

**Authorization Request Response/0110**

The Authorization Platform will perform the following edits on the Authorization Request Response/0110 message when the issuer has provided DE 39 with value 87.

The Authorization Platform will provide two additional occurrence of DE 54, subfields 1–4 in the Authorization Request/0100 message to the issuer; one in the acquirer's transaction currency and one in the issuer's cardholder billing currency. This additional occurrence will be appended to the end of DE 54 before sending to the issuer.

If the issuer provides DE 54, subfield 2 with the value 40 in the Authorization Request Response/0110 message, MasterCard will not forward the cash back amount to the acquirer in the Authorization Request Response/0110 message.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 48, subelement 61 is not present or DE 48, subelement 61, subfield 2 does not contain value 1 in the Authorization Request/0100 message sent to the issuer	Sends to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 039
DE 38 is not present	Sends to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 038
DE 6 is not present	Sends to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 006
The amount in DE 6 of the Authorization Request Response/0110 message does not equal the purchase amount based on the original amounts present in the Authorization Request/0100 message.	Sends to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 039

## **Program and Service Format Requirements**

### **Purchase of Goods or Services with Cash Back**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The amount in DE 6 of the Authorization Request Response/0110 message is greater than the original amount in the Authorization Request/0100 message.	Sends to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 006
DE 51 is not present or is not the issuer's correct cardholder billing currency code	Sends to the issuer an Authorization Response Negative Acknowledgement/0190 message where: DE 39 = 30 DE 44 = 051

### **Authorization Advice/0120—Acquirer-generated**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 39 contains value 87	Creates an Authorization Advice Response/0130—System-generated message containing: DE 39 = 30 DE 44 = 039

### **Reversal/0400 messages**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 54 is not formatted correctly in relation to alphanumeric specifications for the subfields	Returns the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 054
DE 3, subfield 1, contains value 09 and DE 54, subfield 2, value 40 is not present and DE 39 does not contain value 87	Returns the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 003
DE 3, subfield 1 does not contain value 09 and DE 54, subfield 2, value 40 is present	Returns the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 003

## Real-time Substantiation

The Real-time Substantiation (formerly referred to as Auto Substantiation) service supports substantiation at the point-of-sale (POS) for qualified expenses incurred on a Flexible Spending Account (FSA) and Healthcare Reimbursement Arrangement (HRA) cards when used at a merchant with a qualifying Inventory Information Approval System (IIAS).

### Participation in Real-time Substantiation

Issuers must notify MasterCard if they want to support real-time substantiation processing by completing the Real-time Substantiation Participation form and providing the form to their Customer Operations Services (COS) representative.

Participation authorizes MasterCard to provide the issuer with real-time substantiation information in the Authorization Request/0100 or the Authorization Advice/0120 message. The Authorization Platform will remove healthcare related amounts from the Authorization Request/0100 or the Authorization Advice/0120 message for non-participating issuers.

MasterCard supports the issuance of MasterCard Assigned IDs for merchants.

To indicate an IIAS-compliant merchant, acquirers must provide DE 48 (Additional Data—Private Use), subelement 32 (MasterCard Assigned ID) in Authorization Request/0100, Authorization Advice/0120, and Reversal Request/0400 messages when the transaction is indicated as real-time substantiated (DE 48, subelement 61 (POS Data Extended Condition Codes), subfield 3 (Real-time Substantiation Indicator), value 1 (Merchant terminal verified the purchased items against an Inventory Information Approval System [IIAS])).

To obtain MasterCard Assigned IDs for IIAS merchant validation, acquirers should send an e-mail message to [sigis\\_merchant\\_setup@mastercard.com](mailto:sigis_merchant_setup@mastercard.com). The request should specify whether it is an addition or an update of the MasterCard Assigned ID, and at a minimum should include the acquirer name, telephone number, e-mail address, acquirer ID, processor ID, merchant parent/owner name (if applicable), MasterCard Assigned ID (if the request is for an update to the existing MasterCard Assigned ID), and merchant contact information.

Acquirers with existing MasterCard Assigned IDs for their merchants should continue to use those values but must notify MasterCard that those merchants are Special Interest Group for IIAS Standards (SIGIS)-compliant.

#### NOTE

**Acquirers with health care IIAS merchant that have received a Visa-assigned Merchant Verification Value from Visa, should include it in DE 48, sublement 36 (Visa Defined Data) for gateway mapping to Visa Field 62.20.**

## **Merchant Terminal Verification**

Following are the details on how a merchant terminal is IIAS-compliant.

Acquirers must provide DE 48 (Additional Data—Private Use), subelement 32 (MasterCard Assigned ID) in Authorization Request/0100, Authorization Advice/0120, and Reversal Request/0400 messages when the transaction is indicated as real-time substantiated (DE 48, subelement 61 (POS Data Extended Condition Codes), subfield 3 (Real-time Substantiation Indicator), value 1 (Merchant terminal verified the purchased items against an Inventory Information Approval System [IIAS]).

When the merchant terminal has verified the purchased items against an IIAS, the acquirer should populate the Authorization Request/0100 message with DE 48, subelement 61 and the following subfield values:

- Subfield 1 (Partial Approval Terminal Support Indicator) and subfield 2 (Purchase Amount Only Terminal Support Indicator) must contain values of zero or 1
- Subfield 3 must contain a value of 1 (Merchant terminal verified the purchased items against the IIAS).
  - If the issuer is not participating in real-time substantiation, this value will be changed by the Authorization Platform to 0 (Merchant terminal did not verify the purchased items against the IIAS).
  - To indicate to issuers participating in real-time substantiation that the transaction was submitted as IIAS but from a non-IIAS compliant merchant, MasterCard will populate subfield 3 with the value 4 (Transaction was submitted as real-time substantiated, but from a non-IIAS certified merchant).
- Subfields 4 and 5 are reserved for future use and must contain values of zero.

Acquirers will not receive DE 48, subelement 61 in the Authorization Request Response/0110 message.

When an acquirer creates an Authorization Advice/0120 message to advise the issuer of an approved authorization performed by the acquirer, DE 48, subelement 61 should be present if it was present in the original Authorization Request/0100 message.

## **Real-time Substantiation Amounts**

MasterCard defines DE 54 (Additional Amounts), subfield 2 (Amount Type) with a redefined value of 10 (Healthcare Eligibility Amount). When the acquirer is providing the real-time substantiation indicator in DE 48, subelement 61, subfield 3, this redefined amount type allows the acquirer to indicate the portion of DE 4 (Amount, Transaction) that is eligible for real-time substantiation.

In addition to the Healthcare Eligibility Amount, MasterCard supports amount type, DE 54, subfield 2, value 11 (Prescription Eligibility Amount), which allows the acquirer to indicate the portion of the healthcare eligibility amount that includes the amount spent for prescriptions.

Subfield 2, value 11 must only be present when the acquirer provides subfield 2, value 10 in the Authorization Request/0100 or the Authorization Advice/0120 message. In addition, the amount in subfield 2, value 11 must be less than or equal to the amount of subfield 2, value 10.

Values 10 and 11 will not be returned to the acquirer in the Authorization Request Response/0110 or the Authorization Advice Response/0130 message.

## Transaction Processing Examples

Following are examples of Real-time Substantiation transaction processing. The examples only show one occurrence of DE 54 amounts in USD. However, standard currency conversion rules will apply. Therefore, acquirers and issuers will always receive amount-related data elements in the acquirer's transaction currency and the issuer's cardholder billing currency for DE 54.

Because Real-time Substantiation transactions can be used in combination with partial approvals, when the issuer receives an Authorization Request/0100 message containing DE 48, subelement 61, subfield 1, value 1, the issuer has the option to:

- Approve the entire transaction amount.
- Decline the entire transaction amount.
- Respond with a partial approval.

For the issuer to respond with a partial approval, DE 48, subelement 61, subfield 1 must contain a value of 1; otherwise, the issuer must approve or decline the entire transaction amount.

Partial approvals are not valid for Authorization Advice/0120 messages and will be rejected with a format error.

### Example 1—Partial Approval: Entire Healthcare Eligibility Amount

This example illustrates that the issuer approved the entire Healthcare Eligibility Amount, which in this case is a partial approval of the total transaction amount. In this scenario, the merchant would ask the cardholder to use another form of payment for the remaining USD 60 or remove some items from the purchase.

## Program and Service Format Requirements

### Real-time Substantiation

---

Authorization Request/0100	Authorization Request Response/0110
From Issuer	To Acquirer
<ul style="list-style-type: none"><li>• DE 48, subelement 61 = 10100 (indicates terminal can handle partial approvals and has verified against IIAS)</li><li>• DE 4 = USD 100</li><li>• DE 54, subfield 2, value 10 = USD 40</li></ul>	<ul style="list-style-type: none"><li>• DE 6 = USD 40</li><li>• DE 39 = 10</li></ul> <ul style="list-style-type: none"><li>• DE 4 = USD 40 100</li><li>• DE 54, subfield 2, value 57 (Original Amount) = USD</li><li>• DE 39 = 10</li></ul>

### Example 2—Partial Approval: Partial Healthcare Eligibility Amount

This example illustrates that the issuer approved only a portion of the Healthcare Eligibility Amount, which in this case is a partial approval of the total transaction amount. In this scenario, the merchant would ask the cardholder to use another form of payment for the remaining USD 80 or remove some items from the purchase.

Authorization Request/0100	Authorization Request Response/0110
From Issuer	To Acquirer
<ul style="list-style-type: none"><li>• DE 48, subelement 61 = 10100</li><li>• DE 4 = USD 100</li><li>• DE 54, subfield 2, value 10 = USD 40</li></ul>	<ul style="list-style-type: none"><li>• DE 6 = USD 20</li><li>• DE 39 = 10</li></ul> <ul style="list-style-type: none"><li>• DE 4 = USD 20</li><li>• DE 54, subfield 2, value 57 = USD 100</li><li>• DE 39 = 10</li></ul>

### Example 3—Full Approval: Entire Healthcare Eligibility Amount

In this example, the merchant terminal is indicating that they do not support partial approvals; therefore, a full approval or decline is required. The issuer approves the full transaction; thereby approving the entire Healthcare Eligibility Amount.

Authorization Request/0100	Authorization Request Response/0110
From Issuer	To Acquirer
<ul style="list-style-type: none"><li>• DE 48, subelement 61 = 00100</li><li>• DE 4 = USD 100</li><li>• DE 54, subfield 2, value 10 = USD 100</li></ul>	<ul style="list-style-type: none"><li>• DE 4 = USD 100</li><li>• DE 39 = 00</li></ul> <ul style="list-style-type: none"><li>• DE 4 = USD 100</li><li>• DE 39 = 00</li><li>• No DE 54, subfield 2, value 57 (Original Amount) is provided in this scenario because the issuer</li></ul>

Authorization Request/0100	Authorization Request Response/0110
	responded with DE 39 = 00

#### Example 4—Partial Approval: Entire Healthcare Eligibility Amount, including Prescriptions

This example illustrates that the issuer approved the entire Healthcare Eligibility Amount and Prescription Eligibility Amount (the prescription amount is a portion of the healthcare amount), which is a partial approval of the total transaction amount. In this scenario, the merchant would ask the cardholder use another form of payment for the remaining USD 60 or remove some items from the purchase.

Authorization Request/0100	Authorization Request Response/0110
From Issuer	To Acquirer
<ul style="list-style-type: none"> <li>• DE 48, subelement 61 = 10100</li> <li>• DE 4 = USD 100</li> <li>• DE 54, subfield 2, value 10 = USD 40</li> <li>• DE 54, subfield 2, value 11 = USD 30</li> </ul>	<ul style="list-style-type: none"> <li>• DE 6 = USD 40</li> <li>• DE 39 = 10</li> <li>• DE 4 = USD 40</li> <li>• DE 54, subfield 2, value 57 = USD 100</li> <li>• DE 39 = 10</li> </ul>

#### Example 5—Partial Approval: Partial Healthcare Eligibility Amount, including Prescriptions

This example illustrates that the issuer approved only a portion of the Healthcare and Prescription Eligibility amounts. In this scenario, the merchant would ask the cardholder use another form of payment for the remaining USD 80 or remove some items from the purchase.

Authorization Request/0100	Authorization Request Response/0110
From Issuer	To Acquirer
<ul style="list-style-type: none"> <li>• DE 48, subelement 61 = 10100</li> <li>• DE 4 = USD 100</li> <li>• DE 54, subfield 2, value 10 = USD 40</li> <li>• DE 54, subfield 2, value 11 = USD 30</li> </ul>	<ul style="list-style-type: none"> <li>• DE 6 = USD 20</li> <li>• DE 39 = 10</li> <li>• DE 4 = USD 20</li> <li>• DE 54, subfield 2, value 57 = USD 100</li> <li>• DE 39 = 10</li> </ul>

## Program and Service Format Requirements

### Real-time Substantiation

---

#### Example 6—Full Approval: Entire Healthcare Eligibility Amount, including Prescriptions

In this example, the merchant terminal is indicating that they do not support partial approvals; therefore, a full approval or decline is required. The issuer approves the full transaction; thereby approving the entire Healthcare Eligibility Amount, including the Prescription Eligibility Amount.

Authorization Request/0100	Authorization Request Response/0110
From Issuer	To Acquirer
<ul style="list-style-type: none"><li>• DE 48, subelement 61 = 00100</li><li>• DE 4 = USD 100</li><li>• DE 54, subfield 2, value 10 = USD 100</li><li>• DE 54, subfield 2, value 11 = USD 60</li></ul>	<ul style="list-style-type: none"><li>• DE 4 = USD 100</li><li>• DE 39 = 00</li><li>• No DE 54, subfield 2, value 57 (Original Amount) is provided in this scenario since the issuer responded with DE 39=00</li></ul>

### Authorization Platform Edits

The Authorization Platform performs the following edits on Real-time Substantiation transactions.

#### Authorization Request/0100 and Authorization Advice/0120

WHEN...	THEN the Authorization Platform...
DE 54, subfield 2, value 10 or 11 is present and DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) is not 00 (Purchase of goods or services)	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: <ul style="list-style-type: none"><li>• DE 39 = 30 (Format error)</li><li>• DE 44 = 054</li></ul>
DE 54, subfield 2, value 10 is greater than the transaction amount in DE 4	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 054</li></ul>
DE 54 subfield 2, value 10 or 11 is present and the issuer does not support healthcare substantiation transaction processing	Removes DE 54 subfield 2, value 10 and 11 occurrences from the Authorization Request/0100 or Authorization Advice/0120 message to the issuer.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 54, subfield 2, value 11 is present and DE 54, subfield 2, value 10 is not present	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 054</li> </ul>
The amount in DE 54, subfield 2 value 11 is greater than the amount in DE 54, subfield 2, value 10	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 054</li> </ul>
DE 54 contains more than one occurrence of subfield 2, value 10 or DE 54 contains subfield 2, value 10 and the second occurrence is not DE 54, subfield 2, value 11	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 054</li> </ul>
DE 54 contains more than one occurrence of subfield 2, value 11	Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 054</li> </ul>
<b>WHEN DE 48, Subelement 32 is present and...</b>	<b>THEN the Authorization Platform...</b>
The length of the MasterCard Assigned ID is less than six digits in the Authorization Request/0100, Authorization Advice/0120—System-generated, and Reversal Request/0400 message	Sends the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Response/0410 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 048</li> </ul>
<b>WHEN DE 48, subelement 61, subfield 3 is...</b>	<b>THEN the Authorization Platform...</b>
1 (Merchant terminal verified the purchase items against an Inventory Information Approval System [IIAS])	Validates that DE 48, subelement 32 (if present) contains a valid MasterCard Assigned ID for IIAS.
If the MasterCard Assigned ID is valid	Forwards the Authorization Request/0100 message to the issuer.

## **Program and Service Format Requirements**

### **Recurring Payment Test Transactions**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
If the MasterCard Assigned ID is not valid or not present in the Authorization Request/0100 message	Updates the value in DE 48, subelement 61, subfield 3 as follows: <ul style="list-style-type: none"><li>• If the issuer participates in real-time substantiation, sends DE 48, subelement 61, subfield 3, value 4 (Transaction was submitted as real-time substantiated but from a non-IIAS certified merchant).</li><li>• If the issuer does not participate in real-time substantiation sends DE 48, subelement 61, subfield 3, value 0 (Merchant terminal did not verify the purchased items against an Inventory Information Approval System [IIAS]).</li></ul>
<b>WHEN DE 48, subelement 61, subfield 3 is...</b>	<b>THEN the Authorization Platform...</b>
4 (Transaction was submitted as real-time substantiated but from a non-IIAS certified merchant) in the Authorization Request/0100 message	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 048</li></ul>
<b>Reversal Request/0400</b>	
<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 54, subfield 2, value 10 or 11 is present in the Reversal Request/0400 message	Removes DE 54, subfield 2, values 10 and 11 from the Reversal Request/0400 message to the issuer.

## **Recurring Payment Test Transactions**

The recurring payment test transaction allows acquirers to send an Authorization Request/0100 message to an issuer containing a transaction amount of zero.

Before submitting an authorization request for the full amount of a recurring payment, the card acceptor may use a recurring payment test transaction to determine the status of the cardholder account.

Recurring payment test transactions must comply with all existing recurring payment transaction identification requirements.

A recurring payment Authorization Request/0100 message test transaction containing DE 61, subfield 7, value 4 and DE 61 subfield 4, value 4, must include DE 4 containing a zero value transaction amount.

## Reversal Processing

MasterCard supports the reversal of a full transaction amount or a partial transaction amount using reversal processing.

### Full Reversals

The Authorization Platform supports full reversal functionality using the Reversal 04xx messages.

Full reversal functionality may be used for, but is not limited to, the following scenarios:

- Acquirer cannot deliver a response messages 0110 or 0410 to the merchant
- Acquirer cannot match the response message 0110 or 0410 to the original request
- The authorization response message received contains errors
- The authorization response message was received too late

### Partial Reversals

The Authorization Platform supports partial reversal functionality using the Reversal/04xx messages.

Partial reversal functionality is useful in adjusting a portion of the original authorization amount in the following scenarios:

- A merchant ships only a portion of merchandise.
- A cardholder returns a rental vehicle earlier than originally reserved.
- A cardholder checks out of a hotel earlier than originally reserved.
- A cardholder cancels a portion of the transaction.

MasterCard supports Reversal Request/0400 and Reversal Advice/0420 messages where DE 95 (Replacement Amounts), subfield 1 (Actual Amount, Transaction) contains a value other than all zeros. DE 95, subfield 1, in the originating reversal, must be a lesser amount than the amount in DE 4 (Amount, Transaction).

Please refer to the *Chargeback Guide* for rules related to partial reversal functionality.

### Reversals of Balance Inquiry Transactions

Following are the details of the reversal of a Balance Inquiry transaction.

MasterCard supports Reversal Request/0400 and Reversal Advice/0420 messages containing DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 30 (Balance Inquiry). In inquiry transactions, DE 4 must contain a value of all zeros unless an ATM transaction fee DE 28 (Amount, Transaction Fee) has been applied by an acquirer for an ATM transaction in a country where of an ATM transaction fee is allowed.

## **Reversals of Purchase of Goods or Services with Cash Back Transactions**

Following are the details of the reversal of a Purchase of Goods or Services with Cash Back transaction.

MasterCard provides DE 54 (Additional Amounts), subfield 2 (Amount Type), value 40 (Amount Cash Back) to issuers in the Reversal Request/0400 message if DE 54, subfield 2, value 40 was contained in the Reversal Request/0400 message from the acquirer. Acquirers provide DE 4 (Amount, Transaction) in the Reversal Request/0400 message for the full, original amount of the Authorization Request/0100 message. With Purchase of Goods and Services with Cash Back transactions, DE 4 contains the cash back amount, as defined in DE 54.

As with Authorization Request/0100 message processing, the Authorization Platform edits Reversal Request/0400 messages when DE 54, subfield 2, value 40 is present. In this case, the Authorization Platform checks to ensure that DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) contains value 09 (Purchase with Cash Back).

If DE 54, subfield 2, value 40 is not present, the Authorization Platform performs an additional check to ensure that the Reversal Request/0400 message contains DE 39 (Response Code), value 87 (Purchase only, no cash back allowed).

When an acquirer submits a full or partial reversal for a Purchase Amount Only approval where DE 39 (Response Code) of the Authorization Request Response/0110 message contains value 87, MasterCard recommends that the acquirer not send DE 54 in the reversal message. If the acquirer intends the Reversal Request/0400 message as a partial reversal, DE 95 (Replacement Amounts) will also be present, containing the adjusted amount of the original authorization.

DE 54, subfield 2, value 40 is the only instance of DE 54 that MasterCard will forward to issuers in a Reversal Request/0400 message. All other instances of DE 54 will be removed from the Reversal Request/0400 message before forwarding the message to the issuer.

DE 54, subfield 2, value 40 also may be included in the Reversal Advice/0420 message.

## Alternate Processing

While no Stand-In System processing tests will be applied to the Reversal Request/0400 message, the Authorization Platform supports alternate processing of Reversal Request/0400 and Reversal Request Response/0410 messages when the issuer is unable or unavailable to respond to the Reversal Request/0400 message.

The Authorization Platform will perform the following processing when an issuer is unable or is unavailable to respond to the Reversal Request/0400 message:

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The Authorization Platform times out or The issuer is signed-out or The issuer responded with a Reversal Request Response/0410 message with an error or The Authorization Platform cannot deliver the Reversal Request/0400 message to the issuer	Sends the acquirer a Reversal Request Response/0410 message where: DE 39 = 00 (Approved or Completed successfully) Sends a Reversal Advice/0420 message to SAF for immediate availability to the issuer where: <ul style="list-style-type: none"> <li>• DE 39 is The value from the acquirer's Reversal Request/0400 message</li> <li>• DE 60 contains one of the following values as applicable:               <ul style="list-style-type: none"> <li>– 402 = (Banknet Advice: IPS Time-out error)</li> <li>– 403 = (Issuer Sign-out)</li> <li>– 409 = (Issuer Response Error)</li> <li>– 413 = (Issuer Undelivered)</li> </ul> </li> </ul>
The issuer responds with an error in the Reversal Request Response/0410 message	Responds to the issuer with a Negative Acknowledgement/0190 message where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = Data element in error</li> </ul> Provides a Reversal Advice/0420 message to the issuer from SAF for immediate availability to the issuer (as defined above)
The Authorization Platform cannot deliver the Reversal Request Response/0410 message to the acquirer	Will not send a Reversal Advice/0420 message to the issuer. In this case, acquirers have the responsibility to resend the reversal to the issuer.

## Program and Service Format Requirements

### Reversal Processing

---

#### NOTE

**Members in the Europe region that route to an alternate issuer host for alternate processing instead of Stand-In, will still receive an Authorization Advice/0120—Acquirer-generated as described here. Alternate issuer host processing does not send Reversal Request/0400 or Authorization Advice/0120 messages to the alternate host.**

## Authorization Platform Edits

The Authorization Platform performs the following edits on reversal transaction processing.

### Reversal Request/0400

The Authorization Platform will perform the following edits on the Reversal Request/0400 message as it relates to DE 95 (Replacement Amounts) and partial reversals.

WHEN...	THEN the Authorization Platform...
DE 95 (Replacement Amounts) is equal to or greater than DE 4 (Amount, Transaction)	Sends the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 095
DE 95 (Replacement Amounts) is equal to zero	Removes DE 95 from the Reversal Request/0400 message before providing the Reversal Request/0400 message to the issuer.

The Authorization Platform will perform the following edits on the Reversal Request/0400 message as it relates to DE 54 (Additional Amounts) and reversals of Purchase of Goods or Services with Cash Back transactions.

WHEN...	THEN the Authorization Platform...
DE 54 is not formatted correctly in relation to alphanumeric specifications for the subfields	Returns the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 054
DE 3, subfield 1, contains value 09 and DE 54, subfield 2, value 40 is not present and DE 39 does not contain value 87	Returns the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 003
DE 3, subfield 1 does not contain value 09 and DE 54, subfield 2, value 40 is present	Returns the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 003

The Authorization Platform will perform the following edits on the Reversal Request/0400 message as it relates to reversals of Balance Inquiry transactions.

<b>WHEN the Reversal Request/0400 message...</b>	<b>THEN the Authorization Platform...</b>
Contains a value of all zeros in DE 4 (Amount, Transaction) and DE 3, subfield 1, does not contain a value of 30 (Balance Inquiry)	Returns the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 004
Contains a value of 30 (Balance Inquiry) in DE 3, subfield 1 then DE 4 (Amount, Transaction) must contain a value of all zeros unless the transaction contains DE 28 (Amount, Transaction Fee), otherwise	Returns the acquirer a Reversal Request Response/0410 message where: DE 39 = 30 DE 44 = 004

## RiskFinder

RiskFinder® is an optional service that MasterCard offers to help issuers more effectively predict fraudulent card use. RiskFinder uses a state-of-the-art neural network to evaluate authorization transactions and produce a transaction score relative to the potential fraudulent use of the card.

RiskFinder bases scores on all merchant and cardholder data available to the issuer's RiskFinder scoring system. This global information complements the customer's current account-based fraud prediction systems. For those customers not currently using any fraud predictive model, this package provides a comprehensive tool to help issuers to reduce fraudulent card use.

The RiskFinder scoring system receives authorization transaction information by Authorization Advice/0120 messages. Members have the following three options to send transaction information to the RiskFinder scoring system:

- Member-initiated message scoring
- MIP-initiated message scoring
- Member-initiated batch scoring

This topic discusses the Member-initiated message scoring option. Contact your Customer Technology and Operations Services representative for information on MIP-initiated scoring and batch scoring.

### Authorization Advice/0120—To RiskFinder

Authorization Request/0100 messages may contain BINs that customers have selected for scoring. For these transactions, issuers create and send Authorization Advice/0120—Issuer-generated messages to the RiskFinder scoring system. All Authorization Advice/0120 mandatory data elements apply.

## **Program and Service Format Requirements**

### **RiskFinder**

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 60 (Advice Reason Code)	M	M	•	Must be 6500030 = For member-generated transactions
DE 121 (Authorizing Agent ID Code)	C	•	C	The issuer supplies the customer ID.

### **Authorization Advice Response/0130—From RiskFinder**

The RiskFinder scoring system sends to the issuer an Authorization Advice Response/0130 to acknowledge receipt of the Authorization Advice/0120. All Authorization Advice Response/0130 mandatory data elements apply. Note in the following table additional data requirements specific to RiskFinder messages.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 62 (Intermediate Network Facility [INF] Data)	•	CE	CE	A value of “RISK” identifies this as a RiskFinder message.

### **Network Management/08xx—To and From RiskFinder**

Following are the details of how Network Management/08xx messages are used in association with RiskFinder.

#### **Network Management Request/0100 and Network Management Request Response/0110**

Following are scenarios in how customers use Network Management Request/0800—Sign-On/Sign-Off message to notify the RiskFinder scoring system.

- They are ready to receive scored Administrative Advice/0620 messages on a near real-time basis.
- They do not want to receive their real-time scored messages, and RiskFinder should put all its held scored messages in the RiskFinder store-and-forward (SAF) queue.
- They are ready to retrieve Administrative Advice/0620 messages from the RiskFinder SAF queue.

In all three scenarios, the RiskFinder scoring system responds with a Network Management Response/0810—Sign-On/Sign-Off. In the third scenario, customers receive a Network Management Advice/0820—SAF End of File message when RiskFinder completes the SAF process.

All mandatory data elements for these two message types apply. Note in the following table additional data requirements specific to these two messages.

Data Element ID and Name	Org	Sys	Dst	Values/Comments
70 (Network Management Information Code)	M	M	•	<p>Indicates the specific purpose of the message as follows:</p> <p>070 = Sign-on to RiskFinder by BIN (member requests RiskFinder-scored Administrative Advice/0620 messages)</p> <p>071 = Sign-off to RiskFinder by BIN (does not request RiskFinder-scored Administrative Advice/0620 messages)</p> <p>072 = Member wants to receive, by BIN, RiskFinder-scored Administrative Advice/0620 messages from SAF.</p>

### Network Management Advice/0120

The RiskFinder scoring system sends the issuer a Network Management Advice/0820 message to indicate that there are no more Administrative Advice/0620 messages in the SAF queue. All mandatory data elements for this message apply.

Data Element ID and Name	Org	Sys	Dst	Values/Comments
70 (Network Management Information Code)	•	M	M	<p>Indicates the specific purpose of the message as follows:</p> <p>072 = Member wants to receive, by BIN, RiskFinder-scored Administrative Advice/0620 messages from SAF.</p>

### Administrative Advice/0620

The RiskFinder scoring system sends scores to the issuer via Administrative Advice/0620 messages. All Administrative Advice/0620 mandatory data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 33 (Forwarding Institution ID Code)	•	M	M	<p>Identifies the customer, institution, or Authorization Platform facility originating this Administrative Advice/0620.</p> <p>Value 003200 indicates RiskFinder generated the message.</p>
DE 48 (Additional Data—Private Use), TCC	•	C	C	TCC is mandatory; may also contain data for IDs 83, 87, 88, and 89, if these were present in the Authorization Advice/0120—no other IDs are included.

## Program and Service Format Requirements

### RiskFinder

---

Data Element	Org	Sys	Dst	Values/Comments
DE 60 (Advice Reason Code)	•	M	M	Specifies the reason for the Administrative Advice/0620; must be the following: 6500029 = For MIP-generated transactions 6500030 = For member-generated transactions
DE 62 (Intermediate Network Facility (INF) Data)	•	C	C	A value of "RISK" identifies this as a RiskFinder message.
DE 120 (Record Data)	•	C	C	DE 60 = 650, contains RiskFinder scoring information.

### DE 120 Layout for RiskFinder

Following is the DE 120 layout in the Administrative Advice/0620 message.

ID	Subelement Contents	Length	Values/Comments
01	RiskFinder score subelement ID	2	
	Subelement length	2	
	Risk Score	3	Numeric; the RiskFinder scoring system provides this data.
	Model Designator	15	Alphanumeric; identifies the scoring model used to determine the risk score.
	Reason Code	6	Numeric; identifies the first, second, and third reason for the determination of the score.
	Filler	19	Not currently used.
02	ID identifying DE 2 from the Authorization Advice/0120	2	
	Subelement length	2	
	Primary Account Number (PAN)	up to 19	
04	ID identifying DE 4 from the Authorization Advice/0120	2	
	Subelement length	2	
	Amount, Transaction	12	

<b>ID</b>	<b>Subelement Contents</b>	<b>Length</b>	<b>Values/Comments</b>
05	ID identifying DE 5 from the Authorization Advice/0120	2	
	Subelement length	2	
	Amount, Transaction	12	
06	ID identifying DE 6 from the Authorization Advice/0120	2	
	Subelement length	2	
	Amount, Cardholder Billing	12	
09	ID identifying DE 9 from the Authorization Advice/0120	2	
	Subelement length	2	
	Conversion Rate, Settlement	8	
10	ID identifying DE 10 from the Authorization Advice/0120	2	
	Subelement length	2	
	Conversion Rate, Cardholder Billing	8	
12	ID identifying DE 12 from the Authorization Advice/0120	2	
	Subelement length	2	
	Time, Local Transaction	6	
13	ID identifying DE 13 from the Authorization Advice/0120	2	
	Subelement length	2	
	Date, Local Transaction	4	
14	ID identifying DE 14 from the Authorization Advice/0120	2	
	Subelement length	2	

## Program and Service Format Requirements

### RiskFinder

---

ID	Subelement Contents	Length	Values/Comments
	Date, Expiration	4	
18	ID identifying DE 18 from the Authorization Advice/0120	2	
	Subelement length	2	
	Merchant Type	4	
22	ID identifying DE 22 from the Authorization Advice/0120	2	
	Subelement length	2	
	Point-of-Service (POS) Entry Mode	3	
32	ID identifying DE 32 from the Authorization Advice/0120	2	
	Subelement length	2	
	Acquiring Institution ID Code	up to 6	
35	ID identifying DE 35 from the Authorization Advice/0120	2	
	Subelement length	2	
	Track 2 Data	up to 37	
39	ID identifying DE 39 from the Authorization Advice/0120	2	
	Subelement length	2	
	Response Code	2	
41	ID identifying DE 41 from the Authorization Advice/0120	2	
	Subelement length	2	
	Card Acceptor Terminal ID	8	
42	ID identifying DE 42 from the Authorization Advice/0120	2	

<b>ID</b>	<b>Subelement Contents</b>	<b>Length</b>	<b>Values/Comments</b>
	Subelement length	2	
	Card Acceptor ID Code	15	
43	ID identifying DE 43 from the Authorization Advice/0120	2	
	Subelement length	2	
	Card Acceptor Name and Location	40	
45	ID identifying DE 45 from the Authorization Advice/0120	2	
	Subelement length	2	
	Track-1 Data	up to 76	
49	ID identifying DE 49 from the Authorization Advice/0120	2	
	Subelement length	2	
	Currency Code, Transaction	3	
50	ID identifying DE 50 from the Authorization Advice/0120	2	
	Subelement length	2	
	Currency Code, Settlement	3	
51	ID identifying DE 51 from the Authorization Advice/0120	2	
	Subelement length	2	
	Currency Code, Cardholder Billing	3	
61	ID identifying DE 61 from the Authorization Advice/0120	2	
	Subelement length	2	
	Point-of-Service (POS) Data	11–26	

## **Program and Service Format Requirements**

### **Transaction Blocking**

---

#### **Administrative Advice Response/0130**

The issuer sends to the RiskFinder scoring system an Administrative Advice Response to acknowledge receipt of the Administrative Advice/0620. All Administrative Advice Response/0630 mandatory data elements apply.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 62 (Intermediate Network Facility (INF) Data)	CE	CE	•	A value of "RISK" identifies this as a RiskFinder message.

### **Transaction Blocking**

The Transaction Blocking service provides issuers the ability to block transactions based upon the issuing ICA or account range. This service also gives issuers the option to apply blocks to prevent transactions from being forwarded either to the issuer or to the Stand-In System when the issuer is unavailable.

One or more of the following transaction parameters indicates transaction blocking.

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)
- DE 18 (Merchant Type) DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)
- DE 61 (Point-of-Service [POS] Data), subfield 10 (Card Activated Terminal Level [CAT])
- DE 61 (Point-of-Service [POS] Data), subfield 13 (POS Country Code)

Transaction blocks can only be set up using valid values for each parameter. For example, an issuer cannot set up a transaction block using an invalid merchant type.

#### **NOTE**

**Members must comply with the selective Authorization Policy as defined in the MasterCard Rules.**

#### **Transaction Block Setup Configuration**

Issuers must provide the following information for transaction block setup.

- If the transactions will be blocked for all routes or only from going to the Stand-In System when the issuer is unavailable.
- The issuer may define the response code applicable to the transaction block based on the response codes available for the Authorization Request Response/0110 message with the exception of these:
  - 00 = Approved or completed successfully

- 01 = Refer to card issuer
- 08 = Honor with ID
- 10 = Partial approval
- 85 = Not declined
- 87 = Purchase Only, No Cash Back Allowed

If issuers do not specify a decline response code, the default response code will be 57 (Transaction not permitted to issuer/cardholder).

## Authorization Platform Edits

The Authorization Platform performs the following edits on Authorization Request/0100—Transaction Blocking transactions.

WHEN...	THEN the Authorization Platform...
The acquirer sends an Authorization Request/0100 message and the transaction falls within a transaction block	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = The response code identified in the transaction block setup
The transaction does not match any transaction block	Forwards the Authorization Request/0100 message to the issuer or to the Stand-In System if the issuer is unavailable.
The transaction matches one of the transaction blocks that are applicable to Stand-In and the issuer is available	Forwards the Authorization Request/0100 message to the issuer.
The transaction matches one of the transaction blocks that are applicable to Stand-In and the issuer is unavailable	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = The response code identified in the transaction block setup

## Transaction Blocking for Inactive BINs

Transaction Blocking for Inactive BINs allows issuers to block an entire BIN range or a segment of a BIN range, defined up to 11 digits. Through this service, a customer can protect BIN ranges before they go into production or BINs that are not actively used, stopping any fraud attempts on these accounts.

## Authorization Platform Edits

The Authorization Platform performs the following edits on Authorization Request/0100—Transaction Blocking for Inactive BINs transactions.

## Program and Service Format Requirements

### Visa Custom Payment Service

WHEN...	THEN the Authorization Platform...
The acquirer sends an Authorization Request/0100 message and the transaction falls within a transaction block for inactive BINs	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 14 (Invalid card number. The transaction is declined.)

## Visa Custom Payment Service

MasterCard supports Visa Custom Payment Service Authorization Request/0100 messages to accommodate customers. MasterCard accepts and forwards all Visa Authorization Request/0100 messages containing Visa Custom Payment Service information to the Visa network. If the Visa network is unavailable to authorize a transaction through the MasterCard gateway, MasterCard processes the authorization request using the MasterCard Stand-In parameters for Visa-branded activity.

#### NOTE

**This topic applies only to Dual Message System processing of Visa authorization transactions.**

### Authorization Request/0100—Visa Custom Payment Service

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number [PAN])	M	•	M	PAN begins with 4 indicating a Visa card.
DE 14 (Date, Expiration)	C	•	C	Must be present for magnetic stripe transactions and contain same expiration date as in DE 35 or DE 45.
DE 18 (Merchant Type)	M	•	M	Must contain a valid Custom Payment Service MCC.
DE 22 (Point-of-Service (POS) Entry Mode, subfield 1, POS Terminal PAN Entry Mode)	M	•	M	Must contain 90 to indicate that the track 1 or track 2 data is unaltered; where card presence is not required or the transaction is key entered, 01 is valid.
DE 35 (Track 2 Data)	C	•	C	Track 2 or Track 1 must be present and passed unaltered if the DE 22 value is 90.
DE 37 (Retrieval Reference Number)	C	•	C	Must be present for Custom Payment Service incremental authorizations and reversals.
DE 42 (Card Acceptor ID Code)	M	•	M	Must be present for Custom Payment Service transactions.

**Program and Service Format Requirements****Visa Custom Payment Service**

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 43 (Card Acceptor Name and Location)	M	•	M	Must be present for Custom Payment Service transactions.
DE 45 (Track 1 Data)	C	•	C	Track 1 or Track 2 must be present and passed unaltered if the DE 22 value is 90.
DE 48, subelement 90 (Custom Payment Service Request [Visa field 62.1])	M	•	M	Indicates a request for a Visa Custom Payment Service qualified transaction and must contain one of the following values: I = Incremental authorization P = Preferred customer R = Recurring payment Y = Custom Payment Service participation request
DE 48, subelement 91 (Visa Custom Payment Service Request [Transaction ID], [Visa field 62.2])	C	•	C	Must be present for incremental authorization and reversal transactions and contain the Transaction ID of the original transaction.
DE 48, subelement 96 (Visa Market-Specific Data [Visa field 62.4])	C	•	C	Must be present for hotel or automobile transactions and contain one of the following values: A = Automobile rental H = Hotel rental
DE 48, subelement 97 (Visa Prestigious Property Indicator [Visa field 62.6])	C	•	C	May be present for participants in the Visa Prestigious Lodging program and contains one of the following values: D = Visa established limits B = Visa established limits S = Visa established limits
DE 61, (Point-of-Service [POS] Data, subfield 12 (POS Authorization Life Cycle)	M	•	M	Must contain the authorization life cycle if DE 48, subelement 96 (Market-specific Data) is present.

## **Authorization Request Response/0110—Visa Custom Payment Service**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

## Program and Service Format Requirements

### Visa Custom Payment Service

---

Data Element	Org	Sys	Dst	Values/Comments
DE 48, subelement 90 (Custom Payment Service Request [Visa field 62.1])	M	•	M	<p>Contains response data for Visa Custom Payment Service qualified transaction and must be one of the following values:</p> <p>A = Meets card present requirements C = Meets cardholder-activated terminal (CAT) E = Meets card present requirements and merchant name and location present V = Meets address verification requirements N = Not qualified for Custom Payment Service T = No Custom Payment Service program available</p>
DE 48, subelement 91 (Visa Custom Payment Service Request [Transaction ID])	C	•	C	<p>Must be present if DE 48 subelement 90 is present. Contains one of the following response lengths:</p> <p>Length 19 = Contains Transaction ID (15 bytes) and validation code (4 bytes)</p> <p>Length 15 = Contains Transaction ID (15 bytes) for an incremental or reversal response</p> <p>Length 06 = Contains Visa downgrade information.</p> <p>Length 02 = Contains one of the following MasterCard assigned codes:</p> <p>MS = MasterCard Stand-In processing; Custom Payment Service qualified information available MX = MasterCard X-Code processing; qualified information available VS = Visa did not supply a downgrade reason code</p>
DE 48, subelement 96 (Visa Market-Specific Data [Visa field 62.4])	C	•	C	<p>Must be present if present in the original Authorization Request/0100 message. Contains response data for Visa market-specific data and must be one of the following values:</p> <p>A = Automobile rental H = Hotel rental N = Failed market-specific data edit</p>

### DE 48 Structure in a Visa Custom Payment Service Transaction

Following is the structure of DE 48 (Additional Data—Private Use) in a Visa Custom Payment Service transaction.

LLL	"VAR"—999 maximum bytes (TCC + Subelement (SE) data)						
3 bytes	1 byte	2 bytes	2 bytes	1 byte	2 bytes	2 bytes	Variable
Total Data Element Length	TCC	First Subelement Data			Second Subelement Data		
		SE ID 90	SE 90 Length	Authorization Characteristics Indicator	SE ID 91	SE 91 Length	Trans ID
<b>1002 maximum bytes (LLL +TCC + Subelement Data)...</b>							

... "VAR"—999 maximum bytes (TCC + Subelement (SE) data)					
2 bytes	2 bytes	1 byte	2 bytes	2 bytes	1 byte
Third Subelement Data			Fourth Subelement Data		
SE ID 96	SE 96 Length	Market-specific Data ID	SE ID 97	SE 97 Length	Prestigious Property Indicator
<b>...1002 maximum bytes (LLL +TCC + Subelement Data)</b>					

## Visa Programs

### Visa CVV2

Following are Visa CVV2 Authorization/01xx message layouts.

#### Authorization Request/0100—Visa CVV2

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number)	M	•	M	PAN begins with 4 indicating a Visa card.
DE 48, subelement 92 (CVV2 Data), subfield 1 (CVV2 Presence ID)	C	•	C	0 = Merchant did not provide CVV2 or it was deliberately bypassed 1 = CVV2 value present 2 = CVV2 is on card, but not legible 9 = Cardholder states no CVV2 is on card

## **Program and Service Format Requirements**

### **Visa Programs**

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48, subelement 92, subfield 2 (CVV2 Response Code)	C	•	C	0 = Only the normal response code in DE 39 should be returned by the issuer 1 = The normal response code and CVV2 response code should be returned by the issuer
DE 48, subelement 92, subfield 3 (CVV2 Value)	C	•	C	CVV2 value; right-justified and blank-filled

---

### **Authorization Request Response/0110—Visa CVV2**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48, subelement 87 (CVV2 Response)	C	•	C	Contains one of the following CVV2 response codes: M = CVV2 match N = CVV2 no match P = Not processed S = CVV2 is on the card, but the Merchant has indicated that CVV2 is not present U = Issuer is not Visa-certified for CVV2, has not provided Visa encryption keys, or both
DE 48, subelement 92 (CVV2 Data)	CE	•	CE	Must be the same value as in the original Authorization/0100 message.

---

### **Visa Fleet Card ID**

Following are Visa Fleet Card ID Authorization/01xx message layouts.

### **Authorization Request/0100—Visa Fleet Card ID**

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number [PAN])	M	•	M	PAN begins with 4 indicating a Visa card.
DE 48 (Additional Data—Private Use), subelement 93 (Fleet Card ID Request Data), subfield 1 (Fleet Card ID Request Indicator)	C	•	C	Contains request indicator value “\$” for Fleet Card.
DE 48, subelement 93, subfield 2 (Optional Free-form Informational Text)	C	•	C	Contains free-form information text. Additional Point-of-Service (POS) information.

**NOTE**

**The Authorization Platform does not forward DE 48, subelement 93 back to the acquirer in Authorization Request Response/0110 messages.**

## Visa Commercial Card Inquiry

Following are Visa Commercial Card Inquiry Authorization/01xx message layouts.

### Authorization Request/0100—Visa Commercial Card Inquiry

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply.

Data Element	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number [PAN])	M	•	M	PAN begins with 4 indicating a Visa card.
DE 48 (Additional Data—Private Use), subelement 94 (Commercial Card Inquiry Request), subfield 1 (Card Request Indicator)	C	•	C	!01 = Request indicator for Commercial Card
DE 48, subelement 94, subfield 2 (Merchant Request for Commercial Card Type)	C	•	C	0 = Merchant request for Commercial Card type

### Authorization Request Response/0110—Visa Commercial Card Inquiry

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request Response/0110 data elements apply.

## **Program and Service Format Requirements**

### **Visa Programs**

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48 (Additional Data—Private Use), subelement 94 (Commercial Card Inquiry Request), subfield 1 (Card Request Indicator)	C	•	C	!01 = Request indicator for Commercial Card
DE 48, subelement 94, subfield 2 (Merchant Request for Commercial Card Type)	C	•	C	Contains one of the following values: 0 = Decline or not a Commercial Card B = Business Card R = Corporate Card S = Purchase Card