



# Customer Interface Specification

9 April 2019

# Summary of Changes, 9 April 2019

This document reflects changes since the 9 October 2018 publication.

Description of Change	Where to Look
<b>Message Definitions and Flows</b>	
<p>Rewrote the following sections in their entirety to reflect changes to cryptographic key blocks:</p> <ul style="list-style-type: none"> <li>• Network Management Request/0800—PEK Exchange Authorization Platform-Initiated</li> <li>• Network Management Request/0800—PEK Exchange Member-Initiated</li> </ul>	<a href="#">Network Management Request/0800—PEK Exchange Authorization Platform-Initiated</a> <a href="#">Network Management Request/0800—PEK Exchange Member-Initiated</a>
<b>Message Layouts</b>	
<p>Added a row for DE 112 (Additional Data [National Use]) to the tables of data elements applicable to the following messages:</p> <ul style="list-style-type: none"> <li>• Authorization Advice/0120—Acquirer-Generated</li> <li>• Authorization Advice/0120—System-Generated</li> </ul>	<a href="#">Authorization Advice/0120—Acquirer-Generated</a> <a href="#">Authorization Advice/0120—System-Generated</a>
<p>Incorporated the following changes to the table of data elements applicable to the Network Management Request/0800—PEK Exchange message:</p> <ul style="list-style-type: none"> <li>• In the row for DE 48 (Additional Data—Private Use): <ul style="list-style-type: none"> <li>– Replaced the “Mandatory” (M) notation with an “Optional” (O) notation in the Authorization Platform Requirements (Sys) column.</li> <li>– Replaced the “Mandatory” (M) notation with a “Conditional” (C) notation in the Destination Requirements (Dst) column.</li> </ul> </li> <li>• Added a row for DE 110 (Additional Data—2).</li> </ul>	<a href="#">Network Management Request/0800—PEK Exchange</a>
<p>In the table of data elements applicable to the Network Management Request/0800—PEK Exchange On Demand message, revised the comments column for DE 70 (Network Management Information Code) by adding value 163 (Solicitation for Encryption Key Exchange - TR-31 Keyblock) to the list of eligible values.</p>	<a href="#">Network Management Request/0800—PEK Exchange On Demand</a>
<p>Added a row for DE 110 to the table of data elements applicable to the Network Management Request Response/0810—PEK Exchange message.</p>	<a href="#">Network Management Request Response/0810—PEK Exchange</a>

<b>Description of Change</b>	<b>Where to Look</b>
Incorporated the following changes to the table of data elements applicable to the Network Management Advice/0820—PEK Exchange message:	<a href="#">Network Management Advice/0820—PEK Exchange</a>
<ul style="list-style-type: none"> <li>• Revised the comments column for DE 70 by adding values 164 (Encryption TR-31 Block Key Exchange Confirmation of Success) and 165 (Encryption TR-31 Block Key Exchange Advice of Failure) to the list of eligible values.</li> <li>• Added a row for DE 110.</li> </ul>	
<b>Data Element Definitions</b>	
Incorporated the following changes to both the List of Data Elements (Numeric Order) and List of Data Elements (Alphabetic Order) sections:	<a href="#">List of Data Elements (Numeric Order)</a>
<ul style="list-style-type: none"> <li>• Added DE 110 (Additional Data—2).</li> <li>• Updated the Data Representation of DE 54 (Additional Amounts) from “an...120; LLLVAR” to “an...240; LLLVAR”</li> </ul>	<a href="#">List of Data Elements (Alphabetic Order)</a>
In DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), performed the following updates:	<a href="#">Subfield 1—Cardholder Transaction Type Code</a>
<ul style="list-style-type: none"> <li>• Under Values, Cardholder Account Credits, updated value 20 (Purchase Return/Refund) to include the VI category (for Visa activity).</li> <li>• Updated the Application Notes as follows: <ul style="list-style-type: none"> <li>– Deleted the following language: “Value 20 is allowed for issuers participating in the Swedish Domestic Authorization Switching Service (SASS) for Private Label, Mastercard, and Maestro branded transactions.”</li> <li>– Added language to indicate that value 20 (Purchase Return/Refund) will be allowed for Visa gateway capabilities to support the authorization of returns or refunds effective with Release 19.Q2.</li> </ul> </li> </ul>	
Under DE 22 (Point-of-Service [POS] Entry Mode), Authorization Platform Edits, added new section Mastercard Consumer Presented QR Transactions with new edits.	<a href="#">Mastercard Consumer Presented QR Transactions</a>
In DE 22 (Point-of-Service [POS] Entry Mode), Authorization Platform Edits, Chip Transactions, updated the sixth Authorization edit to reflect the enablement of DE 22, subfield 1 (POS Terminal PAN Entry Mode), value 03 (PAN auto-entry via barcode reader) for transactions containing chip data.	<a href="#">Chip Transactions</a>
In DE 38 (Approval Code), position 6, added the following new values: <ul style="list-style-type: none"> <li>• Q—Level 5 (Small Business Spend Processing)</li> <li>• R—Level 5 (Small Business Spend Processing and Product Graduation)</li> </ul>	<a href="#">DE 38—Authorization ID Response</a>

Description of Change	Where to Look
DE 39 (Response Code), revised the “Application Notes” section by adding a portion to the table to reflect that if an issuer provides a response code value of 30 (Message format error), then the Issuer Processing System (IPS) also provides DE 44 with six positions for data element and subelement format errors (For example, 0480nn for DE48 subelement nn), or three positions if no subelements are present (For example, 022 for DE 22)	<a href="#">DE 39—Response Code</a>
<p>In the following sections under DE 39 (Response Code), modified the footnote applied to response code 65 (Exceeds withdrawal count limits) to include card-not-present transaction and explain how e-Commerce merchants should trigger an authentication using Mastercard Identity Check/Mastercard SecureCode following an authorization decline with response code 65:</p> <ul style="list-style-type: none"> <li>• Authorization Request Response/0110 Response Codes</li> <li>• Authorization Advice/0120 Response Codes</li> </ul>	<a href="#">Authorization Request Response/0110 Response Codes</a> <a href="#">Authorization Advice/0120 Response Codes</a>
<p>In DE 44 (Additional Response Data), replaced the language of the introductory paragraph—starting with the third sentence—as follows:</p> <ul style="list-style-type: none"> <li>• Previous language: “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.”</li> <li>• New language: “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, DE 44 will contain either a three- or six-digit value that indicates the data element number (three digits) only or the data element plus subelement numbers (six digits) in which the format error occurred. If the format error occurred in a data element that does not have subelements, DE 44 will contain a three-digit numeric value.”</li> </ul>	<a href="#">DE 44—Additional Response Data</a>
<p>In DE 44, DE 44 Values by Program or Service, updated the table to reflect that if DE 39 contains value 30, then DE 44 contains either the data element only, or the data element and subelement when a format error is detected.</p>	<a href="#">DE 44 Values by Program or Service</a>

<b>Description of Change</b>	<b>Where to Look</b>
In the usage table for DE 48 (Additional Data—Private Use), revised the row for Network Management Request/0800—PEK Exchange messages by:	<a href="#">DE 48—Additional Data—Private Use</a>
<ul style="list-style-type: none"> <li>• Replacing the “Mandatory” (M) notation with an “Optional” (O) notation in the Authorization Platform Requirements (Sys) column.</li> <li>• Replacing the “Mandatory” (M) notation with a “Conditional” (C) notation in the Destination Requirements (Dst) column.</li> </ul>	
In DE 48, List of DE 48 Subelements, performed the following updates:	<a href="#">List of DE 48 Subelements</a>
<ul style="list-style-type: none"> <li>• Updated the Data Representation of subelement 21 (Acceptance Data) from (n-5; LLVAR) to (n...11; LLVAR).</li> <li>• Renamed subelements 28–29 (Reserved for Future Use), Data Representation (N/A), as follows: <ul style="list-style-type: none"> <li>– Subelement 28 (Cardless ATM Order ID), Data Representation (an-10)</li> <li>– Subelement 29 (Additional POS Terminal Locations), Data Representation (an-1)</li> </ul> </li> </ul>	
In DE 48, subelement 21 (Acceptance Data), performed the following updates to the Attributes table:	<a href="#">Subelement 21—Acceptance Data</a>
<ul style="list-style-type: none"> <li>• Updated the Data Representation from (n-5; LLVAR) to (n...11; LLVAR).</li> <li>• Updated the number of subfields from (1) to (2).</li> </ul>	
In DE 48, subelement 21 (Acceptance Data), added new subfield 2 (Additional Terminal Capability Indicator).	<a href="#">Subfield 02—Additional Terminal Capability Indicator</a>
In DE 48, added new subelements 28 (Cardless ATM Order ID) and 29 (Additional POS Terminal Locations).	<a href="#">Subelement 28—Cardless ATM Order ID</a> <a href="#">Subelement 29—Additional POS Terminal Locations</a>
In DE 48, subelement 38 (Account Category), added the following new values:	<a href="#">Subelement 38—Account Category</a>
<ul style="list-style-type: none"> <li>• Q = Level 5 (Small Business Spend Processing)</li> <li>• R = Level 5 (Small Business Spend Processing and Product Graduation)</li> </ul>	

---

<b>Description of Change</b>	<b>Where to Look</b>
<p>In DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), performed the following updates:</p> <ul style="list-style-type: none"> <li>• In position 2 (Cardholder Authentication), updated the description of existing Security Level Indicator (SLI) value 4 from "Digital Secure Remote Payment (DSRP) with UCAF data" to "Tokenized payment."</li> <li>• In position 3 (UCAF Collection Indicator), updated the description of existing Security Level Indicator (SLI) value 4 from "Reserved for future use" to "Merchant has chosen to share authentication data within authorization; UCAF data collection not supported."</li> </ul>	<a href="#">Subfield 1—Electronic Commerce Security Level Indicator and UCAF Collection Indicator</a>
<p>In DE 48, subelement 43 (3-D Secure for Mastercard SecureCode), added the following new SPA2 values for the indicated SPA1 values to support enhancements to AAV Validation for EMV 3-D Secure:</p> <ul style="list-style-type: none"> <li>• For SPA1 value = j: <ul style="list-style-type: none"> <li>– Added new SPA2 values kA, kB, kC, kD, kO, kP</li> </ul> </li> <li>• For SPA1 value = h: <ul style="list-style-type: none"> <li>– Added new SPA2 values kE, kF, kN</li> </ul> </li> </ul>	<a href="#">Subelement 43—3-D Secure for Mastercard SecureCode</a>

---

---

Description of Change	Where to Look
<p>In DE 48, subelement 56 (Security Services Additional Data for Issuers), Subelement 56—Valid Subfield 1 (Security Services Indicator) and Subfield 2 (Security Services Data) Value Combinations, Service Data Content for Decision Intelligence Service—Digital Transaction Insights Feature, performed the following updates to the table to support Mastercard Digital Transaction Insights:</p>	<a href="#">Subelement 56—Valid Subfield 1 and Subfield 2 Value Combinations</a>
<ul style="list-style-type: none"> <li>• Updated column headings as follows: <ul style="list-style-type: none"> <li>– From “Assurance Insights” to “Security Services Indicator.”</li> <li>– From “Assurance Level” to “Risk Level.”</li> <li>– From “Reason Code 1 and Reason Code 2” to two separate column headings, “Reason Code 1” (under “Position 2”) and “Reason Code 2” (under “Position 3”).</li> </ul> </li> <li>• Updated Security Services Indicator entry from “AIQ—Assurance IQ” to “AIQ—Digital Transaction Insights.”</li> <li>• Updated Position 1 Risk Level entry from “0–9 where higher values indicate higher degree of assurance.” to “0–9 where higher values indicate higher degree of risk.”</li> <li>• Updated reason code descriptions for all reason codes A through J and Z. Updated reason code K-Y (Reserved for future use) to individual reason codes, with separate descriptions, for reason codes K through Y.</li> <li>• Added the following Note below the table:</li> </ul>	
<p><b>NOTE: The above codes depict a potential list of reason codes and an appropriate ordering from negative to positive. This list may be further refined. Reason codes A–H reflect riskier, or less information while reason codes I–Z reflect positive information.</b></p>	
<p>In DE 48, subelement 71 (On-behalf [OB] Services), Subelement 71—Valid Subfield 1 and Subfield 2 Value Combinations, added subfield 2 (OB Result 1) values X (Security platform time out) and Z (Security platform system error) for each of the following subfield 1 (OB Service) values:</p>	<a href="#">Subelement 71—Valid Subfield 1 and Subfield 2 Value Combinations</a>
<ul style="list-style-type: none"> <li>• 51 (Mastercard Digital Enablement Service Chip Pre-Validation)</li> <li>• 61 (Mastercard Digital Enablement Service Cloud-based Payments Chip Pre-Validation Service)</li> <li>• 62 (Mastercard Digital Enablement Service Cloud-based Payments Magnetic Stripe Pre-Validation Service)</li> </ul>	
<p>In DE 48, subelement 77 (Funding/Payment Transaction Type Indicator), added the following new payment type value to uniquely identify ATM withdrawal transactions initiated via the Mastercard ATM Cash Pick-Up service:</p>	<a href="#">Subelement 77—Funding/Payment Transaction Type Indicator</a>
<ul style="list-style-type: none"> <li>• P01 (ATM Cash Pick-Up Transaction)</li> </ul>	

---

<b>Description of Change</b>	<b>Where to Look</b>
<p>In DE 54 (Additional Amounts), performed the following updates:</p> <ul style="list-style-type: none"> <li>• In Attributes, Data Representation, updated (an...120; LLLVAR) to (an...240; LLLVAR), and updated (not to exceed 120) to (not to exceed 240).</li> <li>• In Application Notes, updated the Real-time Substantiation application note to accommodate new DE 54, subfield 2 (Amount Type), value 12 (Vision Rx Eligibility Amount).</li> </ul>	<a href="#">DE 54—Additional Amounts</a>
<p>In DE 54, subfield 2 (Amount Type), Example Values, updated value 12 from (Reserved for future use) to (Vision Rx Eligibility Amount).</p>	<a href="#">Subfield 2—Amount Type</a>
<p>In DE 55—Subelement Encoding Scheme, revised the introductory statement by:</p> <ul style="list-style-type: none"> <li>• Removing references to Basic Encoding Rules (BER).</li> <li>• Clarifying that the details regarding the coding of tag-length-value (TLV) data objects are found in Book 3 of the EMV Specification.</li> </ul>	<a href="#">DE 55—Subelement Encoding Scheme</a>
<p>In DE 55—Subelements, added the following new subelements to the table of optional subelements in Authorization Request/0100 messages that contain chip data:</p> <ul style="list-style-type: none"> <li>• 5F34—Application Primary Account Number (PAN) Sequence Number</li> <li>• 9F0A—Application Selection Registered Proprietary Data</li> <li>• 9F6E—Third Party Data</li> </ul>	<a href="#">DE 55—Subelements</a>
<p>In DE 55—Authorization Platform Edits, updated the fourth Authorization edit to reflect the enablement of DE 22, subfield 1, value 03 for transactions containing chip data.</p>	<a href="#">DE 55—Authorization Platform Edits</a>
<p>In DE 61 (Point-of-Service [POS] Data), subfield 3 (POS Terminal Location), added new value 8 (Additional POS Terminal Locations).</p>	<a href="#">Subfield 3—POS Terminal Location</a>

<b>Description of Change</b>	<b>Where to Look</b>
<p>In DE 63 (Network Data), subfield 1 (Financial Network Code), added the following new product codes:</p> <ul style="list-style-type: none"> <li>• Added the following new commercial credit Business-to-Business (B2B) brand product code for future B2B programs: <ul style="list-style-type: none"> <li>– MES (Mastercard Enterprise Solution)</li> </ul> </li> <li>• Added the following two new consumer prepaid card product codes for Platinum Mastercard Prepaid Consumer General Spend to be issued in the Asia/Pacific region: <ul style="list-style-type: none"> <li>– MGS (Platinum Mastercard® Prepaid General Spend)</li> <li>– MRD (Platinum Debit Mastercard® Prepaid General Spend)</li> </ul> </li> <li>• Added the following new consumer prepaid card product code for Prepaid Gold Payroll to be issued in the Latin America and the Caribbean and Middle East/Africa regions: <ul style="list-style-type: none"> <li>– MGP (Mastercard® Prepaid Gold Payroll)</li> </ul> </li> <li>• Added the following 11 new commercial card product codes for use with virtual card transactions acquired in the U.S. region:</li> </ul>	<a href="#">Subfield 1—Financial Network Code</a>
<p><b>NOTE: These 11 product codes are not available for ATM or manual cash disbursement transactions.</b></p> <ul style="list-style-type: none"> <li>– MVA (Mastercard® B2B VIP 1)</li> <li>– MVB (Mastercard® B2B VIP 2)</li> <li>– MVC (Mastercard® B2B VIP 3)</li> <li>– MVD (Mastercard® B2B VIP 4)</li> <li>– MVE (Mastercard® B2B VIP 5)</li> <li>– MVF (Mastercard® B2B VIP 6)</li> <li>– MVG (Mastercard® B2B VIP 7)</li> <li>– MVH (Mastercard® B2B VIP 8)</li> <li>– MVI (Mastercard® B2B VIP 9)</li> <li>– MVJ (Mastercard® B2B VIP 10)</li> <li>– MVK (Mastercard® B2B VIP 11)</li> </ul>	
<p>In DE 70 (Network Management Information Code), Network Management Request/0800—PEK Exchange, revised the description of value 161 from “Encryption key exchange request” to “Encryption key exchange.”</p>	<a href="#">Network Management Request/0800—PEK Exchange</a>
<p>In DE 70, Network Management Request/0800—PEK Exchange-On Demand, incorporated the following changes:</p> <ul style="list-style-type: none"> <li>• Revised the description of value 162 from “Solicitation for key exchange request” to “Solicitation for Encryption Key Exchange.”</li> <li>• Added value 163 (Solicitation for Encryption Key Exchange - TR-31 Keyblock)</li> </ul>	<a href="#">Network Management Request/0800—PEK Exchange-On Demand</a>

---

<b>Description of Change</b>	<b>Where to Look</b>
In DE 70, added new sections dedicated to the DE 70 values that apply to each of the following message types:	<a href="#">Network Management Request Response/0810—PEK Exchange</a>
<ul style="list-style-type: none"> <li>• Network Management Request Response/0810—PEK Exchange</li> <li>• Network Management Advice/0820—PEK Exchange</li> </ul>	<a href="#">Network Management Advice/0820—PEK Exchange</a>
Added new DE 110 (Additional Data—2) and the following new subfields:	<a href="#">DE 110—Additional Data—2</a>
<ul style="list-style-type: none"> <li>• Subelement 9—ANSI X9 TR-31 Key Block Key (128-bit Key Block Protection Key)</li> <li>• Subelement 9—ANSI X9 TR-31 Key Block Key (192-bit Key Block Protection Key)</li> <li>• Subelement 10—Key Check Value</li> </ul>	<a href="#">Subelement 9—ANSI X9 TR-31 Key Block Key (128-bit Key Block Protection Key)</a> <a href="#">Subelement 9—ANSI X9 TR-31 Key Block Key (192-bit Key Block Protection Key)</a> <a href="#">Subelement 10—Key Check Value</a>
In DE 112 (Additional Data [National Use]), incorporated the following changes:	<a href="#">DE 112—Additional Data (National Use)</a>
<ul style="list-style-type: none"> <li>• Updated the Data Representation for Japan domestic usage from (ans-144) to (ans...195; LLLVAR).</li> <li>• Updated the Usage section as follows: <ul style="list-style-type: none"> <li>– In the row for Authorization Advice/0120—Issuer-generated messages: <ul style="list-style-type: none"> <li>– Replaced the “Not Required or Not Applicable” (•) notation with a “Conditional” (C) notation in the Authorization Platform Requirements (Sys) column.</li> <li>– Replaced the “Conditional” (C) notation with a “Not Required or Not Applicable” (•) notation in the Destination Requirements (Dst) column.</li> <li>– Added a row for Authorization Advice/0120—System-generated messages.</li> </ul> </li> </ul> </li> </ul>	

---

---

<b>Description of Change</b>	<b>Where to Look</b>
In DE 112, Brazil—Payment Transactions, added the following new subelements:	<a href="#">Subelement 013—Crediário First Simulation</a>
<ul style="list-style-type: none"> <li>• Subelement 013—Crediário First Simulation</li> <li>• Subelement 014—Crediário Second Simulation</li> <li>• Subelement 015—Crediário Third Simulation</li> <li>• Subelement 019—Original Purchase Amount</li> </ul>	<a href="#">Subelement 014—Crediário Second Simulation</a>
	<a href="#">Subelement 015—Crediário Third Simulation</a>
	<a href="#">Subelement 019—Original Purchase Amount</a>
In DE 112, Japan—Payment Transactions, performed the following updates:	<a href="#">Subelement 030—Japan Domestic POS Data</a>
<ul style="list-style-type: none"> <li>• In subelement 030 (Japan Domestic POS Data), Values, position 105 (Authorization Transmission Mode), deleted value 0 (Online) and added value 2 (Online).</li> </ul>	<a href="#">Subelement 031—Japan Domestic Response Code</a>
<ul style="list-style-type: none"> <li>• In subelement 030 (Japan Domestic POS Data), Application Notes, modified the second paragraph as shown (yields same meaning), and added a new third paragraph as follows:</li> </ul>	<a href="#">Subelement 032—Japan Payment Options</a>
<ul style="list-style-type: none"> <li>– Second paragraph from: “Mastercard does not validate the contents of DE 112, subelement 030 if provided.”</li> <li>– To: “If provided, Mastercard does not validate the contents of DE 112, subelement 030.”</li> <li>– New third paragraph: “If provided, Mastercard will remove subelement 030 from the Authorization Request/0100, Authorization Request Response/0110, Reversal Request/0400, and Reversal Request Response/0410 messages when the acquirer or the issuer country code is not 392 (Japan).”</li> </ul>	
<ul style="list-style-type: none"> <li>• In subelement 031 (Japan Domestic Response Code), added new Application Notes section and the following application note:</li> </ul>	
<ul style="list-style-type: none"> <li>– “If present, Mastercard will remove subelement 031 from the Authorization Request Response/0110 and Reversal Request Response/0410 messages when the acquirer or the issuer country code is not 392 (Japan).”</li> </ul>	
<ul style="list-style-type: none"> <li>• In subelement 032 (Japan Payment Options), Application Notes, modified the second paragraph and added a new third paragraph as follows:</li> </ul>	
<ul style="list-style-type: none"> <li>– In the second paragraph, removed the following final sentence: “Subelement 032 should not be included on a cross-border transaction as non-Japan issuers may decline the transaction.”</li> <li>– Added the following new third paragraph: “Mastercard will remove subelement 032 from the Authorization Request/0100, Authorization Request Response/0110, Reversal Request/0400, and Reversal Request Response/0410 messages when the acquirer or the issuer country code is not 392 (Japan).”</li> </ul>	

---

<b>Description of Change</b>	<b>Where to Look</b>
<p>In DE 112, added the “Netherlands—IBAN—Account Inquiry” section under which new subelement 037 (Additional Cardholder Information), containing the following new subfields, has been added:</p>	<a href="#">Netherlands—IBAN—Account Inquiry</a>
<ul style="list-style-type: none"> <li>• Subfield 01—Primary Cardholder Identifier</li> <li>• Subfield 02—Secondary Cardholder Identifier</li> </ul>	<a href="#">Subelement 037—Additional Cardholder Information</a>
<a href="#">Subfield 01—Primary Cardholder Identifier</a>	
<a href="#">Subfield 02—Secondary Cardholder Identifier</a>	
<p>In DE 112, Parcelas—Payment Transactions, Subelement 001—Installment Payment Data, added value 25 (Crediário) to the list of values for both of the following message types:</p>	<a href="#">Subelement 001—Installment Payment Data</a>
<ul style="list-style-type: none"> <li>• Parcelas Payment Transactions in the Authorization Request/0100</li> <li>• Parcelas Payment Transactions in the Authorization Request Response/0110</li> </ul>	
<b>Program and Service Format Requirements</b>	
<p>In Contactless CVC 3 Processing Service, updated the first sentence of the definition of the Dynamic CVC 3 Pre-validation Service as follows:</p>	<a href="#">Contactless CVC 3 Processing Service</a>
<ul style="list-style-type: none"> <li>• Old language: This is a mandated service for issuers with contactless-enabled authorization systems that do not support dynamic CVC 3 validation.</li> <li>• New language: This is an optional, stand-alone service for issuers with contactless-enabled authorization systems that do not support dynamic CVC 3 validation.</li> </ul>	
<p>In Electronic Commerce Processing, Mastercard SecureCode, clarified the language in the “Accountholder Authentication Value” subsection to indicate the following:</p>	<a href="#">Mastercard SecureCode</a>
<ul style="list-style-type: none"> <li>• Customers must perform AAV validation of Authorization Request/0100 messages, either via their own self-validation process or through the Mastercard SecureCode AAV Verification service.</li> <li>• All customers must participate in Mastercard SecureCode Dynamic AAV Verification in Stand-In Processing.</li> </ul>	
<p>In Real-Time Substantiation, Real-Time Substantiation Amounts, updated existing paragraphs, and added a new paragraph, to accommodate new DE 54, subfield 2 (Amount Type), value 12 (Vision Rx Eligibility Amount).</p>	<a href="#">Real-Time Substantiation Amounts</a>
<p>In Real-Time Substantiation, Transaction Processing Examples, added new examples of Real-time Substantiation transaction processing that feature transactions containing DE 54, subfield 2, value 12.</p>	<a href="#">Transaction Processing Examples</a>

Description of Change	Where to Look
In Real-Time Substantiation, Authorization Platform Edits, revised the Authorization Platform edits that the system performs on Real-time Substantiation transactions. Also added two notes.	<a href="#">Authorization Platform Edits</a>

# Contents

## Summary of Changes, 9 April 2019..... 2

## Chapter 1: Overview..... 44

Customer Interface Specification Format.....	45
Issuer Post-on-Authorization.....	46
Bit Mapped Message Encoding Scheme.....	47
Authorization Platform Processing Terms and Acronyms.....	47
Customer Interface Specification Notations.....	48
Data Length Notations.....	48
Data Representation Notations.....	49
Data Field Notations.....	50
Data Justification Notations.....	50
Date and Time Notations.....	50
Entity Notations.....	51
Presence Notations.....	52
Presence Requirement Notations.....	52
Program and Service Category Notations.....	53
Authorization Platform Messages.....	54
List of Authorization Messages.....	54
Message Type Identifier Presence Requirements by Program and Service.....	56
Character Sets.....	57
Character Sets.....	58
Extended Character Sets.....	66
Swedish Domestic Authorization Switching Character Set.....	71

## Chapter 2: Message Definitions and Flows..... 73

About Message Definitions.....	76
About Authorization Messages.....	76
Authorization Request/0100.....	76
Authorization Request Response/0110.....	76
About Authorization Advice Messages.....	77
Authorization Advice/0120—Acquirer-Generated.....	77
Authorization Advice/0120—Issuer-Generated.....	78
Authorization Advice/0120—System-Generated.....	78
Authorization Advice Response/0130—Issuer-Generated (Responding to an Acquirer-Generated 0120).....	79
Authorization Advice Response/0130—Issuer-Generated (Responding to a System-Generated 0120 from SAF).....	79
Authorization Advice Response/0130—System-Generated.....	79

About Authorization Response Acknowledgement Messages.....	79
Authorization Acknowledgement/0180.....	80
Authorization Negative Acknowledgement/0190.....	80
About Issuer File Update Messages.....	80
Issuer File Update Request/0302.....	80
Issuer File Update Request Response/0312.....	81
About Reversal Messages.....	81
Reversal Request/0400.....	81
Reversal Request Response/0410.....	81
Reversal Advice/0420.....	82
Reversal Advice Response/0430.....	82
About Administrative Messages.....	82
Administrative Request/0600.....	83
Administrative Request Response/0610.....	83
Administrative Advice/0620.....	83
Administrative Advice Response/0630.....	84
About Network Management Messages.....	84
Network Management Request/0800.....	85
Network Management Request Response/0810.....	85
Network Management Advice/0820.....	85
About Message Flows.....	86
Authorization Message Routing Timers.....	86
Authorization Request/0100 and Authorization Request Response/0110.....	87
Authorization Request/0100—Communication Failure at Acquirer.....	88
Authorization Request/0100—Communication Failure at Issuer.....	88
Authorization Request Response/0110—Communication Failure at Acquirer.....	90
Authorization Request Response/0110—Communication Failure at Issuer.....	91
Authorization Request Response/0110—Stand-In System Allowed.....	92
Authorization Request Response/0110—Not Received within the Time Limit.....	92
Authorization Request Response/0110—Received within the Time Limit but after Stand-In System Response.....	93
Authorization Request Response/0110—Received within the Time Limit and before Stand-In System Response.....	94
Authorization Request Response/0110—Not Eligible for Alternate Processing.....	95
Authorization Request Response/0110—No Issuer Response within Issuer Response Time Limit.....	96
Authorization Request Response/0110—Late Issuer Response.....	96
Authorization Request Response/0110—Issuer Edit Error.....	97
Authorization Request/0100—Chip PIN Management.....	98
Authorization Request/0100—Chip PIN Management (Failure to Transmit/Apply Script to Chip Card).....	99
Authorization Request/0100—Chip PIN Management (Issuer Network Failure— Unable to Connect).....	101

Authorization Request/0100—Chip PIN Management (Issuer Network Failure, No Response from Issuer).....	102
Authorization Request/0100—Chip PIN Management (Acquirer Network Failure-Unable to Connect).....	104
Authorization Request/0100—Chip PIN Management (Acquirer Network Failure-Unable to Connect with Acquirer).....	105
Guaranteed Advice Message Delivery.....	106
Standard Advice Delivery—All Advice Message Types.....	107
Authorization Advice/0120—Acquirer-Generated, Issuer Available.....	107
Authorization Advice/0120—Acquirer-Generated, Issuer Unavailable.....	108
Authorization Advice/0120—Issuer-Generated.....	109
Authorization Advice/0120—System-Generated.....	109
Advice Message Error Condition.....	110
Acquirer Response Acknowledgement/0180 Messages.....	111
Alternate Issuer Host Processing for Online Europe Region Customers.....	112
Authorization Request/0100—Communication Failure at Issuer (Issuer is not signed in or transaction cannot be delivered).....	113
Authorization Request Response/0110—Alternate Issuer Allowed.....	113
Authorization Request Response/0110—Not Received within Time Limit.....	115
Authorization Request Response/0110—Received within the Time Limit but after Alternate Issuer Response.....	116
Authorization Request Response/0110—Received within the Time Limit and before Alternate Issuer Response.....	117
Authorization Response Negative Acknowledgement/0190 (Responding to the Authorization Request Response/0110).....	118
Authorization Response Negative Acknowledgement/0190 (Responding to the Reversal Request Response/0410).....	118
Issuer File Update Request/0302 and Issuer File Update Request Response/0312.....	119
Reversal Messages.....	120
Reversal Request/0400 and Reversal Request Response/0410.....	120
Reversal Request/0400—No Issuer Response Received within the Time Limit.....	121
Reversal Request/0400—Issuer Response Received after the Time Limit.....	122
Reversal Request/0400—Issuer Signed Off.....	122
Reversal Request/0400—Issuer Response Contains Errors.....	123
Reversal Request/0400—Not Delivered to Issuer.....	124
Reversal Request Response/0410—Not Delivered to Acquirer.....	125
Reversal Advice/0420 and Reversal Advice Response/0430.....	125
Administrative Request/0600 and Administrative Request Response/0610.....	126
Administrative Request/0600, Acquirer Edit Failure.....	126
Administrative Request/0600, Communication Failure at Issuer.....	127
Administrative Request Response/0610, Communication Failure at Acquirer.....	127
Administrative Request Response/0610, No Issuer Response.....	128
Administrative Request Response/0610, Late Issuer Response.....	128

Administrative Request Response/0610, Issuer Edit Failure.....	129
Administrative Advice/0620 and Administrative Advice Response/0630.....	129
Administrative Advice/0620 and Administrative Advice Response/0630—Invalid Message, System-Generated.....	130
Network Management Request 0800—Sign-On/Sign-Off.....	130
Network Management Request/0800—Solicited SAF.....	131
Network Management Request/0800—Unsolicited SAF.....	132
Network Management Request/0800—Network Connection Status, Member- Generated.....	133
Network Management Request/0800—Network Connection Status, System- Generated.....	133
Network Management Request/0800—Host Session Activation/Deactivation.....	134
Network Management Request/0800—PEK Exchange Authorization Platform- Initiated.....	134
Network Management Request/0800—PEK Exchange Member-Initiated.....	135
<b>Chapter 3: Message Layouts.....</b>	<b>137</b>
Authorization Request/0100.....	139
Authorization Request Response/0110.....	143
Authorization Advice/0120—Acquirer-Generated.....	147
Authorization Advice/0120—Issuer-Generated.....	151
Authorization Advice/0120—System-Generated.....	154
Authorization Advice Response/0130—Issuer-Generated (Responding to a System- Generated 0120 from SAF).....	158
Authorization Advice Response/0130—Issuer-Generated (Responding to an Acquirer- Generated 0120 Response or an Authorization Advice Request 0120).....	160
Authorization Advice Response/0130—System-Generated (Responding to an Acquirer- Generated 0120).....	163
Authorization Advice Response/0130—System-Generated (Responding to an Issuer- Generated 0120).....	165
Authorization Response Acknowledgement/0180.....	167
Authorization Response Negative Acknowledgement/0190.....	167
Issuer File Update Request/0302.....	168
Issuer File Update Request Response/0312.....	169
Reversal Request/0400.....	171
Reversal Request Response/0410.....	176
Reversal Advice/0420.....	179
Reversal Advice Response/0430.....	183
Administrative Request/0600.....	185
Administrative Request Response/0610.....	186
Administrative Advice/0620—System-Generated.....	188
Administrative Advice/0620—Member-Generated.....	189
Administrative Advice Response/0630.....	190

Network Management Request/0800—Sign-On/Sign-Off.....	191
Network Management Request/0800—Network Connection Status, Member-Generated.....	193
Network Management Request/0800—Network Connection Status, System-Generated.	193
Network Management Request/0800—Host Session Activation/Deactivation.....	194
Network Management Request/0800—PEK Exchange.....	195
Network Management Request/0800—PEK Exchange On Demand.....	196
Network Management Request Response/0810—Sign-On/Sign-Off.....	197
Network Management Request Response/0810—Network Connection Status, Member-Generated.....	198
Network Management Request Response/0810—Network Connection Status, System-Generated.....	199
Network Management Request Response/0810—Host Session Activation/Deactivation .	200
Network Management Request Response/0810—PEK Exchange.....	200
Network Management Request Response/0810—PEK Exchange-On Demand.....	201
Network Management Advice/0820—PEK Exchange.....	202
<b>Chapter 4: Data Element Definitions.....</b>	<b>204</b>
Data Element Layout.....	223
Subelement Layout.....	223
Subfield Layout.....	224
Position Layout.....	224
List of Data Elements (Numeric Order).....	224
List of Data Elements (Alphabetic Order).....	229
Message Type Identifier.....	233
Message Types and Applicable Program or Service.....	236
About Primary and Secondary Bit Maps.....	237
Primary Bit Map.....	237
DE 1—Bit Map, Secondary.....	239
DE 2—Primary Account Number (PAN).....	241
About Primary Account Number.....	243
DE 3—Processing Code.....	244
Subfield 1—Cardholder Transaction Type Code.....	246
Subfield 2—Cardholder "From Account" Type Code.....	248
Subfield 3—Cardholder "To Account" Type Code.....	249
DE 4—Amount, Transaction.....	250
DE 5—Amount, Settlement.....	254
DE 6—Amount, Cardholder Billing.....	255
DE 7—Transmission Date and Time.....	257
Subfield 1—Date.....	259
Subfield 2—Time.....	260
DE 8—Amount, Cardholder Billing Fee.....	260

DE 9—Conversion Rate, Settlement.....	260
Subfield 1—Decimal Indicator.....	262
Subfield 2—Conversion Rate.....	262
DE 10—Conversion Rate, Cardholder Billing.....	263
Subfield 1—Decimal Indicator.....	264
Subfield 2—Cardholder Billing Conversion Rate.....	264
DE 11—System Trace Audit Number (STAN).....	265
DE 12—Time, Local Transaction.....	267
DE 13—Date, Local Transaction.....	268
DE 14—Date, Expiration.....	269
DE 15—Date, Settlement.....	270
DE 16—Date, Conversion.....	271
DE 17—Date, Capture.....	272
DE 18—Merchant Type.....	273
DE 19—Acquiring Institution Country Code.....	274
DE 20—Primary Account Number (PAN) Country Code.....	275
DE 21—Forwarding Institution Country Code.....	276
DE 22—Point-of-Service (POS) Entry Mode.....	276
Subfield 1—POS Terminal PAN Entry Mode.....	278
Subfield 2—POS Terminal PIN Entry Mode.....	279
Authorization Platform Edits.....	280
Mastercard Electronic Card Transactions.....	280
Mastercard Consumer Presented QR Transactions.....	280
Chip Transactions.....	281
Magnetic Stripe or Chip-Read Transactions for Mastercard Electronic Card.....	283
Contactless Magnetic Stripe Transactions.....	284
Credential on File Transactions.....	285
DE 23—Card Sequence Number.....	285
DE 24—Network International ID.....	287
DE 25—Point-of-Service (POS) Condition Code.....	288
DE 26—Point-of-Service (POS) Personal ID Number (PIN) Capture Code.....	288
DE 27—Authorization ID Response Length.....	289
DE 28—Amount, Transaction Fee.....	290
Subfield 1—Debit/Credit Indicator.....	291
Subfield 2—Amount.....	292
DE 29—Amount, Settlement Fee.....	292
Subfield 1—Debit/Credit Indicator.....	293
Subfield 2—Amount.....	293
DE 30—Amount, Transaction Processing Fee.....	293
Subfield 1—Debit/Credit Indicator.....	294
Subfield 2—Amount.....	294
DE 31—Amount, Settlement Processing Fee.....	294
Subfield 1—Debit/Credit Indicator.....	295

---

Subfield 2—Amount.....	295
DE 32—Acquiring Institution ID Code.....	296
DE 33—Forwarding Institution ID Code.....	297
DE 34—Primary Account Number (PAN), Extended.....	299
DE 35—Track 2 Data.....	300
DE 36—Track 3 Data.....	301
DE 37—Retrieval Reference Number.....	302
Subfield 1—Transaction Date and Initiator Discretionary Data.....	304
Subfield 2—Terminal Transaction Number.....	304
DE 38—Authorization ID Response.....	304
DE 39—Response Code.....	306
Authorization Request Response/0110 Response Codes.....	309
Authorization Advice/0120 Response Codes.....	311
Authorization Advice Response/0130 Response Codes.....	313
Authorization Advice Response/0180 Response Codes.....	314
Authorization Negative Acknowledgement/0190 Response Codes.....	314
Issuer File Update Request Response/0312 Response Codes.....	314
Reversal Request/0400 Message Response Codes.....	315
Reversal Request Response/0410 Response Codes.....	317
Reversal Advice/0420 Response Codes.....	318
Reversal Advice Response/0430 Message and Administrative Advice Response/0630 Response Codes.....	320
Administrative Request Response/0610 Response Codes.....	320
Network Management Request Response/0810 Response Codes.....	321
DE 40—Service Restriction Code.....	321
DE 41—Card Acceptor Terminal ID.....	322
DE 42—Card Acceptor ID Code.....	323
DE 43—Card Acceptor Name/Location for All Transactions.....	324
Subfield 1—Card Acceptor Name (or Payment Facilitator & Sub-Merchant Information, if applicable).....	325
Subfield 2—Space.....	327
Subfield 3—Card Acceptor City (or Sub-Merchant Information, if applicable).....	327
Subfield 4—Space.....	327
Subfield 5—Card Acceptor State or Country Code (or Sub-Merchant Information, if applicable).....	328
DE 43—Card Acceptor Name/Location for ATM Transactions.....	328
Subfield 1—ATM Owning Institution or Terminal/Merchant Address or Both.....	329
Subfield 2—Space.....	329
Subfield 3—ATM or Merchant Location City.....	330
Subfield 4—Space.....	330
Subfield 5—ATM or Merchant State, Province, or Country Code Location.....	330
DE 43—Card Acceptor Name/Location for Bankcard-Activated Public Phones.....	331
Subfield 1—Abbreviation "TEL" .....	332

Subfield 2—Phone Number Dialed.....	332
Subfield 3—Abbreviation "M" .....	333
Subfield 4—Call Duration.....	333
Subfield 5—Space.....	333
Subfield 6—Call Origin City.....	334
Subfield 7—Space.....	334
Subfield 8—Call Origin State or Country Code.....	334
DE 44—Additional Response Data.....	335
DE 44 Values by Program or Service.....	336
Authorization Platform Edits.....	338
DE 45—Track 1 Data.....	339
DE 46—Expanded Additional Amounts.....	340
DE 47—Additional Data—National Use.....	341
DE 48—Additional Data—Private Use.....	341
DE 48 Transaction Category Code.....	343
DE 48 Subelement Encoding Scheme in Authorization Request/0100 Messages.....	344
DE 48 Subelement Encoding Scheme in Network Management Messages.....	345
List of DE 48 Subelements.....	345
Subelement 10—Encrypted PIN Block Key.....	349
Subelement 11—Key Exchange Block Data (Double-Length Keys).....	349
Subelement 11—Key Exchange Block Data (Triple-Length Keys).....	350
Subelement 12—Routing Indicator.....	352
Subelement 13—Mastercard Hosted Mobile Phone Top-Up Request Data.....	352
Subfield 1—Mobile Phone Number.....	353
Subfield 2—Mobile Phone Service Provider Name.....	353
Subelement 14—Account Type Indicator.....	353
Subelement 15—Authorization System Advice Date and Time.....	354
Subfield 1—Date.....	355
Subfield 2—Time.....	355
Subelement 16—Processor Pseudo ICA.....	356
Subelement 17—Authentication Indicator.....	356
Subelement 18—Service Parameters.....	357
Subfield 01—Canada Domestic Indicator.....	358
Subelement 20—Cardholder Verification Method.....	359
Subelement 21—Acceptance Data.....	359
Subfield 01—mPOS Acceptance Device Type.....	360
Subfield 02—Additional Terminal Capability Indicator.....	361
Subelement 23—Payment Initiation Channel.....	362
Subfield 1—Device Type.....	363
Subelement 25—Mastercard Cash Program Data.....	365
Subfield 01—Message Identifier.....	366
Subelement 26—Wallet Program Data.....	366
Subfield 1—Wallet Identifier.....	367

Subelement 27—Transaction Analysis.....	368
Subfield 1—Overview.....	369
Subfield 2—Test Results.....	370
Subelement 28—Cardless ATM Order ID.....	371
Subelement 29—Additional POS Terminal Locations.....	372
Subelement 30—Token Transaction Identifier.....	372
Subelement 32—Mastercard Assigned ID.....	373
Subelement 33—PAN Mapping File Information.....	374
Subfield 1—Account Number Indicator.....	375
Subfield 2—Account Number.....	376
Subfield 3—Expiration Date.....	376
Subfield 4—Product Code.....	377
Subfield 5—Token Assurance Level.....	377
Subfield 6—Token Requestor ID.....	378
Subfield 7—Primary Account Number, Account Range.....	379
Subfield 8—Storage Technology.....	379
Subelement 34—ATC Information.....	380
Subfield 1—ATC Value.....	381
Subfield 2—ATC Discrepancy Value.....	382
Subfield 3—ATC Discrepancy Indicator.....	382
Subelement 34 Subfield Data Examples.....	382
Subelement 35—Contactless Non-Card Form Factor Request/Response.....	383
Subelement 36—Visa MVV (Visa Only).....	384
Subfield 1—Merchant Verification Value (MVV).....	385
Subelement 37—Additional Merchant Data.....	385
Subfield 1—Payment Facilitator ID.....	386
Subfield 2—Independent Sales Organization ID.....	387
Subfield 3—Sub-Merchant ID.....	387
Subelement 38—Account Category.....	388
Subelement 39—Account Data Compromise Information.....	389
Subelement 40—Electronic Commerce Merchant/Cardholder Certificate Serial Number (Visa Only).....	391
Subfield 1—Merchant Certificate Serial Number.....	392
Subfield 2—Cardholder Certificate Serial Number.....	392
Subelement 41—Electronic Commerce Certificate Qualifying Information.....	392
Subfield 1—Reserved for Future Use.....	393
Subfield 2—Reserved for Future Use.....	393
Subfield 3—Reserved for Future Use.....	393
Subfield 4—Reserved for Future Use.....	394
Subfield 5—Reserved for Future Use.....	394
Subfield 6—Reserved for Future Use.....	394
Subfield 7—Reserved for Future Use.....	394
Subfield 8—Reserved for Future Use.....	395

Subfield 9—Reserved for Future Use.....	395
Subfield 10—Reserved for Future Use.....	395
Subfield 11—Citizen ID.....	395
Subfield 12—Reserved for Future Use.....	396
Subfield 13—Reserved for Future Use.....	396
Subfield 14—Reserved for Future Use.....	396
Subfield 15—Reserved for Future Use.....	396
Subfield 16—Reserved for Future Use.....	397
Subfield 17—Reserved for Future Use.....	397
Subfield 18—Reserved for Future Use.....	397
Subelement 42—Electronic Commerce Indicators.....	397
Subfield 1—Electronic Commerce Security Level Indicator and UCAF Collection Indicator.....	399
Subfield 2—Original Electronic Commerce Security Level Indicator and UCAF Collection Indicator.....	402
Subfield 3—Reason for UCAF Collection Indicator Downgrade.....	403
Subelement 43—Universal Cardholder Authentication Field (UCAF).....	404
Subelement 43—3-D Secure for Mastercard <i>SecureCode</i> .....	405
Subelement 43—Digital Secure Remote Payment Universal Cardholder Authentication Field (UCAF).....	406
Subelement 43—Static AAV.....	407
Subelement 43—3-D Secure Electronic Commerce Verification Service (Visa, JCB, Diners Club and American Express Only).....	408
Subelement 44—3-D Secure Electronic Commerce Transaction Identifier (XID) (Visa and American Express).....	409
Subelement 45—3-D Secure Electronic Commerce Transaction Response Code (Visa and American Express).....	410
Subelement 46—Product ID (Visa Only).....	410
Subelement 47—Mastercard Payment Gateway Transaction Indicator.....	411
Subelement 48—Mobile Program Indicators.....	412
Subfield 1—Remote Payments Program Type Identifier.....	413
Subfield 2—Mastercard Mobile Remote Payment Transaction Type.....	413
Subfield 3—Mobile Phone Number.....	414
Subfield 4—Convenience Fee.....	414
Subelement 49—Time Validation Information.....	415
Subfield 1—Time Value.....	415
Subfield 2—Time Discrepancy Value.....	415
Subfield 3—Time Discrepancy Indicator.....	416
Subelement 51—Merchant On-behalf Services.....	416
Subfield 1—Merchant On-behalf (OB) Service.....	417
Subfield 2—Merchant On-behalf (OB) Result 1.....	417
Subelement 51—Valid Subfield 1 and Subfield 2 Value Combinations.....	418
Subfield 3—Additional Information.....	419

Subelement 52—Transaction Integrity Class.....	420
Subelement 53—E-ID Request Code.....	421
Subfield 1—E-ID Request Value.....	422
Subelement 55—Merchant Fraud Scoring Data.....	423
Subfield 1—Merchant Fraud Score.....	424
Subfield 2—Merchant Score Reason Code.....	424
Subfield 3—Reserved for Future Use.....	424
Subfield 4—Reserved for Future Use.....	425
Subfield 5—Reserved for Future Use.....	425
Subelement 56—Security Services Additional Data for Issuers.....	425
Subfield 1—Security Services Indicator.....	427
Subfield 2—Security Services Data.....	427
Subelement 56—Valid Subfield 1 and Subfield 2 Value Combinations.....	427
Subelement 57—Security Services Additional Data for Acquirers.....	433
Subfield 1—Security Services Indicator.....	434
Subfield 2—Security Services Data.....	434
Subelement 58—ATM Additional Data.....	434
Subfield 1—ATM Time.....	435
Subfield 2—ATM Date.....	435
Subfield 3—Watermark.....	436
Subfield 4—Mark 1.....	436
Subfield 5—Mark 2.....	436
Subfield 6—Mark 3.....	437
Subfield 7—Card Swallowed Status.....	437
Subfield 8—Posting Date.....	438
Subelement 61—POS Data Extended Condition Codes.....	438
Subfield 1—Partial Approval Terminal Support Indicator.....	439
Subfield 2—Purchase Amount Only Terminal Support Indicator.....	439
Subfield 3—Real-time Substantiation Indicator.....	439
Subfield 4—Merchant Transaction Fraud Scoring Indicator.....	440
Subfield 5—Final Authorization Indicator.....	441
Subelement 63—Trace ID.....	442
Subelement 64—Transit Program.....	444
Subfield 1—Transit Transaction Type Indicator.....	445
Subfield 2—Transportation Mode Indicator.....	445
Subelement 65—Terminal Compliant Indicator.....	446
Subfield 1—TLE Compliant.....	447
Subfield 2—UKPT/DUKPT Compliant.....	447
Subelement 66—Authentication Data.....	448
Subfield 1—Program Protocol.....	449
Subfield 2—Directory Server Transaction ID.....	449
Subelement 67—MoneySend Information.....	450
Subfield 1—Sanction Screening Score.....	451

Subelement 71—On-behalf Services.....	451
Subfield 1—On-behalf (OB) Service.....	452
Subfield 2—On-behalf Result 1.....	452
Subfield 3—On-behalf Result 2.....	453
Subelement 71—Valid Subfield 1 and Subfield 2 Value Combinations.....	453
Subelement 72—Issuer Chip Authentication.....	463
Subelement 74—Additional Processing Information.....	464
Subfield 1—Processing Indicator.....	465
Subfield 2—Processing Information.....	465
Valid Subfield 1 and Subfield 2 Value Combinations.....	466
Subelement 75—Fraud Scoring Data.....	466
Subfield 1—Fraud Score.....	468
Subfield 2—Score Reason Code.....	468
Subfield 3—Rules Score.....	469
Subfield 4—Rules Reason Code 1.....	469
Subfield 5—Rules Reason Code 2.....	470
Subelement 76—Mastercard Electronic Acceptance Indicator.....	471
Subelement 77—Funding/Payment Transaction Type Indicator.....	472
Subelement 78—Payment Service Indicators (Visa Only).....	474
Subfield 1—Spend Qualified Indicator.....	475
Subfield 2—Dynamic Currency Conversion Indicator.....	475
Subfield 3—U.S. Deferred Billing Indicator.....	476
Subfield 4—Visa Checkout Indicator.....	477
Subfield 5—Message Reason Code.....	477
Subfield 6—Reserved for Future Use.....	478
Subelement 79—Chip CVR/TVR Bit Error Results.....	478
Subfield 1—CVR or TVR Identifier.....	480
Subfield 2—Byte ID.....	480
Subfield 3—Byte Identifier.....	480
Subfield 4—Value of Bit in Error.....	481
Subelement 80—PIN Service Code.....	481
Subelement 82—Address Verification Service Request.....	482
Subelement 83—Address Verification Service Response.....	483
Subelement 84—Merchant Advice Code.....	485
Subelement 84—Visa Response Codes (Visa Only).....	486
Subelement 85—Account Status (Visa Only).....	486
Subelement 86—Relationship Participant Indicator (Visa Only).....	487
Subelement 87—Card Validation Code Result.....	488
Subelement 87—CVV2 Response (Visa Only).....	489
Subelement 88—Magnetic Stripe Compliance Status Indicator.....	490
Subelement 89—Magnetic Stripe Compliance Error Indicator.....	490
Subelement 90—Lodging and Auto Rental Indicator.....	491
Subelement 90—Custom Payment Service Request (Visa Only).....	492

Subelement 90—Custom Payment Service Request Response (Visa Only).....	493
Subelement 91—Acquirer Reference Data (American Express Only).....	494
Subelement 91—Custom Payment Service Request/Transaction ID (Visa Only).....	494
Subelement 91—Custom Payment Service Response/Transaction ID (Visa Only).....	495
Subelement 92—CVC 2.....	496
Subelement 92—CVV2 Data (Visa Only).....	497
Subelement 93—Fleet Card ID Request Data (Visa Only).....	498
Subfield 1—Fleet Card ID Request Indicator.....	498
Subfield 2—Optional Free-form Informational Text.....	499
Subelement 94—Commercial Card Inquiry Request (Visa Only).....	499
Subelement 94—Commercial Card Inquiry Response (Visa Only).....	500
Subelement 95—Mastercard Promotion Code.....	501
Subelement 95—American Express Customer ID Number (American Express Only)....	502
Subelement 96—Visa Market-Specific Data Identifier (Visa Only).....	502
Subelement 97—Prestigious Properties Indicator (Visa Only).....	503
Subelement 98—Mastercard Corporate Fleet Card ID/Driver Number.....	504
Subelement 99—Mastercard Corporate Fleet Card Vehicle Number.....	505
DE 48—Authorization Platform Edits.....	506
DE 48, Proper Formatting.....	506
DE 48, TCC.....	506
DE 48, TCC and DE 3.....	507
DE 48, Subelement 14.....	508
DE 48, Subelement 26.....	508
DE 48, Subelement 35.....	509
DE 48, Subelement 37.....	510
DE 48, Subelement 38.....	510
DE 48, Subelement 42 and Subelement 43.....	512
DE 48, Subelement 43 (Static AAV).....	514
DE 48, Subelement 42 and DE 61.....	515
DE 48, Subelement 61.....	516
DE 48, Subelement 66.....	517
DE 48, Subelement 77.....	518
DE 48, Subelement 78.....	518
DE 48, Subelement 82.....	519
DE 48, Subelement 84.....	519
DE 48, Subelement 86.....	520
DE 48, Subelement 95.....	520
DE 48, in Authorization Request Response.....	520
DE 49—Currency Code, Transaction.....	521
DE 50—Currency Code, Settlement.....	522
DE 51—Currency Code, Cardholder Billing.....	523
DE 52—Personal ID Number (PIN) Data.....	524
DE 53—Security-Related Control Information.....	525

Subfield 1—PIN Security Type Code.....	526
Subfield 2—PIN Encryption Type Code.....	526
Subfield 3—PIN Block Format Code.....	527
Subfield 4—PIN Key Index Number.....	527
Subfield 5—Reserved for Future Use.....	528
Subfield 6—Reserved for Future Use.....	528
DE 54—Additional Amounts.....	528
Subfield 1—Account Type.....	531
Subfield 2—Amount Type.....	532
Subfield 3—Currency Code.....	532
Subfield 4—Amount.....	533
DE 54—Authorization Platform Edits.....	533
DE 55—Integrated Circuit Card (ICC) System-Related Data.....	534
DE 55—Subelement Encoding Scheme.....	535
DE 55—Subelements.....	536
DE 55—Authorization Platform Edits.....	540
Authorization Platform Edits—Cardholder Authentication Service.....	542
DE 56—Payment Account Data.....	545
Subelement 01—Payment Account Data.....	546
Subfield 01—Payment Account Reference (PAR).....	546
DE 57—DE 59—Reserved for National Use.....	546
DE 60—Advice Reason Code.....	547
Subfield 1—Advice Reason Code.....	548
DE 60, Subfield 1 Values, in Authorization Advice/0120.....	548
DE 60, Subfield 1 Values, in Reversal Advice/0420.....	550
DE 60, Subfield 1 Values, in Administrative Request/0600.....	550
DE 60, Subfield 1 Values, in Administrative Request Response/0610.....	550
DE 60, Subfield 1 Values, in Administrative Advice/0620.....	551
Subfield 2—Advice Detail Code.....	551
DE 60, Subfield 2 Values, in Authorization Advice/0120—Issuer-Generated.....	552
DE 60, Subfield 2 Values, in Authorization Advice/0120—System-Generated.....	552
DE 60, Subfield 2 Values, in Administrative Advice/0620.....	553
DE 60, Subfield 2 Values, in Customer Service Messages.....	553
DE 60, Subfield 2 Values, in Dynamic CVC 3 Validation.....	554
DE 60, Subfield 2 Values, in Mastercard In Control Service.....	554
DE 60, Subfield 2 Values, in M/Chip On-Behalf Services.....	555
DE 60, Subfield 2 Values, in Mastercard Digital Enablement Service.....	555
DE 60, Subfield 2 Values, in Mastercard Merchant Presented QR Service.....	556
DE 60, Subfield 2 Values, in Pay with Rewards.....	557
DE 60, Subfield 2 Values, in PIN Validation.....	557
DE 60, Subfield 2 Values, in Private Label Processing.....	557
DE 60, Subfield 2 Values, in TCC, CAT Level, and Promotion Code in Failed Parameter Combinations (Country-Specific).....	557

DE 60, Subfield 2 Values, in TCC, CAT Level, and Promotion Code in Failed Parameter Combinations (Global).....	558
DE 60, Subfield 2 Values, in MCC, CAT Level, and Promotion Code in Failed Parameter Combinations (Country-Specific).....	558
DE 60, Subfield 2 Values, in MCC and Promotion Code in Failed Parameter Combinations (Country-Specific).....	559
DE 60, Subfield 2 Values, in MCC and Promotion Code in Failed Parameter Combinations (Global).....	559
DE 60, Subfield 2 Values, in TCC and Promotion Code in Failed Parameter Combinations (Country-Specific).....	560
DE 60, Subfield 2 Values, in TCC and Promotion Code in Failed Parameter Combinations (Global).....	560
DE 60, Subfield 2 Values, in MCC and CAT Level in Failed Parameter Combinations (Country-Specific).....	561
DE 60, Subfield 2 Values, in MCC and CAT Level in Failed Parameter Combinations (Global).....	561
DE 60, Subfield 2 Values, in TCC and CAT Level in Failed Parameter Combinations (Country-Specific).....	562
DE 60, Subfield 2 Values, in TCC and CAT Level in Failed Parameter Combinations (Global).....	562
DE 60, Subfield 2 Values, in MCC in Failed Parameter Combinations (Country-Specific).....	563
DE 60, Subfield 2 Values, in MCC in Failed Parameter Combinations (Global).....	563
DE 60, Subfield 2 Values, in TCC in Failed Parameter Combinations (Country-Specific).....	564
DE 60, Subfield 2 Values, in TCC in Failed Parameter Combinations (Global).....	564
DE 60, Subfield 2 Values, in Miscellaneous Processing.....	565
Subfield 3—Advice Detail Text.....	565
DE 61—Point-of-Service (POS) Data.....	566
Subfield 1—POS Terminal Attendance.....	567
Subfield 2—Reserved for Future Use.....	567
Subfield 3—POS Terminal Location.....	568
Subfield 4—POS Cardholder Presence.....	568
Subfield 5—POS Card Presence.....	569
Subfield 6—POS Card Capture Capabilities.....	569
Subfield 7—POS Transaction Status.....	569
Subfield 8—POS Transaction Security.....	570
Subfield 9—Reserved for Future Use.....	570
Subfield 10—Cardholder-Activated Terminal Level.....	571
Subfield 11—POS Card Data Terminal Input Capability Indicator.....	571
Subfield 12—POS Authorization Life Cycle.....	573
Subfield 13—POS Country Code (or Sub-Merchant Information, if applicable).....	573
Subfield 14—POS Postal Code (or Sub-Merchant Information, if applicable).....	573

Authorization Platform Edits.....	574
DE 62—Intermediate Network Facility (INF) Data.....	577
DE 63—Network Data.....	578
Subfield 1—Financial Network Code.....	580
Subfield 2—Banknet Reference Number.....	590
DE 64—Message Authentication Code.....	590
DE 65—Bit Map, Extended.....	591
DE 66—Settlement Code.....	591
DE 67—Extended Payment Code.....	592
DE 68—Receiving Institution Country Code.....	592
DE 69—Settlement Institution Country Code.....	593
DE 70—Network Management Information Code.....	593
Network Management Request/0800—Sign-On/Sign-Off.....	594
Network Management Request/0800—Network Connection Status, Member-Generated.....	595
Network Management Request/0800—Network Connection Status, System-Generated.....	595
Network Management Request/0800—Host Session Activation/Deactivation.....	595
Network Management Request/0800—PEK Exchange.....	596
Network Management Request/0800—PEK Exchange-On Demand.....	596
Network Management Request Response/0810—PEK Exchange.....	596
Network Management Advice/0820—PEK Exchange.....	596
DE 71—Message Number.....	597
DE 72—Message Number Last.....	597
DE 73—Date, Action.....	597
DE 74—Credits, Number.....	598
DE 75—Credits, Reversal Number.....	598
DE 76—Debits, Number.....	599
DE 77—Debits, Reversal Number.....	599
DE 78—Transfers, Number.....	600
DE 79—Transfers, Reversal Number.....	600
DE 80—Inquiries, Number.....	600
DE 81—Authorizations, Number.....	601
DE 82—Credits, Processing Fee Amount.....	601
DE 83—Credits, Transaction Fee Amount.....	602
DE 84—Debits, Processing Fee Amount.....	602
DE 85—Debits, Transaction Fee Amount.....	603
DE 86—Credits, Amount.....	603
DE 87—Credits, Reversal Amount.....	603
DE 88—Debits, Amount.....	604
DE 89—Debits, Reversal Amount.....	604
DE 90—Original Data Elements.....	605
Subfield 1—Original Message Type Identifier.....	606

Subfield 2—Original DE 11 (Systems Trace Audit Number).....	606
Subfield 3—Original DE 7 (Transmission Date and Time).....	606
Subfield 4—Original DE 32 (Acquiring Institution ID Code).....	607
Subfield 5—Original DE 33 (Forwarding Institution ID Code).....	607
DE 91—Issuer File Update Code.....	608
DE 92—File Security Code.....	608
DE 93—Response Indicator.....	609
DE 94—Service Indicator.....	609
Subfield 1—Reserved for Future Use.....	610
Subfield 2—Acquirer/Issuer Indicator.....	610
Subfield 3—Address Data Indicator.....	610
DE 95—Replacement Amounts.....	611
Subfield 1—Actual Amount, Transaction.....	612
Subfield 2—Actual Amount, Settlement.....	613
Subfield 3—Actual Amount, Cardholder Billing.....	613
Subfield 4—Zero Fill.....	613
DE 96—Message Security Code.....	614
DE 97—Amount, Net Settlement.....	614
Subfield 1—Debit/Credit Indicator.....	615
Subfield 2—Amount.....	615
DE 98—Payee.....	615
DE 99—Settlement Institution ID Code.....	616
DE 100—Receiving Institution ID Code.....	616
DE 101—File Name.....	617
DE 102—Account ID 1.....	618
DE 103—Account ID 2.....	619
DE 104—Transaction Description.....	619
DE 105—DE 107—Reserved for Mastercard Use.....	620
DE 108—MoneySend Reference Data.....	620
DE 108—Authorization Platform Edits.....	622
Subelement 01—Receiver/Recipient Data.....	623
Subfield 01—Receiver/Recipient First Name.....	625
Subfield 02—Receiver/Recipient Middle Name.....	626
Subfield 03—Receiver/Recipient Last Name.....	626
Subfield 04—Receiver/Recipient Street Address.....	627
Subfield 05—Receiver/Recipient City.....	628
Subfield 06—Receiver/Recipient State/Province Code.....	628
Subfield 07—Receiver/Recipient Country.....	629
Subfield 08—Receiver/Recipient Postal Code.....	629
Subfield 09—Receiver/Recipient Phone Number.....	630
Subfield 10—Receiver/Recipient Date of Birth.....	630
Subfield 11—Receiver/Recipient Account Number.....	631
Subfield 12—Receiver/Recipient Identification Type.....	632

Subfield 13—Receiver/Recipient Identification Number.....	632
Subfield 14—Receiver/Recipient Identification Country Code.....	633
Subfield 15—Receiver/Recipient Identification Expiration Date.....	633
Subfield 16—Receiver/Recipient Nationality.....	634
Subfield 17—Receiver/Recipient Country of Birth.....	634
Subelement 02—Sender Data.....	635
Subfield 01—Sender First Name.....	636
Subfield 02—Sender Middle Name.....	637
Subfield 03—Sender Last Name.....	638
Subfield 04—Sender Street Address.....	639
Subfield 05—Sender City.....	639
Subfield 06—Sender State/Province Code.....	640
Subfield 07—Sender Country.....	640
Subfield 08—Postal Code.....	641
Subfield 09—Sender Phone Number.....	641
Subfield 10—Sender Date of Birth.....	642
Subfield 11—Sender Account Number.....	642
Subfield 12—Sender Identification Type.....	643
Subfield 13—Sender Identification Number.....	644
Subfield 14—Sender Identification Country Code.....	645
Subfield 15—Sender Identification Expiration Date.....	645
Subfield 16—Sender Nationality.....	646
Subfield 17—Sender Country of Birth.....	646
Subelement 03—MoneySend Transaction Data.....	647
Subfield 01—Unique Transaction Reference.....	647
Subfield 02—Additional Message.....	648
Subfield 03—Funding Source.....	649
Subfield 04—Participation ID.....	650
Subfield 05—Transaction Purpose.....	651
Subelement 04—MoneySend Language Description.....	652
Subfield 01—Language Identification.....	652
Subfield 02—Language Data.....	653
Subelement 05—Digital Account Information.....	653
Subfield 01—Digital Account Reference Number.....	654
Subfield 02—Mastercard Merchant Presented QR Receiving Account Number.....	655
Subelement 06—QR Dynamic Code Data.....	656
DE 109—Reserved for ISO Use.....	657
DE 110—Additional Data—2.....	658
Subelement 9—ANSI X9 TR-31 Key Block Key (128-bit Key Block Protection Key).....	659
Subelement 9—ANSI X9 TR-31 Key Block Key (192-bit Key Block Protection Key).....	659
Subelement 10—Key Check Value.....	660
DE 111—Reserved for ISO Use.....	660
DE 112—Additional Data (National Use).....	661

---

DE 112—Encoding Scheme.....	662
DE 112—Authorization Platform Edits.....	663
All Regions—Installment Payment Transactions.....	664
Subelement 21—Installment Payment Data 1.....	664
Subelement 22—Installment Payment Data 2.....	665
Subelement 23—Installment Payment Data 3.....	668
Alternate Processing.....	669
Brazil—Payment Transactions.....	669
Subelement 012—Brazil Commercial and Financing Data.....	669
Subelement 013—Crediário First Simulation.....	672
Subelement 014—Crediário Second Simulation.....	675
Subelement 015—Crediário Third Simulation.....	678
Subelement 018—Brazil Post-Dated Transaction Data.....	680
Subelement 019—Original Purchase Amount.....	683
Brazil—Merchant Fraud Scoring Data.....	684
Subelement 028—Merchant Fraud Score Data.....	684
Chile—Payment Transactions.....	685
Subelement 010—Installment Payment Data.....	685
Colombia—Domestic Transactions.....	686
Subelement 035—Issuer Fee Inquiry Indicator.....	686
Subelement 036—Issuer Fee Amount.....	686
Colombia—Payment Transactions.....	687
Subelement 010—Installment Payment Data.....	687
Subelement 011—Customer ID.....	688
Cuotas—Payment Transactions.....	688
Subelement 001—Installment Payment Data.....	688
Subelement 003—Installment Payment Response Data.....	690
Subelement 027—ATM Credit Card Cash Advance Installments.....	690
Europe Region and Philippines—Payment Transactions.....	694
Subelement 009—Installment Payment Data.....	694
Subelement 020—Domestic Card Acceptor Tax ID.....	696
Greece—Payment Transactions.....	697
Subelement 006—Installment Payment Data.....	697
Subelement 008—Installment Payment Response Data.....	698
Japan—Payment Transactions.....	699
Subelement 030—Japan Domestic POS Data.....	699
Subelement 031—Japan Domestic Response Code.....	701
Subelement 032—Japan Payment Options.....	702
Mexcta—Payment Transactions.....	707
Subelement 004—Credit Line Usage Fee (CLUF).....	707
Subelement 005—Issuing Bank Name (AKA Doing Business As [DBA]).....	707
Subelement 006—Financial Institution ID (FIID).....	708
Subelement 007—Installment Payment Data.....	708

---

Subelement 008—Installment Payment Response Data.....	709
Netherlands—IBAN—Account Inquiry.....	710
Subelement 037—Additional Cardholder Information.....	710
Parcelas—Payment Transactions.....	712
Subelement 001—Installment Payment Data.....	713
Subelement 002—Installment Payment Response Data.....	713
Subelement 016—Additional Installment Payment Response Data.....	714
Percita—Payment Transactions.....	715
Subelement 007—Installment Payment Data.....	715
Subelement 008—Installment Payment Response Data.....	716
Spain—Domestic ATM Transactions.....	717
Subelement 017—ATM Domestic Fee.....	717
United Kingdom—Debt Repayment Transactions.....	719
Subelement 033—UK Recipient Details.....	719
DE 113—Reserved for National Use.....	721
Generic Data, Administrative Request/0600 Message.....	722
Banking Data, Administrative Request/0600 Message.....	723
DE 114—Reserved for National Use.....	724
Consumer Application Request Data Administrative Request/0600 Message.....	725
Consumer Status Inquiry or Preapproved Offer Inquiry Data Administrative Request/0600 Message.....	727
Consumer Account Maintenance Data Administrative Request/0600 Message.....	728
Consumer Application Response Data Administrative Request Response/0610 Message.....	731
Consumer Account Maintenance Data Administrative Request Response/0610 Message.....	732
DE 115—Reserved for National Use.....	736
Business Application Request Data Administrative Request/0600 Message.....	736
Business Application Status Inquiry Data or Business Preapproved Offer Inquiry Data Administrative Request/0600 Message.....	738
Business Account Maintenance Data Administrative Request/0600 Message.....	739
Business Application Response Data Administrative Request Response/0610 Message.....	742
Business Account Maintenance Data Administrative Request Response/0610 Message.....	743
DE 116—Reserved For National Use.....	747
Consumer User Lookup Inquiry Data Administrative Request/0600.....	748
Consumer Account Lookup Inquiry Data Administrative Request/0600 Message.....	749
Consumer Account Lookup Response Data Administrative Request Response/0610 Message.....	750
DE 117—Reserved for National Use.....	751
Business User Lookup Inquiry Data Administrative Request/0600 Message.....	752
Business Account Lookup Inquiry Data Administrative Request/0600 Message.....	753

Business Account Lookup Response Data Administrative Request Response/0610 Message.....	754
DE 118—Reserved for National Use.....	755
Authorized User Data Administrative Request/0600 Message.....	756
Trade Reference Data Administrative Request/0600 Message.....	757
Authorized User Response Data Administrative Request/0610 Message.....	758
DE 119—Reserved for National Use.....	759
Using DE 113–119 in Administrative 06xx Messages.....	760
DE 120—Record Data.....	763
Subfield 01—AVS Service Indicator 1.....	765
Subfield 02—AVS Service Indicator 2.....	765
Subfield 03—AVS Service Indicator 3.....	766
Subfield 04—AVS Service Indicator 4.....	766
Online File Maintenance.....	767
MCC102—Stand-In Account File.....	768
MCC103—Electronic Warning Bulletin File.....	769
MCC104—Local Stoplist File.....	771
MCC105—Payment Cancellation File.....	775
MCC106—PAN Mapping File.....	778
MCC107—Enhanced Value File.....	783
MCC108—Product Graduation File.....	785
MCC109—Application Transaction Counter File.....	787
MCC111—PAN-PAR (Payment Account Reference) Mapping File.....	789
DE 120 Error Codes.....	790
DE 121—Authorizing Agent ID Code.....	806
DE 122—Additional Record Data.....	808
DE 123—Receipt Free Text.....	809
DE 124—Member-Defined Data.....	810
DE 124—Member-Defined Data (General Use).....	810
DE 124—Member-Defined Data (MoneySend Only).....	812
DE 124—Member-Defined Data (Brazil Maestro Only).....	812
Subfield 1—Unique Reference Number.....	812
Subfield 2—Sender/Payer/User ID.....	813
Subfield 3—Sender/Payer Address.....	813
Subfield 4—Additional Sender Information.....	814
Subfield 6—Discretionary Message on Sales Slip Supported.....	815
Subfield 7—Discretionary Message on Sales Slip Code.....	815
Subfield 8—Discretionary Message on Sales Slip Content.....	816
Subfield 9—Phoneshop (Phone Company ID).....	816
Subfield 10—Phoneshop (Cell Phone Number).....	816
Subfield 11—Phoneshop (Message Security Code).....	817
Subfield 12—Merchant CNPJ Number.....	817
Subfield 13—Total Annual Effective Cost.....	817

---

DE 124—Member-Defined Data (Colombia Domestic Use Only).....	818
Subfield 1—Card Issuer Data.....	818
Subfield 2—Tax (IVA).....	818
Subfield 3—Tax Amount Base.....	819
Subfield 4—Retailer Data.....	819
Subfield 5—Terminal Acquirer Data.....	820
Subfield 6—Acquirer Original Processing Code.....	820
Subfield 7—Bill Payment/Top up Data.....	820
Subfield 8—Local POS Data.....	821
Subfield 9—Local Response Codes.....	821
Subfield 10—Original Transaction Data.....	822
Subfield 11—IAC Tax Amount.....	822
DE 125—New PIN Data.....	823
DE 126—Private Data.....	823
DE 127—Private Data.....	824
DE 128—Message Authentication Code.....	825

## **Chapter 5: Program and Service Format Requirements..... 827**

Product Value Constraints.....	837
Permitted Transactions by Card Program.....	837
Value Constraints by Transaction Type.....	841
Account Status Inquiry Service.....	845
Purchase Account Status Inquiry / Recurring Payment Account Status Inquiry.....	845
Payment Account Status Inquiry.....	847
Authorization Platform Edits.....	850
Address Verification Service.....	851
Authorization Request/0100—AVS and Authorization Request.....	852
Authorization Request Response/0110—AVS and Authorization Request.....	853
Network Management Request/0800—AVS Sign-on.....	854
Alternate Processing.....	854
DE 48 and DE 120 Structure in AVS Transactions.....	855
Authorization Platform Edits.....	856
Automated Fuel Dispenser Completion.....	857
AFD Message Scenarios.....	858
Authorization Request/0100—Automated Fuel Dispenser Pre-authorization.....	858
Authorization Advice/0120—Acquirer-Generated (Automated Fuel Dispenser Completion).....	859
Authorization Advice/0120—Acquirer-Generated (Automated Fuel Dispenser Completion).....	860
Authorization Advice Response/0130—Issuer-Generated (Responding to an Acquirer-Generated).....	861
Alternate Processing.....	861

---

Clearing AFD Transactions.....	862
Account Level Management.....	862
Alternate Processing.....	862
ATM Bill Payment Service.....	864
Authorization Request/0100—ATM Bill Payment, Europe Acquired.....	864
Authorization Request/0100—ATM Bill Payment, Non-Europe Acquired.....	865
Authorization Platform Edits.....	865
ATM Credit Card Cash Advance in Installments.....	866
Authorization Request/0100—ATM Installment Inquiry.....	866
Authorization Request Response/0110—ATM Installment Inquiry.....	867
Authorization Request/0100—ATM Installment Withdrawal.....	868
Authorization Request Response/0110—ATM Installment Withdrawal.....	868
Authorization and Preauthorization Processing Standards.....	869
Balance Inquiry—ATM.....	876
Authorization Request/0100—ATM Balance Inquiry.....	876
Authorization Request/0100—ATM Balance Inquiry Edits.....	877
Authorization Request Response/0110—ATM Balance Inquiry.....	878
Authorization Request Response/0110—ATM Balance Inquiry Edits.....	878
Authorization Advice/0120—Acquirer-Generated—ATM Balance Inquiry Edits.....	879
Alternate Processing.....	879
Balance Inquiry—Point-of-Sale.....	880
Authorization Request/0100—POS Balance Inquiry.....	880
Authorization Request Response/0110—POS Balance Inquiry.....	881
Authorization Request/0100—POS Balance Inquiry Edits.....	882
Authorization Request/0110—POS Balance Inquiry Edits.....	884
Authorization Advice/0120—Acquirer-Generated—POS Balance Inquiry Edits.....	885
Alternate Processing.....	885
Balance Inquiry—Short Message Service.....	885
Authorization Request/0100—Short Message Service Balance Inquiry.....	885
Balance Inquiry—Mobile Remote Payments Program.....	886
Authorization Request/0100—Mobile Remote Payments Program Balance Inquiry.....	886
Chip-Specific Value Constraints.....	887
Chip Partial Grade Value Constraints.....	887
Chip Full Grade Value Constraints.....	888
Contact and Contactless Chip Specific Value Constraints.....	889
Canada Region Debit Mastercard Merchant Acceptance.....	890
Acquirers.....	890
Issuers.....	891
Authorization Platform Edits.....	891
Cardholder Authentication Service.....	893
Authorization Platform Edits—Cardholder Authentication Service.....	894
Card Validation Code 2.....	897
Authorization Request/0100—CVC 2 Verified.....	897

---

Authorization Request/0100—CVC 2 Unverified.....	898
Authorization Request/0100—CVC 2 Processed by Stand-In.....	899
Authorization Request/0100—CVC 2 Processed by X-Code.....	900
CVC 2 DE 48 Structure.....	901
Authorization Request/0100—CVC 2 .....	901
Authorization Request Response/0110—CVC 2.....	902
Authorization Platform Edits.....	902
Card Validation Code 3.....	903
Authorization Request Response/0110—CVC 3 Result.....	903
Contactless CVC 3 Processing Service.....	904
Authorization Request/0100—CVC 3.....	904
Dynamic CVC 3 Application Transaction Counter (ATC) Processing.....	905
Dynamic CVC 3 Application Transaction Counter (ATC) Information.....	906
MCC109 (Application Transaction Counter File).....	907
Authorization Platform Edits.....	907
Card Validation Code Result.....	908
Optional Non-valid CVC 3 Processing.....	908
ATC Data Extract File.....	909
Alternate Processing.....	910
Contactless Mapping Service for Contactless M/Chip and Contact M/Chip Transactions.	910
Contactless Mapping Service Processing of Contactless M/Chip and Contact M/Chip Transactions.....	911
Authorization Platform Edits.....	912
Cross-Border Fee Manager Service.....	913
Currency Conversion.....	913
Amount-Related Data Elements in Authorization and Reversal Messages.....	914
Dual Message System Processing.....	916
Acquirer Send MTIs in Authorization and Reversal Messages.....	917
Acquirer Receive MTIs in Authorization and Reversal Messages.....	918
Issuer Receive MTIs in Authorization and Reversal Messages.....	918
Issuer Send MTIs in Authorization and Reversal Messages.....	919
Alternate Processing.....	920
Authorization Platform Edits.....	921
Electronic Commerce Processing.....	924
Best Practices for E-Commerce Transactions.....	924
No Security Protocol.....	927
Channel Encryption.....	928
Authorization Request/0100—Electronic Commerce Purchase.....	929
Authorization Request Response/0110—Electronic Commerce Purchase.....	931
Authorization Platform Edits.....	932
Mastercard SecureCode.....	933
Static AAV.....	935
Forgotten Card at ATM.....	936

---

Reversal Request/0400—Forgotten Card.....	936
Gaming Payment Transactions.....	936
Gaming Payment Transaction Processing in the Europe and Middle East/Africa Regions.....	937
Authorization Request/0100—Gaming Payment.....	938
Reversal Request/0400—Gaming Payment.....	938
Authorization Platform Edits.....	939
Gaming Payment Transaction Processing in the United States Region.....	940
ICCR Service.....	940
ICCR Service Overview.....	940
ICCR Enrollment.....	941
Incremental Preauthorization Standards.....	941
Authorization Platform Edits.....	947
Maestro Pre-authorized Transactions.....	950
Authorization Request/0100—Maestro Pre-Authorization.....	950
Authorization Advice/0120—Maestro Pre-Authorization Completion.....	951
Maestro Recurring Payments Program.....	951
Authorization Request/0100—Maestro Recurring Payment.....	952
Authorization Platform Edits.....	953
Magnetic Stripe Compliance.....	954
Authorization Request/0100—Magnetic Stripe-read.....	956
Authorization Request Response/0110—Magnetic Stripe-read.....	956
Mastercard Commercial Payments Account.....	957
Authorization Platform Edit to Support MAP in Brazil.....	957
Authorization Platform Edits to Support MAP in Mastercard European Economic Area Subregion.....	957
Mastercard Digital Enablement Service.....	959
Message Layouts—Pre-digitization Payment Network Messages.....	959
Authorization Request/0100—Tokenization Eligibility.....	960
DE 124 Subfields in Authorization Request/0100—Tokenization Eligibility.....	962
Authorization Request Response/0110—Tokenization Eligibility.....	966
DE 124 Subfields for Authorization Request Response/0110—Tokenization Eligibility.....	967
Authorization Request/0100—Tokenization Authorization.....	970
DE 124 Subfields in Authorization Request/0100—Tokenization Authorization.....	974
Authorization Request Response/0110—Tokenization Authorization.....	978
DE 124 Subfields in Authorization Request Response/0110—Tokenization Authorization.....	979
Authorization Request/0100—Activation Code Notification.....	983
DE 124 Subfields in Authorization Request/0100—Activation Code Notification....	986
Authorization Request Response/0110—Activation Code Notification.....	988
Authorization Request/0100—Tokenization Complete Notification.....	988

DE 124 Subfields in Authorization Request/0100—Tokenization Complete Notification.....	991
Authorization Request Response/0110—Tokenization Complete Notification.....	993
Authorization Request/0100—Tokenization Event Notification.....	993
DE 124 Subfields in Authorization Request/0100—Tokenization Event Notification.....	995
Authorization Request Response/0110—Tokenization Event Notification.....	998
Issuer File Update Request/0302—Maintenance (Token/PAN Update).....	998
DE 120 Layout for MCC106 Mastercard Digital Enablement Service (Token Update).....	998
DE 120 Layout for MCC106 Mastercard Digital Enablement Service (PAN Update—Deactivate/Suspend/Resume Token).....	1000
Issuer File Update Request Response/0312—Issuer Token Maintenance Response (Token/PAN Update).....	1001
Administrative Advice/0620—Issuer Token Notification Advice.....	1002
DE 120 Layout for Administrative Advice/0620—Issuer Token Notification Advice for Activation Code Notification.....	1003
DE 120 Layout for Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Complete Notification.....	1006
DE 120 Layout for Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Event Notification.....	1009
Administrative Advice Response/0630—Issuer Token Notification Advice Response.....	1012
MDES for Merchants.....	1012
Mastercard Fraud Scoring Services.....	1014
Expert Monitoring for Issuers.....	1015
For More Information.....	1015
Fraud Rule Manager.....	1015
To Participate.....	1016
For More Information.....	1016
Decision Intelligence.....	1016
Overview.....	1016
How it Works.....	1016
Issuers' Potential Benefit from Decision Intelligence.....	1017
Message Specification Requirements.....	1017
To Participate.....	1018
For More Information.....	1018
Expert Monitoring for Merchants.....	1018
Benefits.....	1018
To Participate.....	1019
For More Information.....	1019
Authorization Request/0100—Fraud Scoring.....	1019
Alternate Processing.....	1020

Mastercard Hosted Mobile Phone Top-Up ATM Transactions.....	1020
Authorization Request/0100—Mastercard Hosted Mobile Phone Top-Up.....	1020
Authorization Platform Edits.....	1021
Mastercard In Control Service.....	1023
Authorization Request/0100—In Control Purchase Control.....	1023
Dual Message System Processing.....	1024
Mastercard In Control Virtual Card Service.....	1025
Mastercard In Control Real Card Spend Control.....	1025
Process of a Mastercard In Control Service Eligible Transaction.....	1025
Authorization Request/0100—In Control Real Card Spend Control.....	1027
Authorization Advice/0120—In Control Real Card Spend Control.....	1028
Mastercard In Control Virtual Card Mapping and Spend Control Service.....	1028
Authorization Request/0100—In Control Virtual Card Mapping and Spend Control Service.....	1029
Exception Processing.....	1029
Mastercard Installment Payment Service.....	1030
Mastercard Merchant Presented QR.....	1030
Authorization Platform Edits.....	1031
Alternate Processing.....	1042
Mastercard MoneySend.....	1043
Authorization Request/0100—Mastercard MoneySend Funding Transactions.....	1043
Reversal Request/0400—MoneySend Funding Transaction.....	1044
Authorization Platform Edits.....	1045
Authorization Request/0100—MoneySend Payment Transactions.....	1046
Reversal Request/0400—MoneySend Payment Transaction.....	1048
Authorization Platform Edits.....	1050
Mastercard MoneySend Issuer Transaction Controls.....	1062
Network Blocking.....	1062
Sanction Screening.....	1063
For More Information About Implementing the MoneySend Program.....	1063
Mastercard Safety Net.....	1063
Masterpass Transactions.....	1064
Authorization Request/0100—Masterpass Online Wallet.....	1065
Authorization Advice/0120—Acquirer-Generated.....	1066
Authorization Advice/0120—System-Generated.....	1066
Authorization Platform Edits.....	1066
Merchant Advice Codes.....	1067
Merchant Advice Codes Used with Response Codes.....	1067
M/Chip Processing Services.....	1069
Program use of M/Chip Processing Service Data Elements.....	1069
Chip To Magnetic Stripe Conversion.....	1071
Authorization and Stand-In Processing.....	1072
M/Chip Cryptogram Pre-validation.....	1075

---

Validation of the Application Cryptogram.....	1076
Generation of the Issuer Chip Authentication Data.....	1078
DE 60 (Advice Reason Code).....	1078
Alternate Processing.....	1080
Authorization Platform Edits.....	1080
Combined Service Option.....	1080
M/Chip Cryptogram Validation in Stand-In Processing.....	1080
Validation of the Application Cryptogram.....	1081
Generation of the Issuer Chip Authentication Data.....	1083
DE 60—Advice Reason Code.....	1083
Alternate Processing.....	1084
Authorization Platform Edits.....	1084
MIP Transaction Blocking.....	1085
MIP Transaction Block Setup.....	1086
Authorization Platform Edits.....	1086
Full BIN Block.....	1087
Authorization Platform Edits.....	1088
Mobile Remote Payments.....	1088
Authorization Platform Edits.....	1089
Partial Approvals.....	1090
Authorization Request/0100—Partial Approval.....	1090
Authorization Request Response/0110—Partial Approval.....	1090
Reversal Request/0400—Partial Approval.....	1092
Reversal Advice/0420—Partial Approval.....	1092
Authorization Advice/0120—Acquirer-Generated.....	1093
Alternate Processing.....	1093
Authorization Platform Edits.....	1093
Payment Transactions.....	1096
Authorization Request/0100—Payment Transaction Message.....	1096
Authorization Request Response/0110—Payment Transaction.....	1097
Authorization Platform Edits.....	1098
PIN Management Service.....	1100
Chip PIN Management Service.....	1100
Authorization Request/0100—PIN Change or PIN Unblock (Chip Card).....	1100
Authorization Request Response/0110—PIN Change or PIN Unblock (Chip Card).....	1101
Reversal Request/0400—PIN Change (Chip Card).....	1102
Magnetic Stripe PIN Management Service.....	1103
Authorization Request/0100—PIN Change (Magnetic Stripe Card).....	1103
Authorization Request Response/0110—PIN Change (Magnetic Stripe Card).....	1105
Reversal Request/0400—PIN Change (Magnetic Stripe Card).....	1105
Authorization Request/0100 Edits (Magnetic Stripe Card).....	1106
Authorization Advice/0120—Acquirer-Generated Edits (Magnetic Stripe Card)....	1108
Reversal Request/0400 Edits (Magnetic Stripe Card).....	1108

---

Issuer Response Options to a Magnetic Stripe PIN Change Request.....	1109
PIN Processing for Europe Region Customers.....	1110
PIN Translation Edits.....	1111
PIN Validation.....	1112
PIN Validation Edits.....	1113
PIN Key Management.....	1115
PIN Verification Value/PIN Offset on File Service.....	1116
Processing Transactions Using PVV/PIN Offset.....	1116
Processing Parameters.....	1116
PVV/PIN Offset File Format.....	1117
Alternate Processing.....	1118
PIN Processing for Non-Europe Customers.....	1119
Acquirer Requirements.....	1119
Support either Static or Dynamic PIN Encryption Key (PEK) Exchanges.....	1119
Mastercard Magnetic Stripe Compliance Program Compliance.....	1120
Authorization Request/0100—PIN Transactions.....	1120
Authorization Request Response/0110—PIN Transactions.....	1121
Issuer Requirements.....	1123
Receive Purchase Transactions that Contain a PIN.....	1123
Support Static or Dynamic PEK Exchanges.....	1123
Authorization Request/0100—PIN Messages.....	1124
Authorization Advice/0120—PIN Messages.....	1125
Reversal Advice/0420—PIN Messages.....	1126
Alternate Processing.....	1126
Support for Both Acquiring and Issuing Processing.....	1127
Cleartext Use Prohibited.....	1127
Emergency Static PEK or Emergency KEK Process.....	1127
Previous PEKs.....	1128
PIN Verification Value on File Service.....	1128
PIN Translation and Verification Process.....	1130
Detection of PEK Corruption Using Sanity Checks.....	1134
Authorization Platform Sanity Check Error.....	1134
Issuer Sanity Check Error.....	1136
Private Label Processing.....	1137
Authorization Request/0100—Private Label Processing.....	1137
Card Activation for Private Label Processing.....	1138
Authorization Request/0100 and Reversal Request/0400—Card Activation at Point of Sale.....	1138
Alternate Processing.....	1140
Authorization Platform Edits.....	1140
Card Activation Plus Initial Load for Private Label Processing.....	1142
Product Inquiry Service.....	1143
Authorization Request/0100—Product Inquiry Service.....	1144

---

Proximity Payments.....	1145
Authorization Request/0100—Proximity Payments.....	1145
Purchase of Goods or Services with Cash Back.....	1146
Authorization Request/0100—Purchase of Goods or Services with Cash Back.....	1146
Issuer Response Options.....	1147
Reversal Request/0400.....	1148
Reversal Advice/0420.....	1149
Authorization Advice/0120.....	1149
Authorization Advice/0120—Acquirer-Generated.....	1149
Alternate Processing.....	1149
Authorization Platform Edits.....	1150
Real-Time Substantiation.....	1153
Participation in Real-Time Substantiation.....	1154
Merchant Terminal Verification.....	1154
Real-Time Substantiation Amounts.....	1155
Transaction Processing Examples.....	1156
Authorization Platform Edits.....	1161
Reversal Processing.....	1163
Best Practices for Authorization Reversal Processing.....	1163
Full Reversals.....	1167
Partial Reversals.....	1167
Reversals of Balance Inquiry Transactions.....	1167
Reversals of Purchase of Goods or Services with Cash Back Transactions.....	1167
Alternate Processing.....	1168
Authorization Platform Edits.....	1169
Visa Transaction Processing.....	1171
Visa Custom Payment Service.....	1171
Authorization Request/0100—Visa Custom Payment Service.....	1171
Authorization Request Response/0110—Visa Custom Payment Service.....	1173
DE 48 Structure in a Visa Custom Payment Service Transaction.....	1174
Visa Programs.....	1175
Visa CVV2.....	1175
Visa Fleet Card ID.....	1176
Visa Commercial Card Inquiry.....	1177
Visa Token Processing.....	1178
Authorization Request/0100—Visa Token Request.....	1179
Authorization Request Response/0110—Visa Token Request Response.....	1180
<b>Notices.....</b>	<b>1182</b>

---

# 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.*

---

Customer Interface Specification Format.....	45
Issuer Post-on-Authorization.....	46
Bit Mapped Message Encoding Scheme.....	47
Authorization Platform Processing Terms and Acronyms.....	47
Customer Interface Specification Notations.....	48
Data Length Notations.....	48
Data Representation Notations.....	49
Data Field Notations.....	50
Data Justification Notations.....	50
Date and Time Notations.....	50
Entity Notations.....	51
Presence Notations.....	52
Presence Requirement Notations.....	52
Program and Service Category Notations.....	53
Authorization Platform Messages.....	54
List of Authorization Messages.....	54
Message Type Identifier Presence Requirements by Program and Service.....	56
Character Sets.....	57
Character Sets.....	58
Extended Character Sets.....	66
Swedish Domestic Authorization Switching Character Set.....	71

## **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 processing 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 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 customer processing system (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
- Data Field
- Data Justification
- Date and Time
- Entities
- Presence
- Presence Requirements
- Program and Service Category

### Data Length Notations

Data length notations indicate the format of the data length.

Notation	Description
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.  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 represents the number of positions in the variable-length data field that follows. The length field contains a value in the range 01–99.

---

<b>Notation</b>	<b>Description</b>
VAR	The variable-length data field  Example: "an...25; LLVAR" represents a variable-length alphanumeric data element with a length of 1–25 positions.
LLVAR	Present with a variable-length data element attribute, indicates that the data element contains two fields:  LLL      The length field 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; LLVAR" 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.

**NOTE: Special characters are any non-numeric or non-alphabetic characters (for example, @, #, &, and \$), including spaces.**

---

<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 (or blank)
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)

---

---

<b>Notation</b>	<b>Description</b>
s	special character  Special characters are any non-numeric or non-alphabetic characters (for example, @, #, &, and \$), including spaces. For a complete list of valid character sets, refer to the Character Sets section.
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 <b>bytes</b> .	

---

## Data Field Notations

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

---

<b>Notation</b>	<b>Description</b>
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.

---

<b>Notation</b>	<b>Description</b>
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.

<b>Notation</b>	<b>Description</b>
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

<b>Notation</b>	<b>Description</b>
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).

<b>Notation</b>	<b>Description</b>
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.
•	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 or Dst column.
P	Sys passes data between Org and Dst.

## 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).

<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Description</b>
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.
•	X	M	Authorization Platform always provides the data element.

---

<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Description</b>
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.

## Authorization Platform Messages

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

The Authorization Platform supports the following online transaction message types:

- Authorization/01xx messages
- Issuer File Update/03xx messages
- Reversal/04xx messages
- Administrative/06xx messages
- Network Management/08xx messages

## List of Authorization Messages

The following table lists the message types the Authorization Platform supports and indicates the originating entities for each message type. 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>				
0302	Issuer File Update Request	✓		

<b>MTI</b>	<b>Description</b>	<b>Acquirer</b>	<b>Issuer</b>	<b>Authorization Platform</b>
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—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			√
0810	Network Management Request Response—Network Connection Status, Member-generated	√	√	
0810	Network Management Request Response—Network Connection Status, System-generated			√
0810	Network Management Request—Host Session Activation/Deactivation	√	√	√

<sup>1</sup> Because the Mastercard 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.)

<b>MTI</b>	<b>Description</b>	<b>Acquirer</b>	<b>Issuer</b>	<b>Authorization Platform</b>
0810	Network Management Request Response/—PEK Exchange	✓	✓	
0810	Network Management Request Response/—PEK Exchange—On Demand			✓
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.

<b>MTI</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</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 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	✓	✓	•	•	•	•

MTI	Description	MC	NP	VI	TE	MS	CI
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. Customers 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).

**NOTE: 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.

Customers 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)

Customers that want to receive messages in standard EBCDIC or extended or standard ASCII must inform Mastercard.

## Character Sets

These tables contains valid ASCII to EBCDIC character sets.

### ASCII to EBCDIC Character Set—ASCII hex order

**Note:** For the purposes of ISO 8583, the < space > character is treated as a special character (attribute "s"). It may, however, also be used in fields designated as alphanumeric (attribute "an") but only in the form of trailing spaces used to pad out significant data to fill a fixed-length field.

Decimal Value	ASCII Hex	EBCDIC Hex	ASCII Symbol	Meaning	EBCDIC Symbol	Meaning
032	20	40	< space >	Space	DS	digit select
033	21	4F	!	exclamation mark	SOS	start of significance
034	22	7F	"	straight double quotation mark	FS	field separator
035	23	7B	#	number sign	WUS	word underscore
036	24	5B	\$	dollar sign	BYP/INP	bypass/inhibit presentation
037	25	6C	%	percent sign	LF	line feed
038	26	50	&	ampersand	ETB	end of transmission block
039	27	7D	'	apostrophe	ESC	escape

<b>Decimal Value</b>	<b>ASCII Hex</b>	<b>EBCDIC Hex</b>	<b>ASCII Symbol</b>	<b>Meaning</b>	<b>EBCDIC Symbol</b>	<b>Meaning</b>
040	28	4D	(	left parenthesis	SA	set attribute
041	29	5D	)	right parenthesis	SFE	
042	2A	5C	*	asterisk	SM/SW	set mode switch
043	2B	4E	+	addition sign	CSP	control sequence prefix
044	2C	6B	,	comma	MFA	modify field attribute
045	2D	60	-	subtraction sign	ENQ	enquiry
046	2E	4B	.	period	ACK	acknowledge
047	2F	61	/	right slash	BEL	bell
048	30	F0	0			
049	31	F1	1			
050	32	F2	2		SYN	synchronous idle
051	33	F3	3		IR	index return
052	34	F4	4		PP	presentation position
053	35	F5	5		TRN	
054	36	F6	6		NBS	numeric backspace
055	37	F7	7		EOT	end of transmission
056	38	F8	8		SBS	subscript
057	39	F9	9		IT	indent tab
058	3A	7A	:	colon	RFF	required form feed
059	3B	5E	;	semicolon	CU3	customer use 3

Decimal Value	ASCII Hex	EBCDIC Hex	ASCII Symbol	Meaning	EBCDIC Symbol	Meaning
060	3C	4C	<	less than	DC4	device control 4
061	3D	7E	=	equal	NAK	negative acknowledge
062	3E	6E	>	greater than		
063	3F	6F	?	question mark	SUB	substitute
064	40	7C	@	at symbol	SP	space
065	41	C1	A		RSP	
066	42	C2	B		â	
067	43	C3	C		ä	
068	44	C4	D		à	
069	45	C5	E		á	
070	46	C6	F		ã	
071	47	C7	G		å	
072	48	C8	H		ç	
073	49	C9	I		ñ	
074	4A	D1	J		¢	cent
075	4B	D2	K		.	period
076	4C	D3	L		<	less than
077	4D	D4	M		(	left parenthesis
078	4E	D5	N		+	addition sign
079	4F	D6	O			logical or
080	50	D7	P		&	ampersand
081	51	D8	Q		é	
082	52	D9	R		ê	
083	53	E2	S		ë	
084	54	E3	T		è	
085	55	E4	U		í	

Decimal Value	ASCII Hex	EBCDIC Hex	ASCII Symbol	Meaning	EBCDIC Symbol	Meaning
086	56	E5	V		↑	
087	57	E6	W		ī	
088	58	E7	X		ì	
089	59	E8	Y		ß	
090	5A	E9	Z		!	exclamation point
091	5B	4A	[	left bracket	\$	dollar sign
092	5C	E0	\	left slash	*	asterisk
093	5D	5A	]	right bracket	)	right parenthesis
094	5E	5F	^	hat, circumflex	;	semicolon
095	5F	6D	_	underscore	¬	logical not
096	60	79	`	grave	-	subtraction sign
097	61	81	a		/	right slash
098	62	82	b		Â	
099	63	83	c		Ä	
100	64	84	d		À	
101	65	85	e		Á	
102	66	86	f		Ã	
103	67	87	g		Å	
104	68	88	h		Ç	
105	69	89	i		Ñ	
106	6A	91	j		¡	split vertical bar
107	6B	92	k	,	,	comma
108	6C	93	l		%	percen sign
109	6D	94	m		_	underscore
110	6E	95	n		>	greater than

Decimal Value	ASCII Hex	EBCDIC Hex	ASCII Symbol	Meaning	EBCDIC Symbol	Meaning
111	6F	96	o		?	question mark
112	70	97	p		Ø	
113	71	98	q		É	
114	72	99	r		Ê	
115	73	A2	s		Ë	
116	74	A3	t		È	
117	75	A4	u		Í	
118	76	A5	v		Î	
119	77	A6	w		Ї	
120	78	A7	x		Ӯ	
121	79	A8	y		߱	grave
122	7A	A9	z		:	colon
123	7B	C0	{	left brace	#	number sign
124	7C	6A		logical or	@	at symbol
125	7D	D0	]	right brace	'	apostrophe
126	7E	A1	~	similar, tilde	=	equal

**ASCII to EBCDIC Character Set—EBCDIC hex order**

**Note:** For the purposes of ISO 8583, the < space > character is treated as a special character (attribute "s"). It may, however, also be used in fields designated as alphanumeric (attribute "an") but only in the form of trailing spaces used to pad out significant data to fill a fixed-length field.

Decimal Value	EBCDIC Hex	ASCII Hex	EBCDIC Symbol	Meaning	ASCII Symbol	Meaning
032	40	20	DS	digit select	< space >	Space
091	4A	5B	\$	dollar sign	[	left bracket
046	4B	2E	ACK	acknowledge	.	period
060	4C	3C	DC4	device control	<	less than

Decimal Value	EBCDIC Hex	ASCII Hex	EBCDIC Symbol	Meaning	ASCII Symbol	Meaning
040	4D	28	SA	set attribute	(	left parenthesis
043	4E	2B	CSP	control sequence prefix	+	addition sign
033	4F	21	SOS	start of significance	!	exclamation mark
038	50	26	ETB	end of transmission block	&	ampersand
093	5A	5D	)	right parenthesis	]	right bracket
036	5B	24	BYP/INP	bypass/inhibit presentation	\$	dollar sign
042	5C	2A	SM/SW	set mode switch	*	asterisk
041	5D	29	SFE		)	right parenthesis
059	5E	3B	CU3	customer use 3	;	semicolon
094	5F	5E	;	semicolon	^	hat, circumflex
045	60	2D	ENQ	enquiry	-	subtraction sign
047	61	2F	BEL	bell	/	right slash
124	6A	7C	@	at symbol		logical or
044	6B	2C	MFA	modify field attribute	,	comma
037	6C	25	LF	line feed	%	percent sign
095	6D	5F	¬	logical not	_	underscore
062	6E	3E			>	greater than
063	6F	3F	SUB	substitute	?	question mark

Decimal Value	EBCDIC Hex	ASCII Hex	EBCDIC Symbol	Meaning	ASCII Symbol	Meaning
096	79	60	-	subtraction sign	'	grave
058	7A	3A	RFF	required form feed	:	colon
035	7B	23	WUS	word underscore	#	number sign
064	7C	40	SP	space	@	at symbol
039	7D	27	ESC	escape	'	apostrophe
061	7E	3D	NAK	negative acknowledge	=	equal
034	7F	22	FS	field separator	"	straight double quotation mark
097	81	61	/	right slash	a	
098	82	62	Â		b	
099	83	63	Ä		c	
100	84	64	À		d	
101	85	65	Á		e	
102	86	66	Ã		f	
103	87	67	Å		g	
104	88	68	Ҫ		h	
105	89	69	Ñ		i	
106	91	6A	፣	split vertical bar	j	
107	92	6B	,	comma	k	
108	93	6C	%	percen sign	l	
109	94	6D	_	underscore	m	
110	95	6E	>	greater than	n	
111	96	6F	?	question mark	o	
112	97	70	Ø		p	

Decimal Value	EBCDIC Hex	ASCII Hex	EBCDIC Symbol	Meaning	ASCII Symbol	Meaning
113	98	71	É		q	
114	99	72	Ê		r	
126	A1	7E	=	equal	~	similar, tilde
115	A2	73	Ë		s	
116	A3	74	È		t	
117	A4	75	Í		u	
118	A5	76	Î		v	
119	A6	77	Ï		w	
120	A7	78	Ì		x	
121	A8	79	`	grave	y	
122	A9	7A	:	colon	z	
123	C0	7B	#	number sign	{	left brace
065	C1	41	RSP		A	
066	C2	42	â		B	
067	C3	43	ä		C	
068	C4	44	à		D	
069	C5	45	á		E	
070	C6	46	ã		F	
071	C7	47	å		G	
072	C8	48	ç		H	
073	C9	49	ñ		I	
125	D0	7D	'	apostrophe	]	right brace
074	D1	4A	¢	cent	J	
075	D2	4B	.	period	K	
076	D3	4C	<	less than	L	
077	D4	4D	(	left parenthesis	M	
078	D5	4E	+	addition sign	N	
079	D6	4F		logical or	O	

Decimal Value	EBCDIC Hex	ASCII Hex	EBCDIC Symbol	Meaning	ASCII Symbol	Meaning
080	D7	50	&	ampersand	P	
081	D8	51	é		Q	
082	D9	52	ê		R	
092	E0	5C	*	asterisk	\	left slash
083	E2	53	ë		S	
084	E3	54	è		T	
085	E4	55	í		U	
086	E5	56	↑		V	
087	E6	57	ī		W	
088	E7	58	ì		X	
089	E8	59	ß		Y	
090	E9	5A	!	exclamation point	Z	
048	F0	30			0	
049	F1	31			1	
050	F2	32	SYN	synchronous idle	2	
051	F3	33	IR	index return	3	
052	F4	34	PP	presentation position	4	
053	F5	35	TRN		5	
054	F6	36	NBS	numeric backspace	6	
055	F7	37	EOT	end of transmission	7	
056	F8	38	SBS	subscript	8	
057	F9	39	IT	indent tab	9	

## Extended Character Sets

These tables contains valid ASCII to EBCDIC extended character sets.

**Extended Character Set—ASCII Hex order**

Decimal Value	ASCII Hex	EBCDIC Hex	ASCII Character Representation	Meaning	Mapped Character	Mapping Hex
192	C0	64	À	capital A, grave	A	41
193	C1	65	Á	capital A, acute	A	41
194	C2	62	Â	capital A, circumflex	A	41
195	C3	66	Ã	capital A, tilde	A	41
196	C4	63	Ä	capital A, umlaut	A	41
197	C5	67	Å	capital A, ring	A	41
198	C6	9E	Æ	capital AE, diphthong	E	45
199	C7	68	Ç	capital C, cedilla	C	43
200	C8	74	È	capital E, grave	E	45
201	C9	71	É	capital E, acute	E	45
202	CA	72	Ê	capital E, circumflex	E	45
203	CB	73	Ë	capital E, umlaut	E	45
204	CC	78	Ì	capital I, grave	I	49
205	CE	75	Í	capital I, acute	I	49
206	CD	76	Î	capital I, circumflex	I	49
207	CF	77	Ï	capital I, umlaut	I	49
208	D0	AC	Ð	capital Eth, Icelandic	D	44
209	D1	69	Ñ	capital N, tilde	N	4E
210	D2	ED	Ò	capital O, tilde	O	4F
211	D3	EE	Ó	capital O, acute	O	4F
212	D4	EB	Ô	capital O, circumflex	O	4F
213	D5	EF	Õ	capital O, tilde	O	4F
214	D6	EC	Ö	capital O, umlaut	O	4F
215	D7	BF	×	multiply sign	x	78
216	D8	80	Ø	capital O, slash	O	4F
217	D9	FD	Ù	capital U, grave	U	55

Decimal Value	ASCII Hex	EBCDIC Hex	ASCII Character Representation	Meaning	Mapped Character	Mapping Hex
218	DA	FE	Ú	capital U, acute	U	55
219	DB	FB	Û	capital U, circumflex	U	55
220	DC	FC	Ü	capital U, umlaut	U	55
221	DD	BA	Ý	capital Y, acute	Y	59
222	DE	AE	þ	capital THORN, Icelandic	P	50
223	DF	59	ß	small sap s, German	S	53
224	E0	44	à	small a, grave	a	61
225	E1	45	á	small a, acute	a	61
226	E2	42	â	small a, circumflex	a	61
227	E3	46	ã	small a, tilde	a	61
228	E4	43	ä	small a, umlaut	a	61
229	E5	47	å	small a, ring	a	61
230	E6	9C	æ	small ae diphthong	e	65
231	E7	48	ç	small c, cedilla	c	63
232	E8	54	è	small e, grave	e	65
233	E9	51	é	small e, acute	e	65
234	EA	52	ê	small e, circumflex	e	65
235	EB	53	ë	small e, umlaut	e	65
236	EC	58	ì	small i, grave	i	69
237	ED	55	í	small i, acute	i	69
238	EE	56	î	small i, circumflex	i	69
239	EF	57	ï	small i, umlaut	i	69
240	F0	8C	ð	small eth, Icelandic	d	64
241	F1	49	ñ	small n, tilde	n	6E
242	F2	CD	ò	small o, grave	o	6F
243	F3	CE	ó	small o, acute	o	6F
244	F4	CB	ô	small o, circumflex	o	6F
245	F5	CF	õ	small o, tilde	o	6F

Decimal Value	ASCII Hex	EBCDIC Hex	ASCII Character Representation	Meaning	Mapped Character	Mapping Hex
246	F6	CC	ö	small o, umlaut	o	6F
247	F7	E1	÷	division sign	/	2F
248	F8	70	ø	small o, slash	o	6F
249	F9	DD	ù	small u, grave	u	75
250	FA	DE	ú	small u, acute	u	75
251	FB	DB	û	small u, circumflex	u	75
252	FC	DC	ü	small u, umlaut	u	75
253	FD	8D	ý	small y, acute	y	79
254	FE	8E	þ	small thorn, Icelandic	p	70
255	FF	DF	ÿ	small y, umlaut	y	79

**Extended Character Set—EBCDIC Hex order**

Decimal Value	EBCDIC Hex	ASCII Hex	ASCII Character Representation	Meaning	Mapped Character	Mapping Hex
226	42	E2	â	small a, circumflex	a	61
228	43	E4	ä	small a, umlaut	a	61
224	44	E0	à	small a, grave	a	61
225	45	E1	á	small a, acute	a	61
227	46	E3	ã	small a, tilde	a	61
229	47	E5	å	small a, ring	a	61
231	48	E7	ç	small c, cedilla	c	63
241	49	F1	ñ	small n, tilde	n	6E
233	51	E9	é	small e, acute	e	65
234	52	EA	ê	small e, circumflex	e	65
235	53	EB	ë	small e, umlaut	e	65
232	54	E8	è	small e, grave	e	65
237	55	ED	í	small i, acute	i	69
238	56	EE	î	small i, circumflex	i	69

Decimal Value	EBCDIC Hex	ASCII Hex	ASCII Character Representation	Meaning	Mapped Character	Mapping Hex
239	57	EF	ï	small i, umlaut	i	69
236	58	EC	ì	small i, grave	i	69
223	59	DF	ß	small sap s, German	S	53
194	62	C2	Â	capital A, circumflex	A	41
196	63	C4	Ä	capital A, umlaut	A	41
192	64	C0	À	capital A, grave	A	41
193	65	C1	Á	capital A, acute	A	41
195	66	C3	Ã	capital A, tilde	A	41
197	67	C5	Å	capital A, ring	A	41
199	68	C7	Ҫ	capital C, cedilla	C	43
209	69	D1	Ñ	capital N, tilde	N	4E
248	70	F8	ø	small o, slash	o	6F
201	71	C9	É	capital E, acute	E	45
202	72	CA	Ê	capital E, circumflex	E	45
203	73	CB	Ë	capital E, umlaut	E	45
200	74	C8	È	capital E, grave	E	45
205	75	CE	Í	capital I, acute	I	49
206	76	CD	Î	capital I, circumflex	I	49
207	77	CF	Ï	capital I, umlaut	I	49
204	78	CC	Ї	capital I, grave	I	49
216	80	D8	Ø	capital O, slash	O	4F
240	8C	F0	ð	small eth, Icelandic	d	64
253	8D	FD	ý	small y, acute	y	79
254	8E	FE	þ	small thorn, Icelandic	p	70
230	9C	E6	æ	small ae diphthong	e	65
198	9E	C6	Æ	capital AE, diphthong	E	45
208	AC	D0	Ð	capital Eth, Icelandic	D	44
222	AE	DE	Þ	capital THORN, Icelandic	P	50

Decimal Value	EBCDIC Hex	ASCII Hex	ASCII Character Representation	Meaning	Mapped Character	Mapping Hex
221	BA	DD	Ý	capital Y, acute	Y	59
215	BF	D7	×	multiply sign	×	78
244	CB	F4	ô	small o, circumflex	o	6F
246	CC	F6	ö	small o, umlaut	o	6F
242	CD	F2	ð	small o, grave	o	6F
243	CE	F3	ó	small o, acute	o	6F
245	CF	F5	ö	small o, tilde	o	6F
251	DB	FB	û	small u, circumflex	u	75
252	DC	FC	ü	small u, umlaut	u	75
249	DD	F9	ù	small u, grave	u	75
250	DE	FA	ú	small u, acute	u	75
255	DF	FF	ÿ	small y, umlaut	y	79
247	E1	F7	÷	division sign	/	2F
212	EB	D4	Ô	capital O, circumflex	O	4F
214	EC	D6	Ö	capital O, umlaut	O	4F
210	ED	D2	Ò	capital O, tilde	O	4F
211	EE	D3	Ó	capital O, acute	O	4F
213	EF	D5	Õ	capital O, tilde	O	4F
219	FB	DB	Û	capital U, circumflex	U	55
220	FC	DC	Ü	capital U, umlaut	U	55
217	FD	D9	Ù	capital U, grave	U	55
218	FE	DA	Ú	capital U, acute	U	55

### Swedish Domestic Authorization Switching Character Set

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

EBCDIC IBM-278	EBCDIC (Hexadecimal)	ASCII (Hexadecimal)	Graphic	Attribute
Å	5B	24	\$	s
Ä	7B	23	#	s

---

EBCDIC IBM-278	EBCDIC (Hexadecimal)	ASCII (Hexadecimal)	Graphic	Attribute
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.....	76
About Authorization Messages.....	76
Authorization Request/0100.....	76
Authorization Request Response/0110.....	76
About Authorization Advice Messages.....	77
Authorization Advice/0120—Acquirer-Generated.....	77
Authorization Advice/0120—Issuer-Generated.....	78
Authorization Advice/0120—System-Generated.....	78
Authorization Advice Response/0130—Issuer-Generated (Responding to an Acquirer-Generated 0120).....	79
Authorization Advice Response/0130—Issuer-Generated (Responding to a System-Generated 0120 from SAF).....	79
Authorization Advice Response/0130—System-Generated.....	79
About Authorization Response Acknowledgement Messages.....	79
Authorization Acknowledgement/0180.....	80
Authorization Negative Acknowledgement/0190.....	80
About Issuer File Update Messages.....	80
Issuer File Update Request/0302.....	80
Issuer File Update Request Response/0312.....	81
About Reversal Messages.....	81
Reversal Request/0400.....	81
Reversal Request Response/0410.....	81
Reversal Advice/0420.....	82
Reversal Advice Response/0430.....	82
About Administrative Messages.....	82
Administrative Request/0600.....	83
Administrative Request Response/0610.....	83
Administrative Advice/0620.....	83
Administrative Advice Response/0630.....	84
About Network Management Messages.....	84
Network Management Request/0800.....	85
Network Management Request Response/0810.....	85

---

Network Management Advice/0820.....	85
About Message Flows.....	86
Authorization Message Routing Timers.....	86
Authorization Request/0100 and Authorization Request Response/0110.....	87
Authorization Request/0100—Communication Failure at Acquirer.....	88
Authorization Request/0100—Communication Failure at Issuer.....	88
Authorization Request Response/0110—Communication Failure at Acquirer.....	90
Authorization Request Response/0110—Communication Failure at Issuer.....	91
Authorization Request Response/0110—Stand-In System Allowed.....	92
Authorization Request Response/0110—Not Received within the Time Limit.....	92
Authorization Request Response/0110—Received within the Time Limit but after Stand-In System Response.....	93
Authorization Request Response/0110—Received within the Time Limit and before Stand-In System Response.....	94
Authorization Request Response/0110—Not Eligible for Alternate Processing.....	95
Authorization Request Response/0110—No Issuer Response within Issuer Response Time Limit.....	96
Authorization Request Response/0110—Late Issuer Response.....	96
Authorization Request Response/0110—Issuer Edit Error.....	97
Authorization Request/0100—Chip PIN Management.....	98
Authorization Request/0100—Chip PIN Management (Failure to Transmit/Apply Script to Chip Card).....	99
Authorization Request/0100—Chip PIN Management (Issuer Network Failure-Unable to Connect).....	101
Authorization Request/0100—Chip PIN Management (Issuer Network Failure, No Response from Issuer).....	102
Authorization Request/0100—Chip PIN Management (Acquirer Network Failure-Unable to Connect).....	104
Authorization Request/0100—Chip PIN Management (Acquirer Network Failure-Unable to Connect with Acquirer).....	105
Guaranteed Advice Message Delivery.....	106
Standard Advice Delivery—All Advice Message Types.....	107
Authorization Advice/0120—Acquirer-Generated, Issuer Available.....	107
Authorization Advice/0120—Acquirer-Generated, Issuer Unavailable.....	108
Authorization Advice/0120—Issuer-Generated.....	109
Authorization Advice/0120—System-Generated.....	109
Advice Message Error Condition.....	110
Acquirer Response Acknowledgement/0180 Messages.....	111
Alternate Issuer Host Processing for Online Europe Region Customers.....	112

---

Authorization Request/0100—Communication Failure at Issuer (Issuer is not signed in or transaction cannot be delivered).....	113
Authorization Request Response/0110—Alternate Issuer Allowed.....	113
Authorization Request Response/0110—Not Received within Time Limit.....	115
Authorization Request Response/0110—Received within the Time Limit but after Alternate Issuer Response.....	116
Authorization Request Response/0110—Received within the Time Limit and before Alternate Issuer Response.....	117
Authorization Response Negative Acknowledgement/0190 (Responding to the Authorization Request Response/0110).....	118
Authorization Response Negative Acknowledgement/0190 (Responding to the Reversal Request Response/0410).....	118
Issuer File Update Request/0302 and Issuer File Update Request Response/0312.....	119
Reversal Messages.....	120
Reversal Request/0400 and Reversal Request Response/0410.....	120
Reversal Request/0400—No Issuer Response Received within the Time Limit.....	121
Reversal Request/0400—Issuer Response Received after the Time Limit.....	122
Reversal Request/0400—Issuer Signed Off.....	122
Reversal Request/0400—Issuer Response Contains Errors.....	123
Reversal Request/0400—Not Delivered to Issuer.....	124
Reversal Request Response/0410—Not Delivered to Acquirer.....	125
Reversal Advice/0420 and Reversal Advice Response/0430.....	125
Administrative Request/0600 and Administrative Request Response/0610.....	126
Administrative Request/0600, Acquirer Edit Failure.....	126
Administrative Request/0600, Communication Failure at Issuer.....	127
Administrative Request Response/0610, Communication Failure at Acquirer.....	127
Administrative Request Response/0610, No Issuer Response.....	128
Administrative Request Response/0610, Late Issuer Response.....	128
Administrative Request Response/0610, Issuer Edit Failure.....	129
Administrative Advice/0620 and Administrative Advice Response/0630.....	129
Administrative Advice/0620 and Administrative Advice Response/0630—Invalid Message, System-Generated.....	130
Network Management Request 0800—Sign-On/Sign-Off.....	130
Network Management Request/0800—Solicited SAF.....	131
Network Management Request/0800—Unsolicited SAF.....	132
Network Management Request/0800—Network Connection Status, Member-Generated.....	133
Network Management Request/0800—Network Connection Status, System-Generated.....	133
Network Management Request/0800—Host Session Activation/Deactivation.....	134
Network Management Request/0800—PEK Exchange Authorization Platform-Initiated.....	134
Network Management Request/0800—PEK Exchange Member-Initiated.....	135

## 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 processing 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.

#### 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 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—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—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.

### **Offline Account Status Inquiry for Account Ranges Registered for the Authentication Indicator Service**

Acquirers of merchants supporting EMV®<sup>2</sup> offline account status inquiry transactions send an Authorization Advice/0120 message containing DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code), value 192 (M/Chip Offline Advice to Issuer) to the issuer.

### **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 risk scoring system. The risk 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.

---

### **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.

---

<sup>2</sup> EMV is a registered trademark or trademark of [EMVCo LLC](#) in the United States and other countries.

### **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.

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

## **About Administrative Messages**

Administrative messages request confirmation of data or transmit 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.

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 System 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.
- Administrative Advice/0620—Member-generated messages are used to transmit administrative (free format) textual messages between any two parties participating as customers on the Authorization Platform.

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, customer processing systems (CPSs), acquirer processing systems (APSs), issuer processing systems (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

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 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: May not be originated by any party other than the Authorization Platform.</b>	
Response	None

## 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, system-generated Reversal/0420, 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>a</sup>	3	12 <sup>b</sup>
Mastercard—POS PIN for Credit	18 <sup>c</sup>	6	24
Mastercard—ATM	12	6	18
Debit Mastercard—POS	Same as Mastercard Credit—POS		
Maestro—All	18 <sup>d</sup>	6	24
CIRRUS—ATM	18	6	24
Private Label—POS	12	6	18
AMEX—POS	12	6	18

Product and Transaction Type	Issuer Response Time (in seconds)	Alternate Authorization Service Provider (if applicable)	Acquirer Minimum Wait Time (in seconds)
Visa—POS	12	6	18

<sup>a</sup> 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.

<sup>b</sup> Because the Mastercard 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).

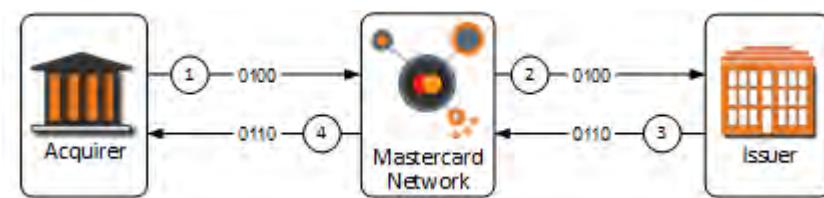
<sup>c</sup> A transaction is considered to be PIN for Credit if it is Dual Message System acquired, but the issuer keys are managed by the Single Message System. If the issuer is Dual Message System managed, the transaction is not flagged as being PIN for Credit and defaults to the standard POS timer of 9 seconds.

<sup>d</sup> For Maestro POS transactions acquired in the Netherlands, Mastercard has reduced the timer to 7 seconds, which is the maximum time Mastercard will wait before invoking alternate authorization provider processing. If no response is received within 10 seconds, Mastercard will send a time-out response to the acquirer.

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 Bulletin*.

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

This message flow describes the standard authorization transaction process.

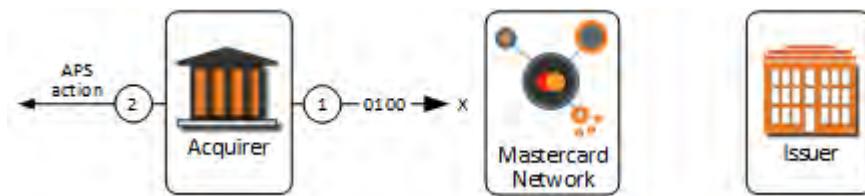


1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Authorization Request/0100 message to the issuer.
3. The issuer generates an appropriate Authorization Request Response/0110 message and sends it to the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

**NOTE:** 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).



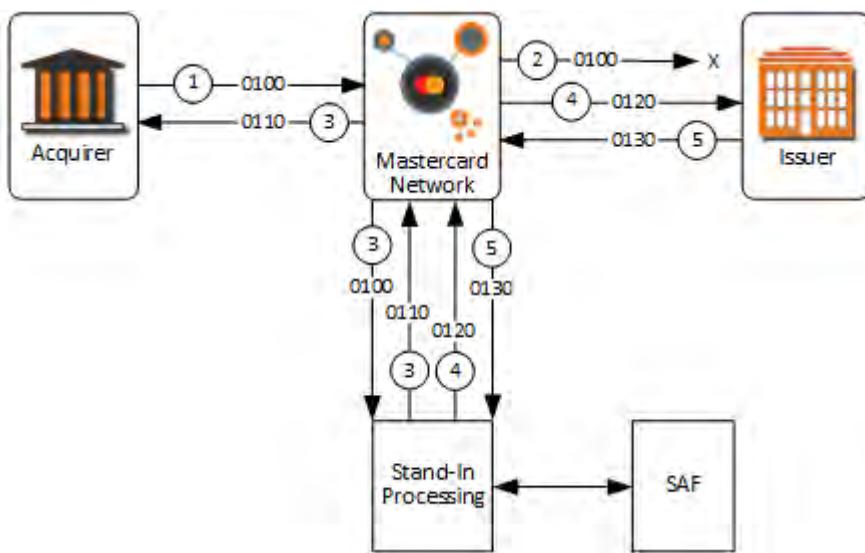
1. The acquirer initiates an Authorization Request/0100 message, but it cannot be delivered to the Authorization Platform because of system failure.
2. The acquirer completes the transaction at the point of interaction. In most cases, the APS simply denies the transaction. However, the APS may elect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

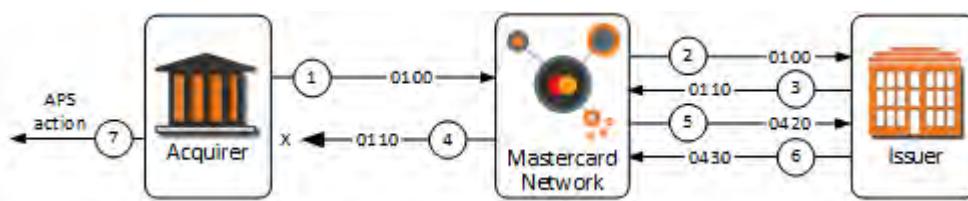
**NOTE: Stand-In processing generates and forwards Authorization Advice/0120 messages for “approved,” “declined,” and “capture card” Authorization Request/0100 messages.**

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 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, 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 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.

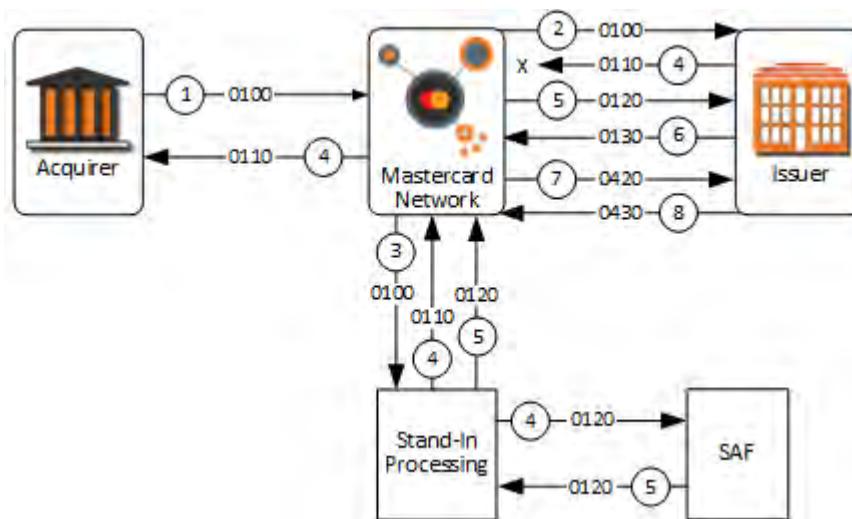
6. The issuer responds back to the Authorization Platform with a Reversal Advice Response/0430 message to acknowledge positive receipt of the Reversal Advice/0420 message.
7. Meanwhile, if the APS is still operating, it detects a time-out condition on the Authorization Request Response/0110 message that 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.

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.

**NOTE: 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.**

### 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.
- 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 (Issuer Time-out)
  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:

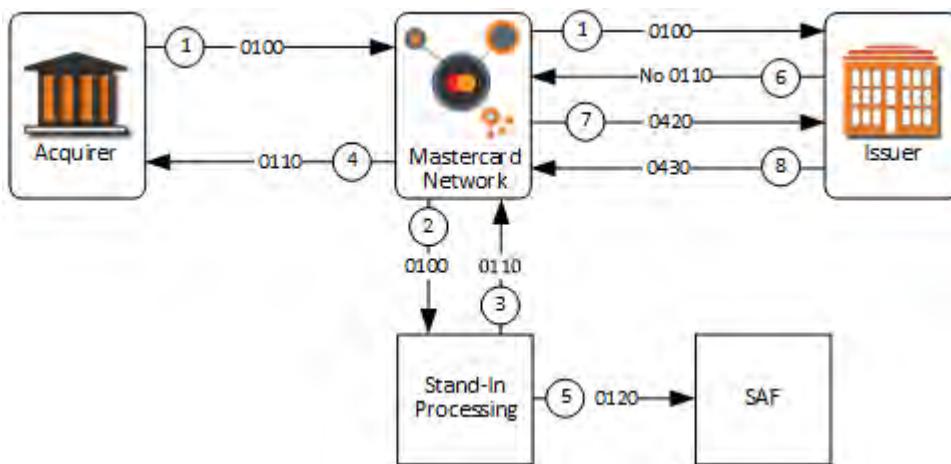
- Authorization Request Response/0110—Not Received within Time Limits
- Authorization Request Response/0110—Received within the Time Limit but after Stand-In System Response
- Authorization Request Response/0110—Received within Time Limit and before Stand-In System Response

**NOTE: Authorization Message Routing Timers provides details regarding specific time limits.**

### **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

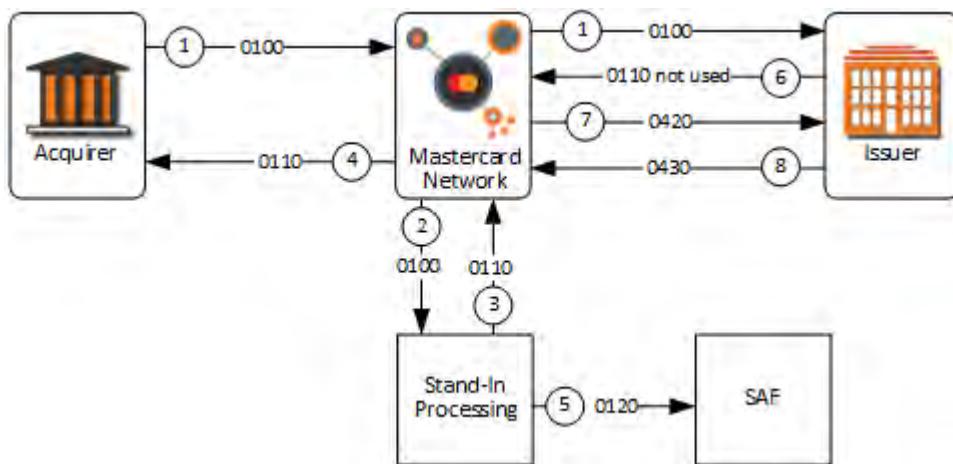
Authorization Request/0100 message for transactions that are allowed to be processed by the Stand-In System.



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 (Issuer Time-out)
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**

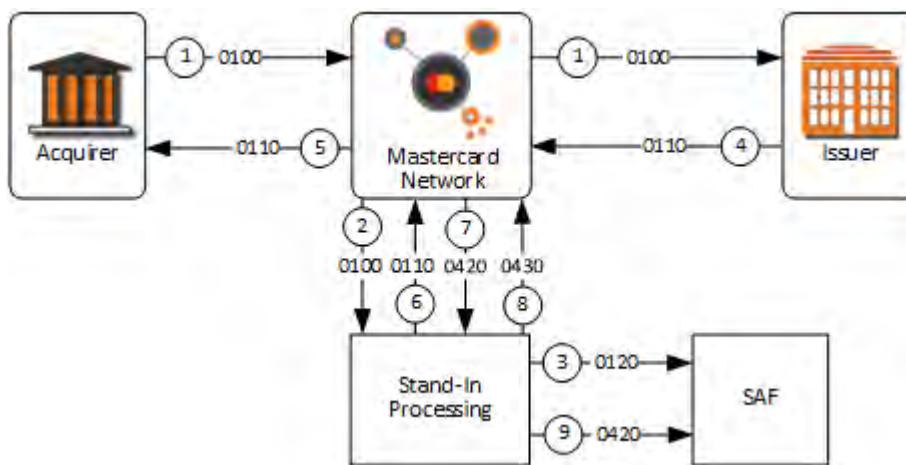
This message flow describes exception processing when the issuer's Authorization Request Response/0110 message is received within the time limit but after the Stand-In System response. Issuers can retrieve SAF messages upon request.



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**

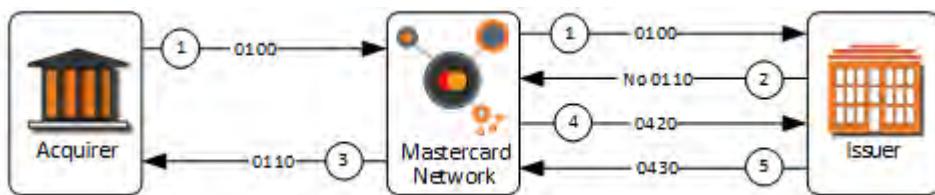
These message flows describe authorization message processing when the transaction is not eligible for alternate processing.

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

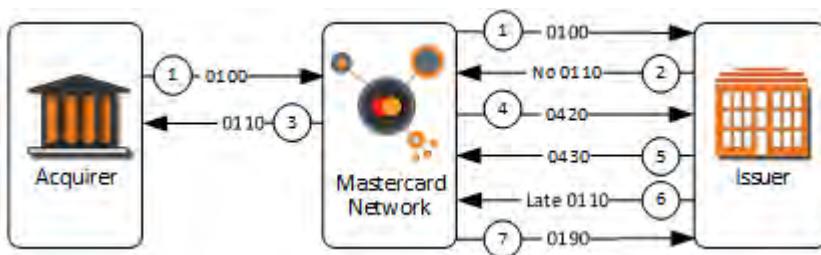
This message flow describes exception processing when the issuer's Authorization Request Response/0110 message is not received within the allowed issuer response time limit after receipt of the Authorization Request/0100 message.



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 (Authorization System or issuer system 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 (Issuer Time-out)
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 (Authorization System or issuer system 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 (Issuer Time-out)
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**

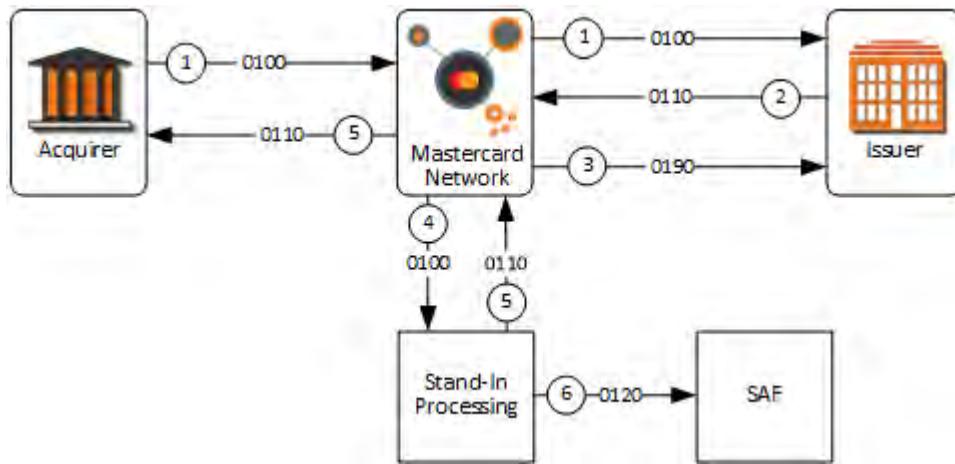
This message flow describes exception processing when an invalid issuer Authorization Request Response/0110 message is received after receipt of the Authorization Request/0100 message for transactions that are allowed to be processed by the Stand-In System.

Mastercard will provide the issuer's response to the Authorization Request/0110 message whenever possible. If the issuer returns an Authorization Request Response/0110 message, Mastercard evaluates the authorization response to determine if the transaction can be parsed and if data element (DE) 39 (Response Code) can be read. If DE 39 can be read and the issuer has approved the transaction, inclusive of the following response codes, this message flow is used (the request is sent to Stand-In processing):

- 00 Approved or completed successfully
- 10 Partial Approval
- 87 Purchase Amount Only, No Cash Back Allowed
- 91 Authorization System or issuer system inoperative
- 92 Unable to route transaction
- 96 System error (inclusive of Response Codes)

If the response code is any other than those previously listed, Mastercard replaces or removes the data responsible for the format error and forwards the remainder of the message to the

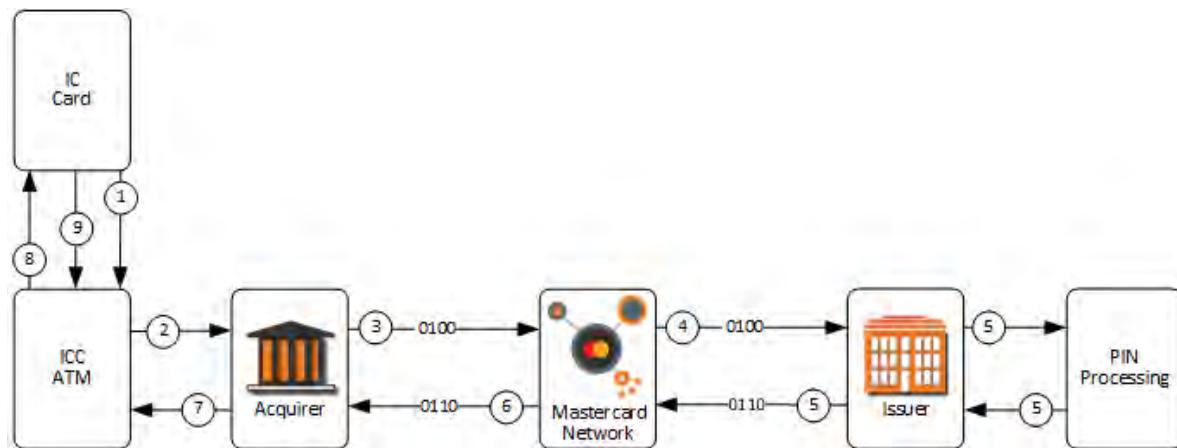
acquirer. Mastercard continues to log information relevant to the format error for reference purposes.



1. The acquirer sends the Authorization Request/0100 message.
2. The issuer generates an invalid or late Authorization 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 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

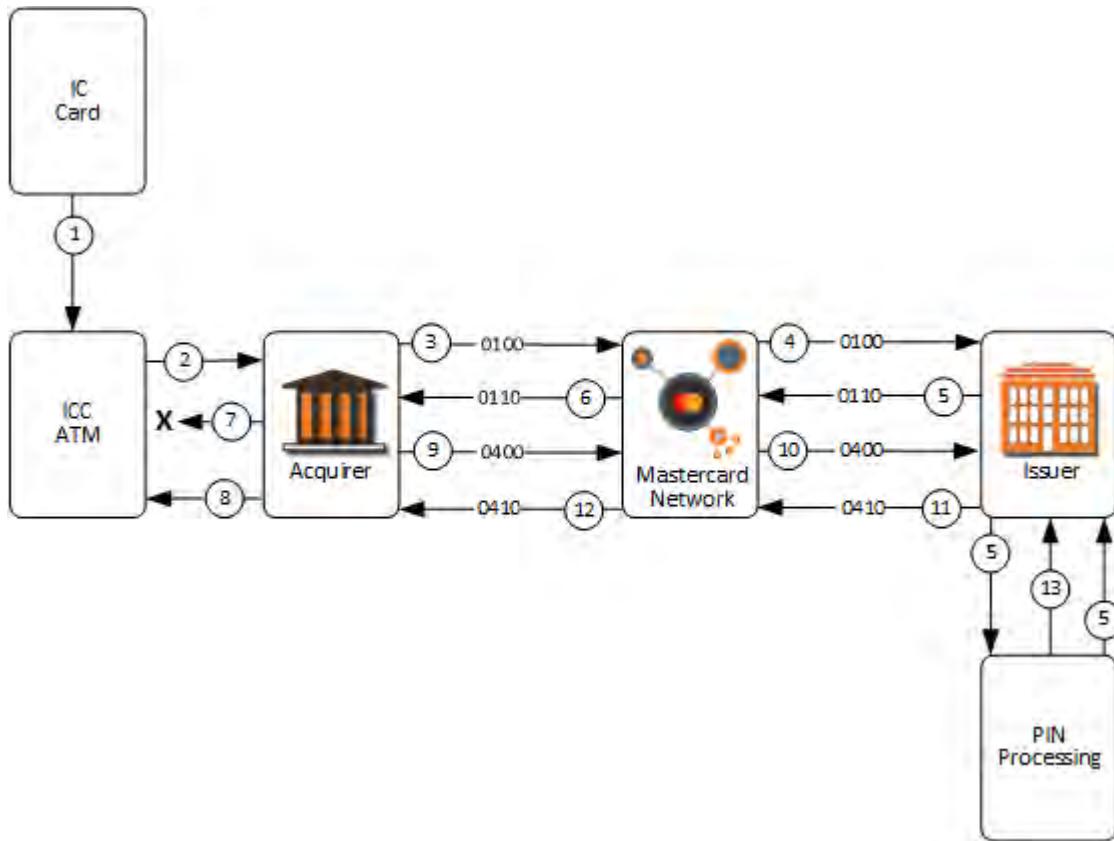
This message flow describes standard transaction processing when changing or unblocking a PIN on a chip card.



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.
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.

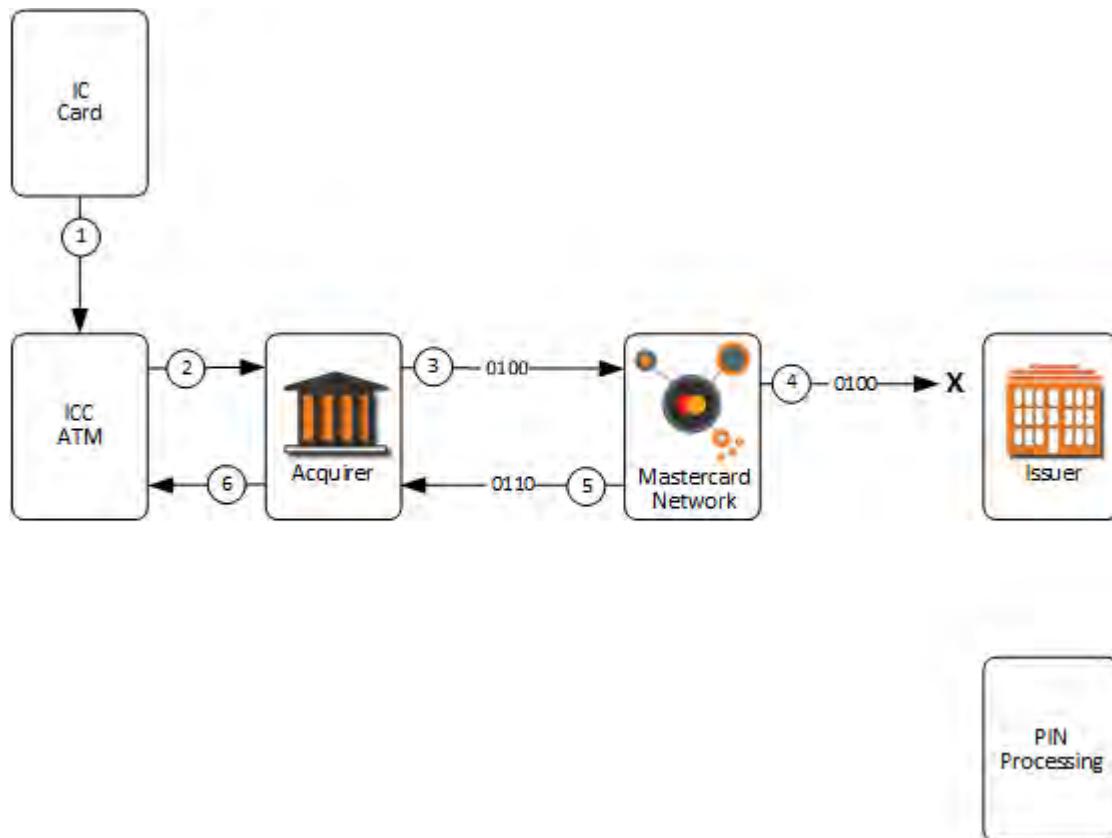


1. The cardholder initiates a PIN change or PIN unblock transaction at the ATM.
2. The ATM requests an Authorization Request Cryptogram (ARQC) from the chip card.
  - For a **PIN change** transaction, if the card does not provide the ARQC and declines the request with an Application Authentication Cryptogram (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.

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)**

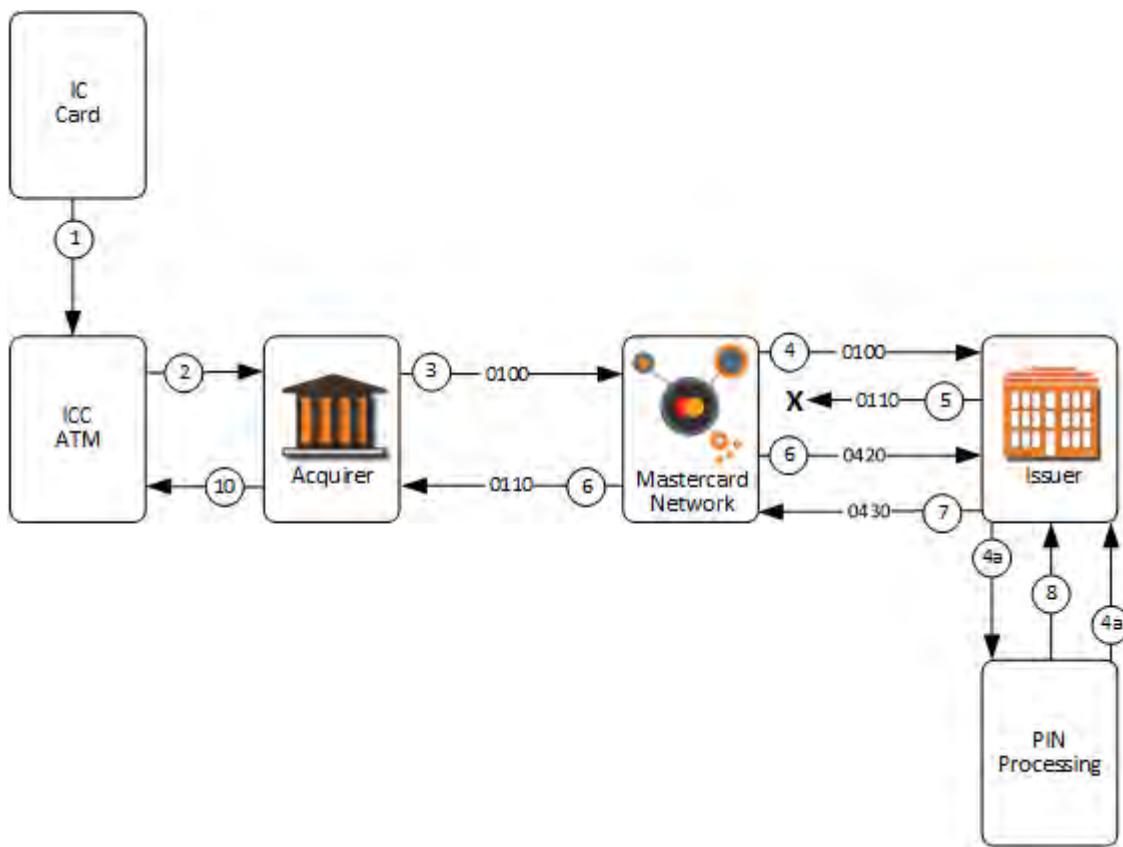
This message flow describes the transaction process when there is a network failure at the issuer.



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 System 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.



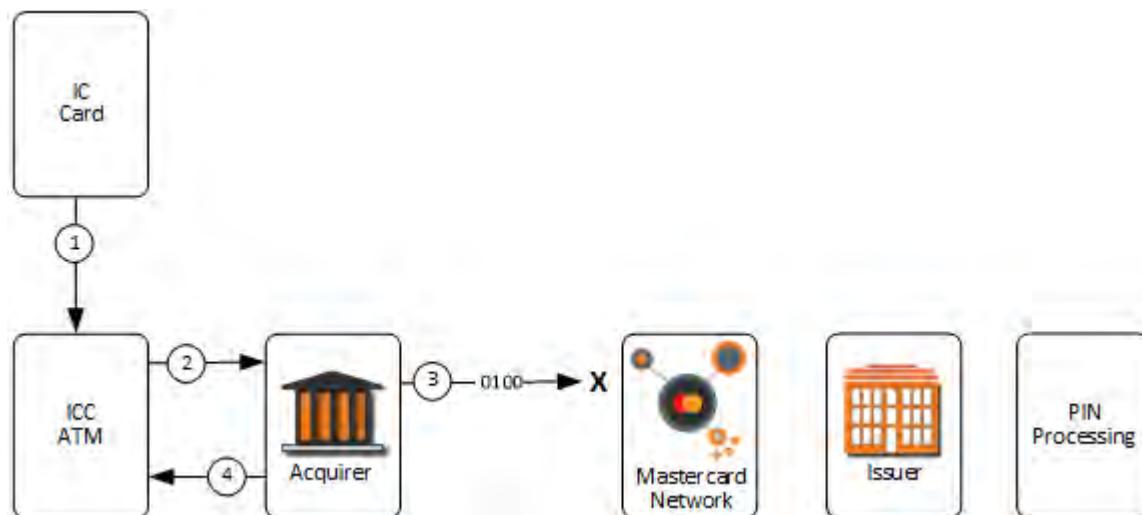
1. The cardholder initiates a PIN change or PIN unblock transaction at the ATM.
  2. The ATM requests an Authorization Request Cryptogram (ARQC) with a zero amount from the chip card.
    - For a PIN change transaction, if the card does not provide the ARQC and declines the request with an Application 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.
- 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 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>3</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 System or issuer system inoperative).
10. The acquirer sends a message to the ATM, indicating that the service is unavailable.

### **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.



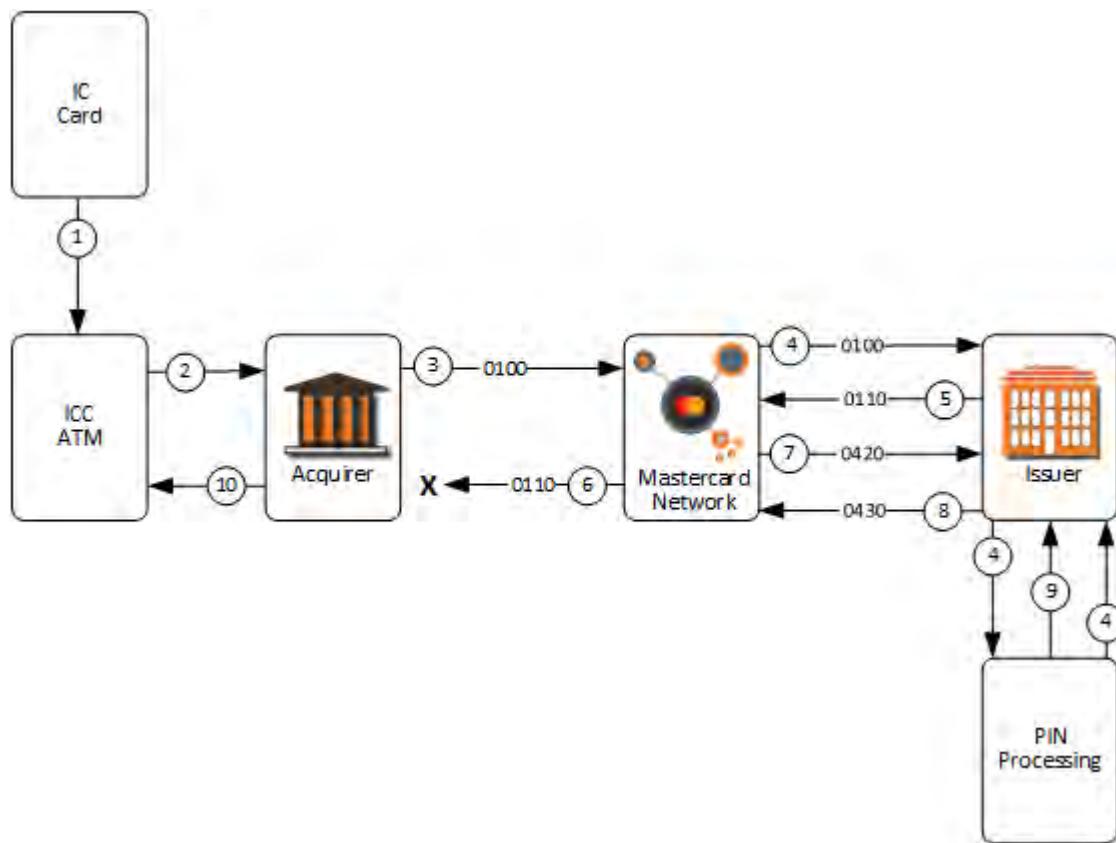
1. The cardholder initiates a PIN change or PIN unblock transaction at the ATM.
2. The ATM requests an Authorization Request Cryptogram (ARQC) with a zero amount from the chip card.
  - For a **PIN change** transaction, if the card does not provide the ARQC and declines the request with an Application 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.

<sup>3</sup> For Mastercard and Debit Mastercard only.

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.
  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 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.

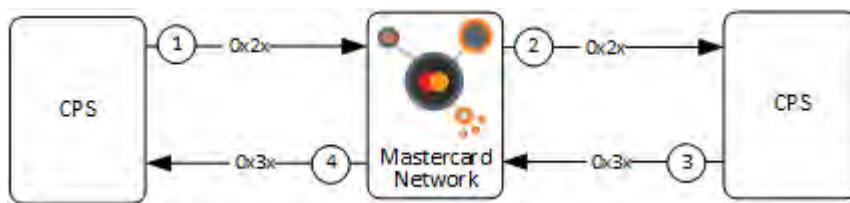
Authorization Advice/0120—Acquirer-generated messages are immediately sent to the issuer. The issuer responds with an Authorization Advice/0130—Issuer-generated message that the Authorization Platform forwards to the acquirer.

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

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

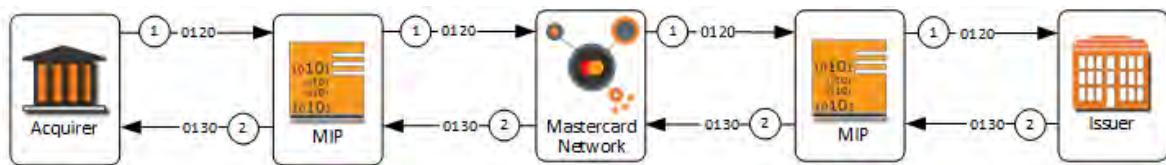


1. The CPS forwards the advice message to the Authorization Platform.
2. The Authorization Platform returns an appropriate advice response message when it secures the advice message.
3. The Authorization Platform forwards the advice message to the receiving entity.
4. The receiving entity returns an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



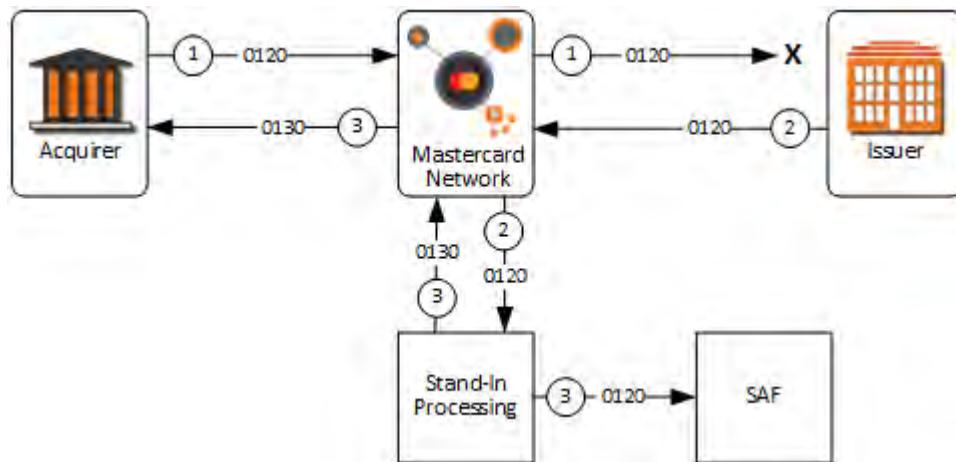
1. The acquirer initiates an Authorization Advice/0120—Acquirer-generated message containing DE 60, subfield 1, value 190 or 191, and then passes the 0120 message to the Authorization Platform.

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).

#### **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.



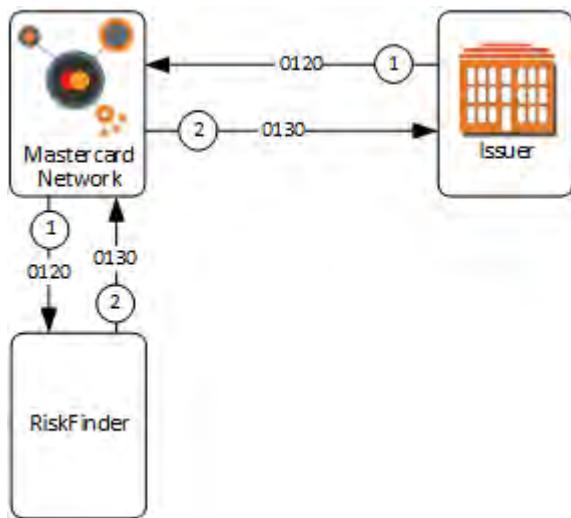
1. The acquirer initiates an Authorization Advice/0120—Acquirer-generated message containing DE 60, subfield 1, value 190 or 191, and then forwards the 0120 message to the Authorization Platform.
2. The Authorization Platform determines that the Authorization Advice/0120—Acquirer-generated message cannot 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: Customers 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 risk scoring system. The risk scoring system sends to the issuer an Authorization Advice Response/0130 message to acknowledge receipt of the Authorization Advice/0120 message.

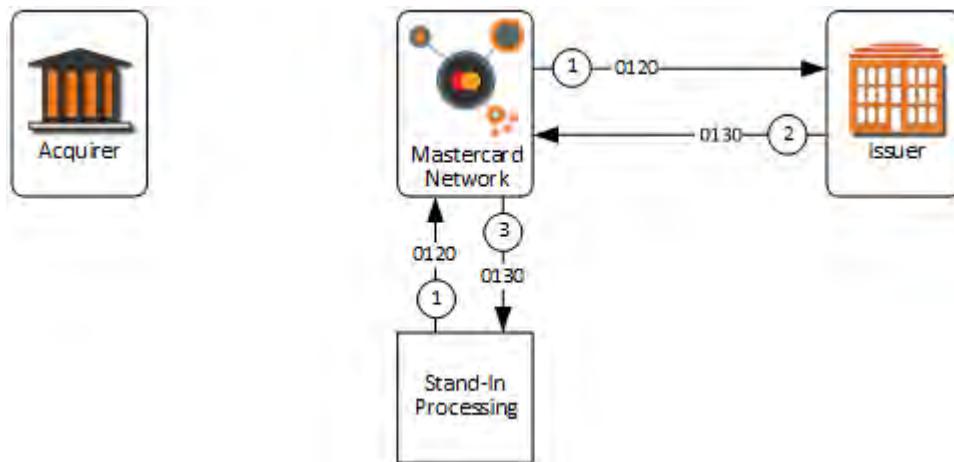


1. The issuer initiates an Authorization Advice/0120—Issuer-generated message and sends it to the Authorization Platform. The Authorization Platform forwards the message to the risk scoring system.
2. The risk scoring system creates an Authorization Advice Response/0130—System-generated message and sends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

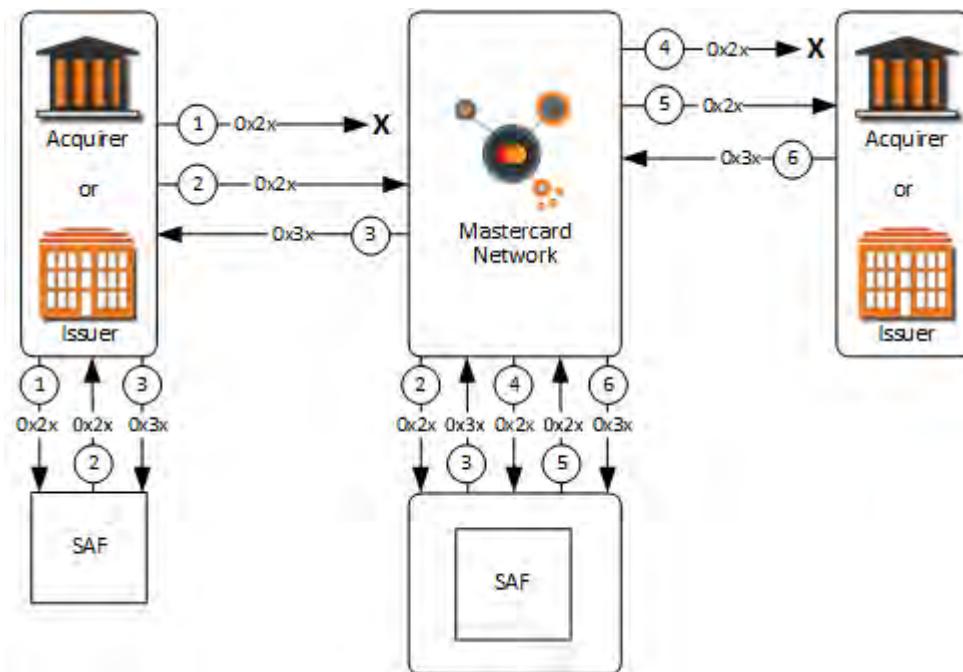


1. Stand-In System processing generates an Authorization Advice/0120—System generated message and sends it to the issuer.
2. The issuer returns an Authorization Advice Response/0130—Issuer-generated message.
3. The Authorization Platform receives the Authorization Advice Response/0130—Issuer-generated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

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.

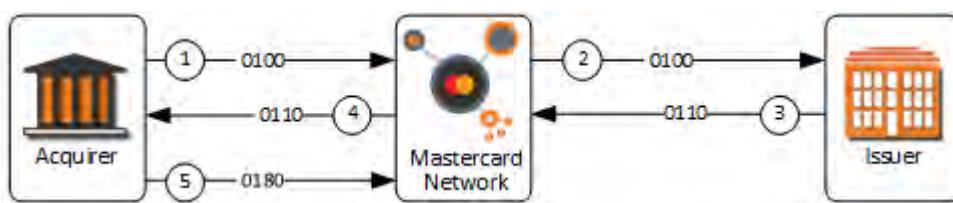
### Acquirer Response Acknowledgement/0180 Messages

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 Customers

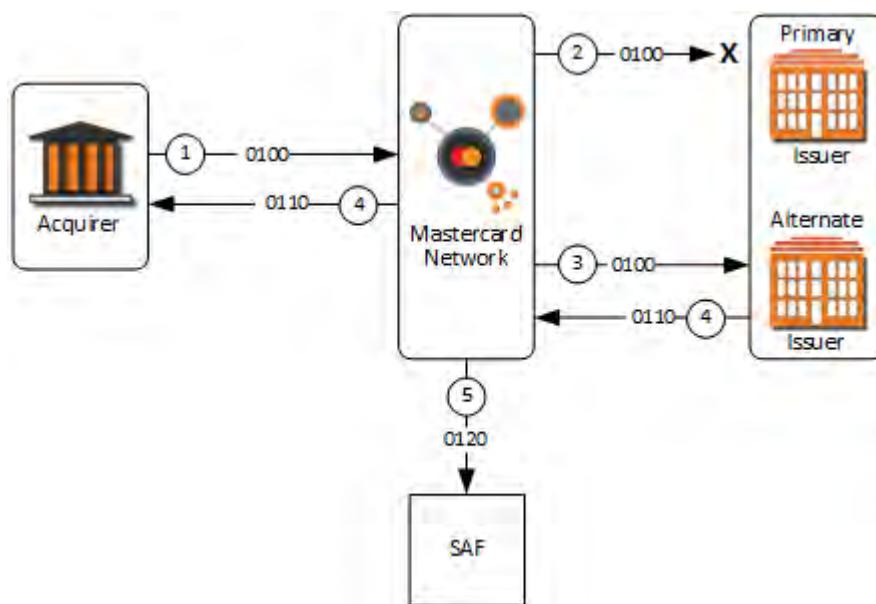
To support customers in the Europe region that route to an alternate issuer host for alternate processing instead of using the Stand-In System, Mastercard offers alternate issuer host processing.

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)

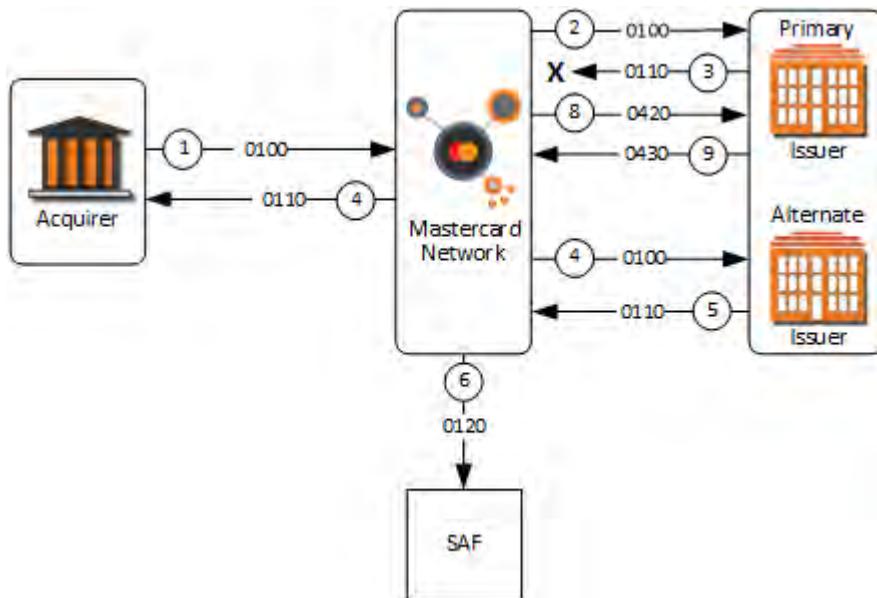
This message flow describes exception processing when the primary issuer is not signed in, the transaction could not be delivered to the primary issuer, or when the primary issuer does not respond with an Authorization Response/0110 message within the time limit defined for the acceptance brand.



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

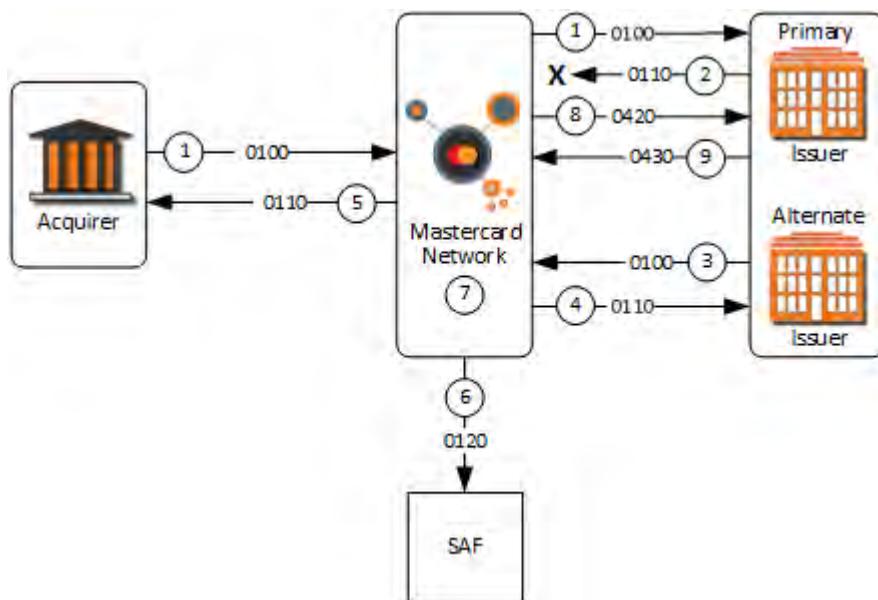
This message flow describes exception processing when communication fails between the Authorization Platform and the issuer processing system (IPS) during an Authorization Request Response/0110 message.



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 (Issuer Time-out)
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.

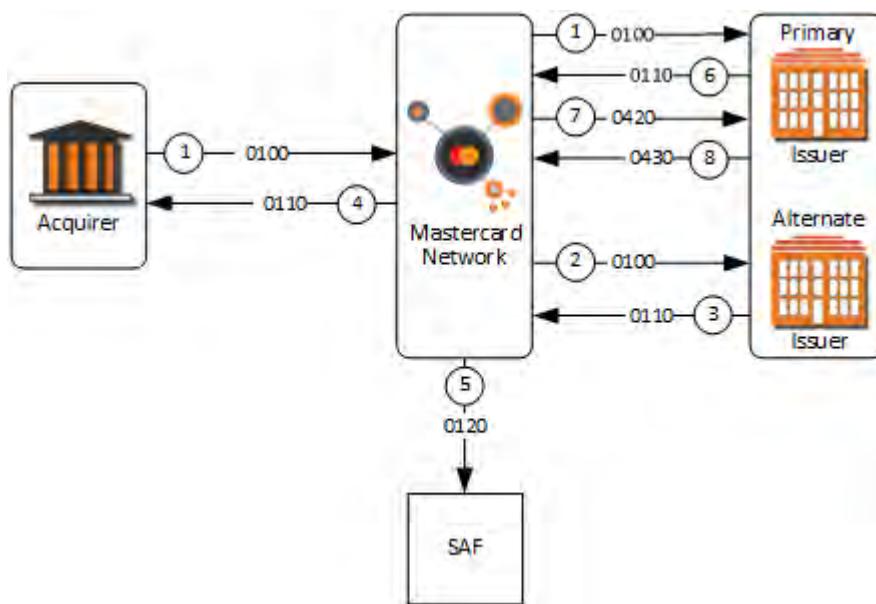


1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization Platform and then the Authorization Platform forwards the Authorization Request/0100 message to the primary issuer.
2. The Authorization Platform does not receive the Authorization Request Response/0110 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 (Issuer Time-out)

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.

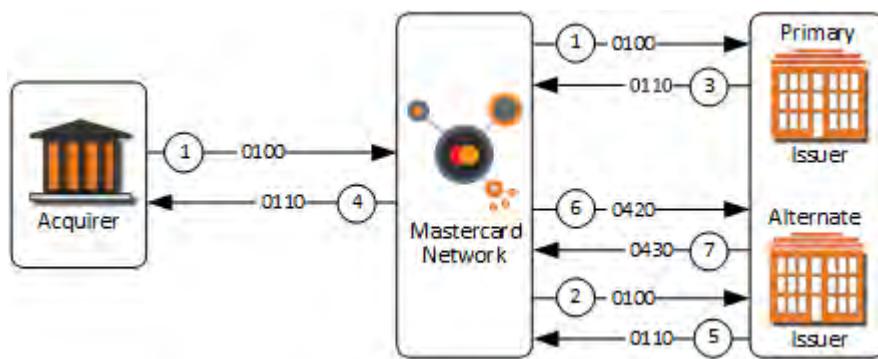


1. The acquirer initiates an Authorization Request/0100 message and sends it to the Authorization Platform and then the Authorization Platform forwards the Authorization Request/0100 message to the primary issuer.
2. If the Authorization Platform does not receive the Authorization Request Response/0110 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.

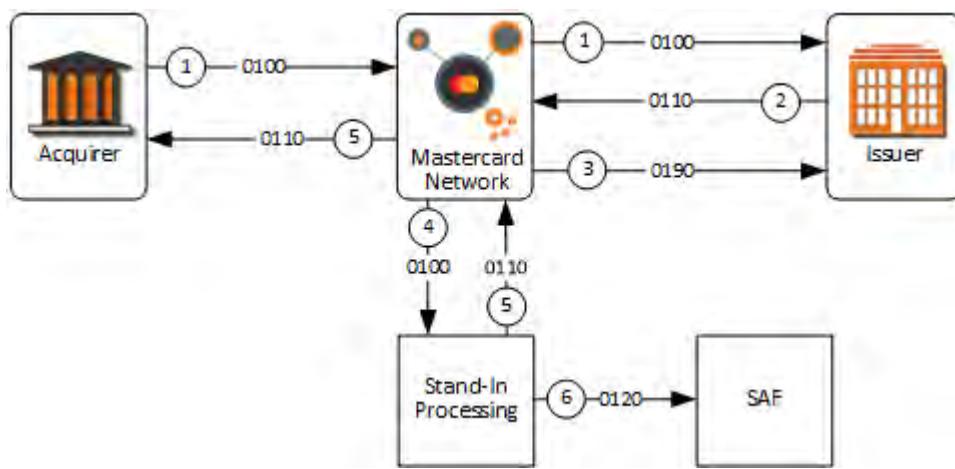


1. The acquirer sends the Authorization Request/0100 message to the Authorization Platform, and the Authorization Platform forwards the Authorization Request/0100 message to the primary issuer.
2. If the Authorization Platform does not receive the Authorization Request Response/0110 message within the 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)

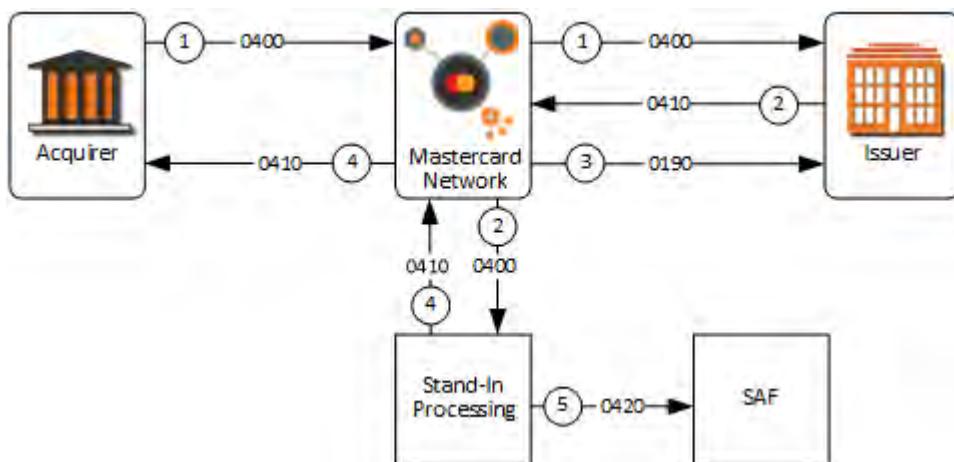
This message flow describes transaction processing when the issuer host generates an invalid or late Authorization Request Response/0110 message, and the Stand-In System processes the transaction and generates a response on behalf of the issuer. The Authorization Platform also sends an Authorization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

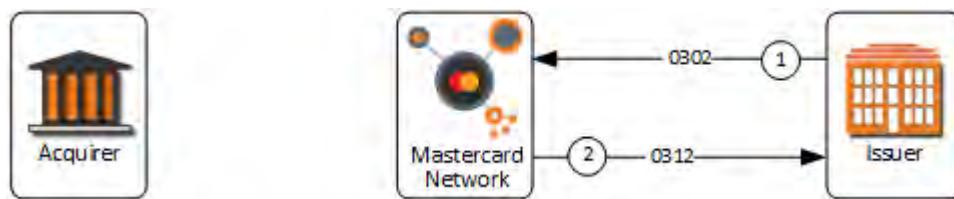


1. The acquirer sends the Reversal Request/0400 message.
2. The issuer generates an invalid or late Reversal Request Response/0410 message and forwards it to the Authorization Platform. The Authorization Platform routes the Reversal Request/0400 to the Stand-In System.
3. The Authorization Platform sends 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: Customers in the Europe region that route to an alternate issuer host for alternate processing instead of the Stand-In System will still receive a Reversal Advice/0420 message 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 is 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 acquirers 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).**

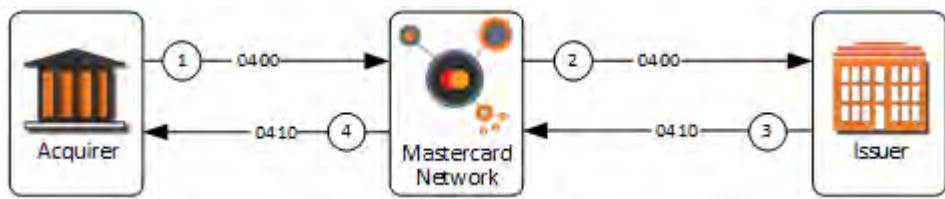
**The acquirer must send a Reversal Request/0400 message as a result of an acquirer time-out based on transaction processing rules dictated by the brand. When an acquirer sends a reversal, it is possible that an issuer will receive two reversals for the same authorization request. Issuers must decline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

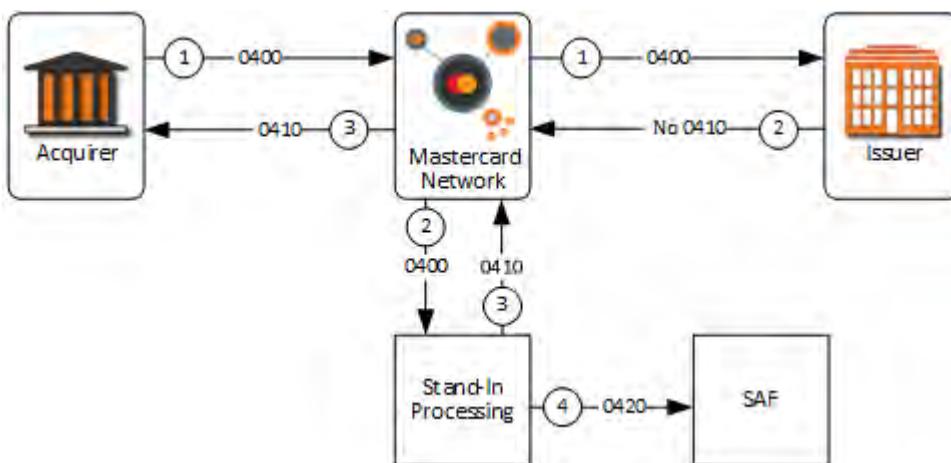
This message flow describes transaction processing of the Reversal Request/0400 and Reversal Request Response/0410 messages.



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.

#### **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.

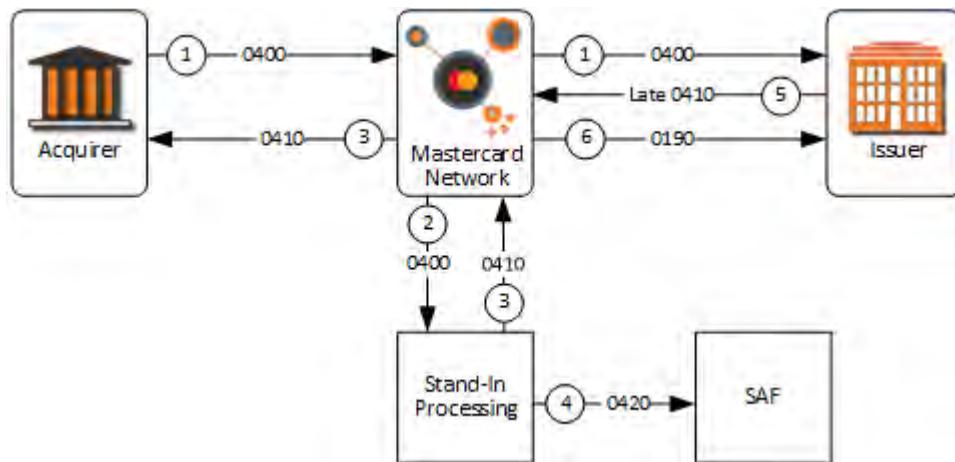


1. The acquirer sends the Reversal Request/0400 message to the Authorization Platform, and then the Authorization Platform forwards the Reversal Request/0400 message to the issuer.
2. If the Authorization Platform does not receive the issuer's Reversal Request Response/0410 message within the time limit, 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 (Issuer Time-out)

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

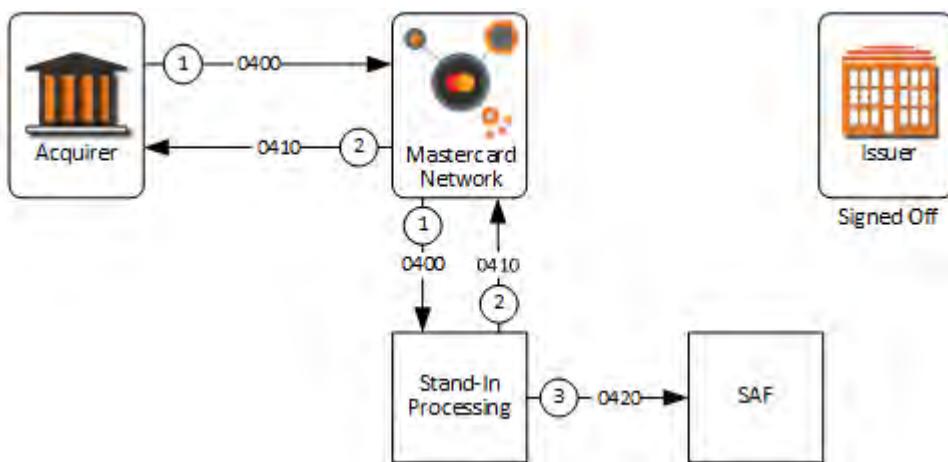
This message flow describes transaction processing when the issuer responds to the Reversal Request/0400 message after the time limit.



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 (Issuer Time-out)
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.

### Reversal Request/0400—Issuer Signed Off

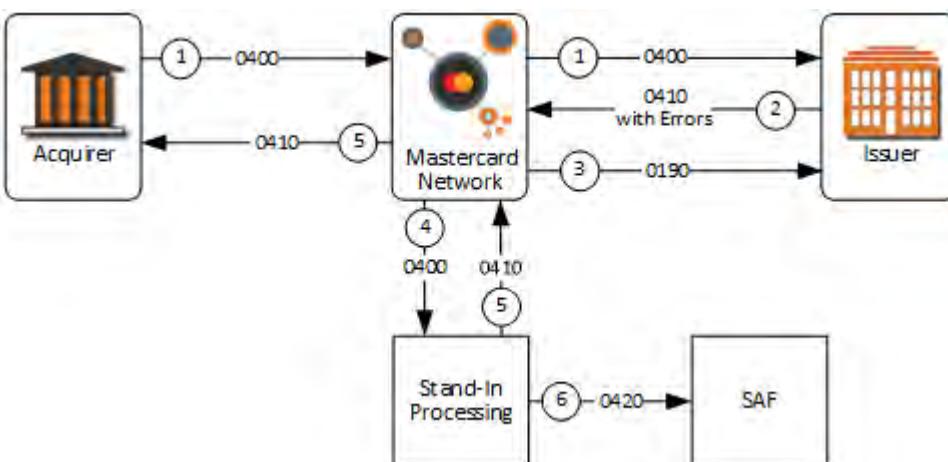
This message flow describes transaction processing when the issuer does not respond to the Reversal Request/0400 message because the issuer is signed off.



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 (Issuer Sign-out)

### Reversal Request/0400—Issuer Response Contains Errors

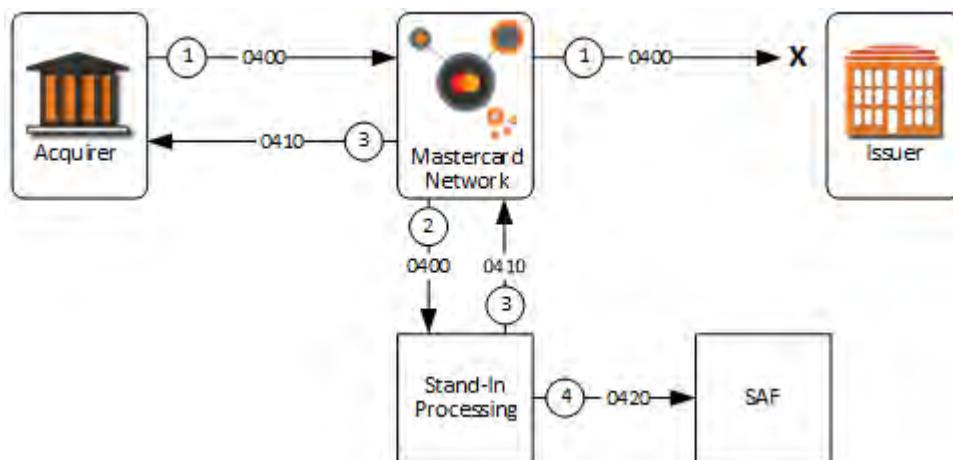
This message flow describes transaction processing when the issuer's response message contains errors.



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 (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.

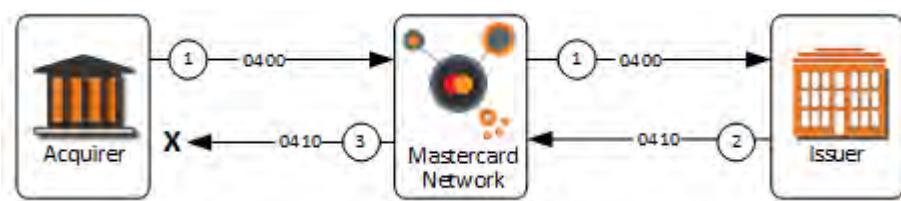


1. The acquirer sends the Reversal Request/0400 message to the Authorization Platform and the Authorization Platform is unable to deliver the Reversal Request/0400 message to the issuer.
2. The Authorization Platform sends the Reversal Request/0400 message to the Stand-In System.
3. The Stand-In System 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 (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.

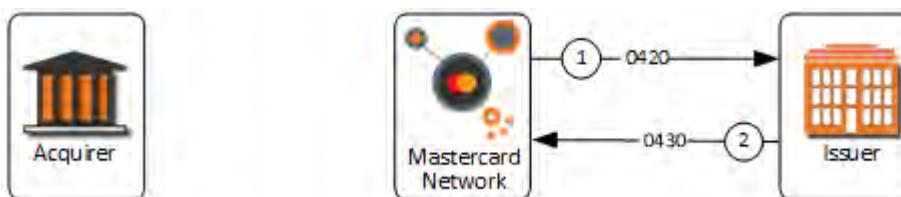


1. The acquirer sends the Reversal Request/0400 message to the Authorization Platform, and then the Authorization Platform forwards the Reversal Request/0400 message to the issuer.
2. The Authorization Platform receives the issuer's Reversal Request Response/0410 message.
3. The Authorization Platform 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

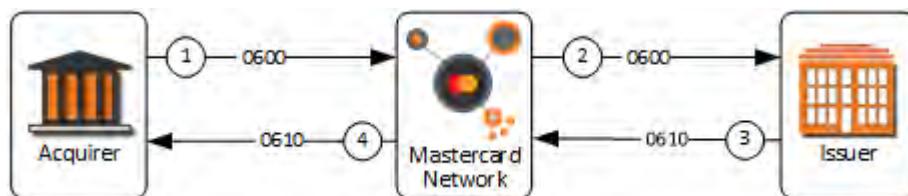
This message flow describes transaction processing of the Reversal Advice/0420 and the Reversal Advice/0430 messages.



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

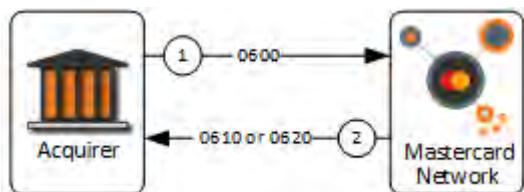
This message flow describes transaction processing of the Administrative Request/0600 and Administrative Request Response/0610 messages.



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 issuer

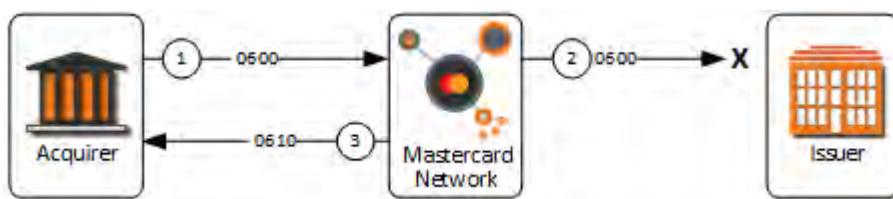
OR

Using the Administrative Advice/0620 message when the Administrative Request/0600 message:

- cannot be parsed
- exceeds the maximum message length of 8k bytes

### Administrative Request/0600, Communication Failure at Issuer

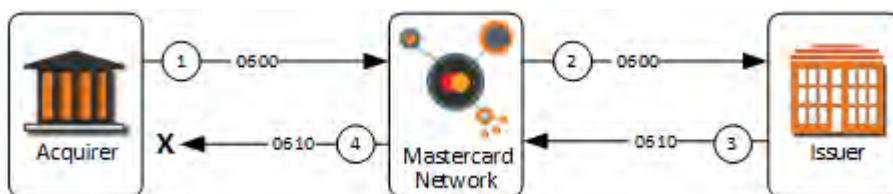
This message flow describes exception processing when communication fails between the issuer and the Authorization Platform during an Administrative Request/0600 message.



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.

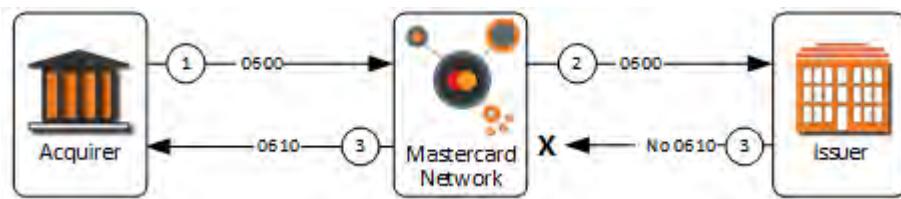


1. The acquirer initiates an Administrative Request/0600 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Administrative Request/0600 message to the issuer based upon the account range contained in DE 2 (Primary Account Number [PAN]).
3. The issuer sends 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

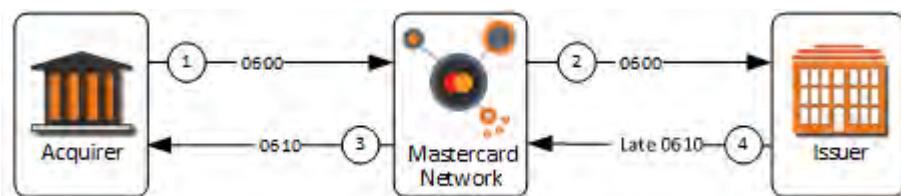
This message flow describes exception processing when there is no response from the issuer to the Authorization Platform for an Administrative Request/0600 message.



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 System 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.

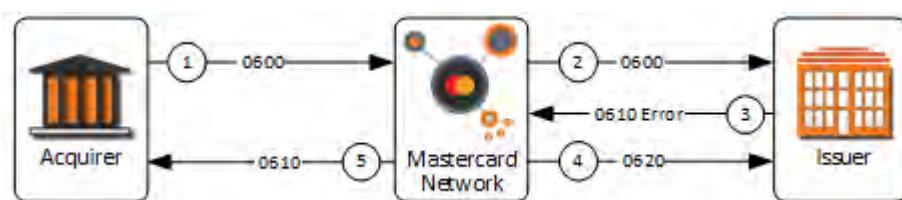


1. The acquirer initiates an Administrative Request/0600 message and sends it to the Authorization Platform.
2. The Authorization Platform forwards the Administrative Request/0600 message to the issuer based upon the account range contained in DE 2 (PAN).
3. If the Authorization Platform receives no 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 System 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

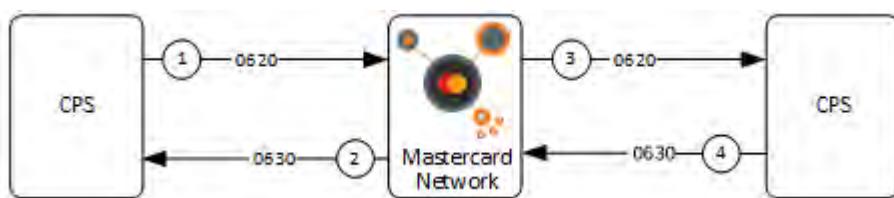
This message flow describes exception processing when the Authorization Platform receives an Administrative Request Response/0610 message that contains an edit failure from the issuer.



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 bytes
  - 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 System or issuer system inoperative).

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

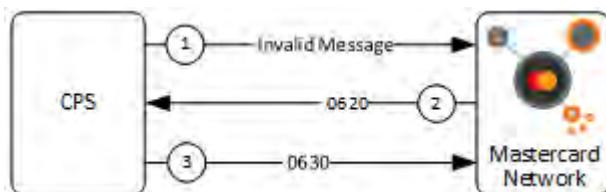
This message flow describes the standard Administrative Advice/06xx message process.



1. A customer processing 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**

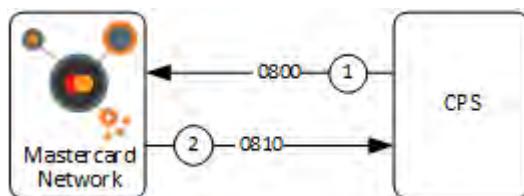
This message flow describes the standard Administrative Advice/06xx invalid message process.



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.

### **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 Network or to sign off from the Mastercard 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.

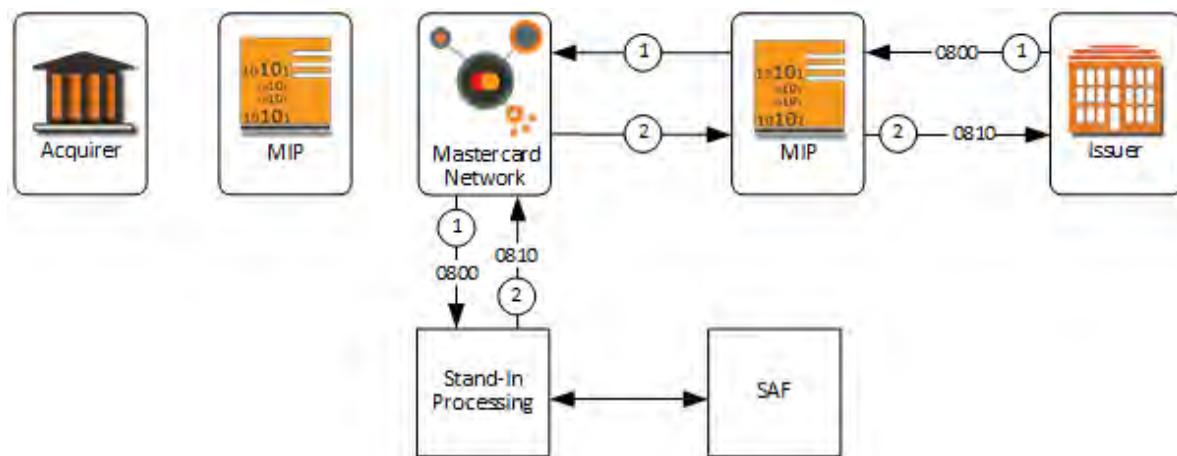
**NOTE:** Customers are reminded that they should use any one or a combination of the network connectivity management options described in the *Authorization Manual*. These varying levels of probes or echo tests are recommended in place of using a sign-on Network Management Request/0800 message to verify host connectivity to Mastercard.

### 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.

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.

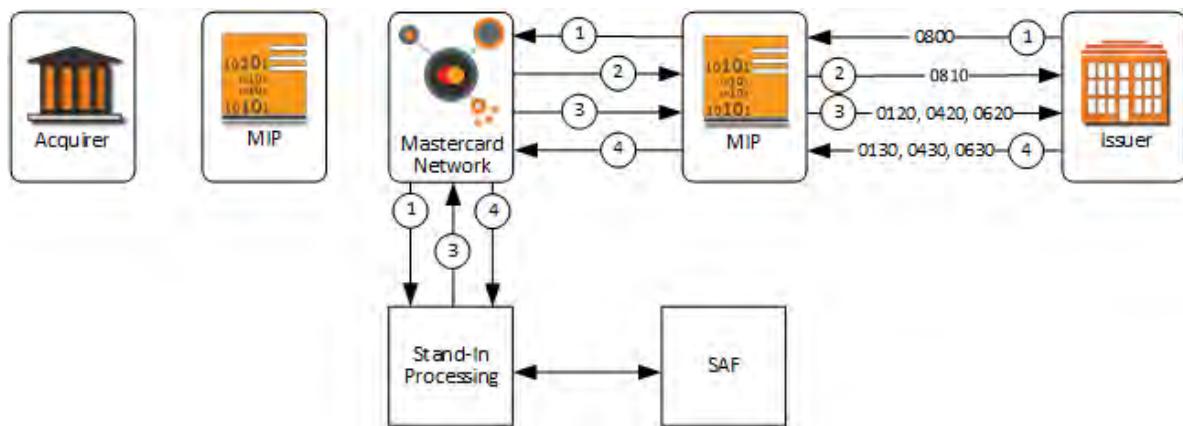
When Mastercard begins to create the bulk file for transmission, it halts the online transmission of SAF records. This halt prevents Mastercard from distributing duplicate SAF records via an online transmission.



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.

### **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 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 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.

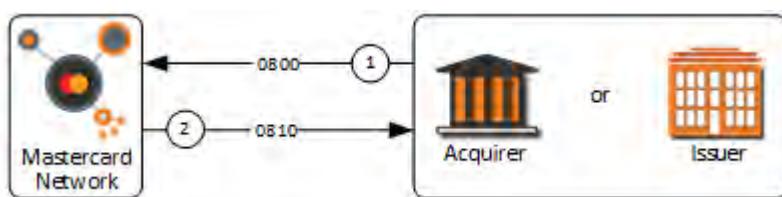
**NOTE: Issuers receive SAF messages intermixed with authorization and reversal request messages.**

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

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

Customers should send the Network Management Request/0800 message with DE 70 (Network Management Information Code) value 270 (Network Connection Status—echo test) when they want to investigate the status of their Mastercard 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.



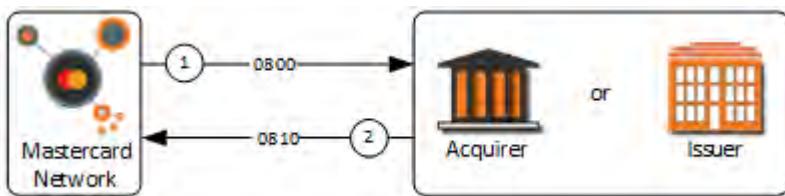
1. The customer sends a Network Management Request/0800—Network Connection Status, Member-generated message where DE 70 is 270 to the Authorization Platform to verify the customer's connection to the Mastercard Network.
2. The Authorization Platform responds with a Network Management Request Response/0810—Network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

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

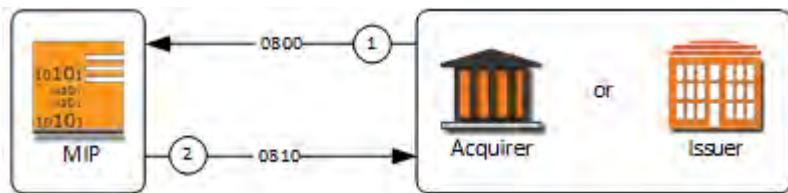
A customer must respond with a Network Management Request Response/0810 message containing DE 70, value 270 to indicate positive acknowledgement of the Network Management Request/0800 message.



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 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.

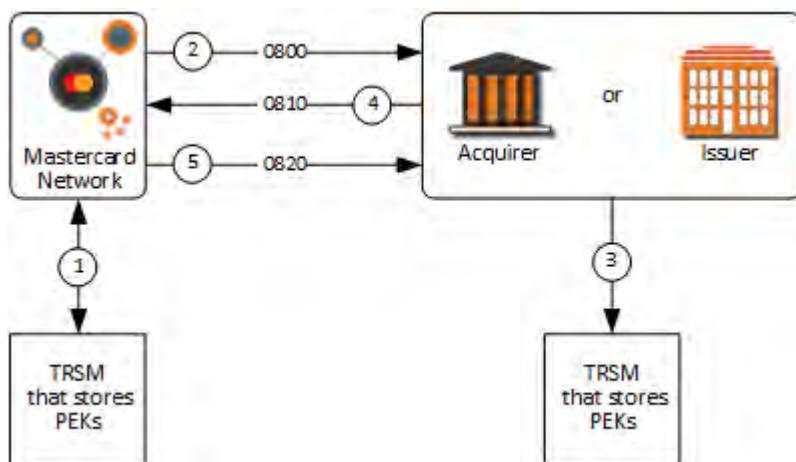


1. The customer sends a Network Management Request/0800—Host Session Activation/Deactivation message where DE 70 (Network Management Information Code) contains either a value of 081 (Host session activation) or 082 (Host session deactivation) to identify session activation or session deactivation to 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 Encryption Key (PEK) service is not available for use by customers in the Europe region that use Mastercard Network PIN Processing services. The Dynamic PIN Encryption Key service is available to customers outside the Europe region that use Single Message System PIN Processing services.**

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

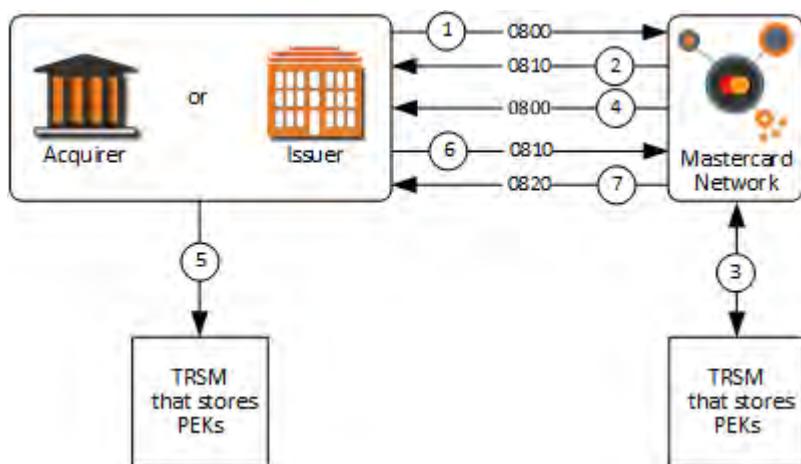
This message flow describes transaction processing as it exchanges new PEKs with the customer every 24 hours.



1. The pre-determined time 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 or DE 110 and the customer ID in DE 2 (Primary Account Number [PAN]).
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.
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 or to advise of the failure. If the Network Management Advice/0820—PEK Exchange message indicated that the PEK is active and operational, then 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. Customers 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 or DE 110 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.
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 or advising of the failure. If the Network Management Advice/0820—PEK Exchange message indicated that the PEK is active and operational, then 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.....	139
Authorization Request Response/0110.....	143
Authorization Advice/0120—Acquirer-Generated.....	147
Authorization Advice/0120—Issuer-Generated.....	151
Authorization Advice/0120—System-Generated.....	154
Authorization Advice Response/0130—Issuer-Generated (Responding to a System-Generated 0120 from SAF).....	158
Authorization Advice Response/0130—Issuer-Generated (Responding to an Acquirer-Generated 0120 Response or an Authorization Advice Request 0120).....	160
Authorization Advice Response/0130—System-Generated (Responding to an Acquirer-Generated 0120).....	163
Authorization Advice Response/0130—System-Generated (Responding to an Issuer-Generated 0120).....	165
Authorization Response Acknowledgement/0180.....	167
Authorization Response Negative Acknowledgement/0190.....	167
Issuer File Update Request/0302.....	168
Issuer File Update Request Response/0312.....	169
Reversal Request/0400.....	171
Reversal Request Response/0410.....	176
Reversal Advice/0420.....	179
Reversal Advice Response/0430.....	183
Administrative Request/0600.....	185
Administrative Request Response/0610.....	186
Administrative Advice/0620—System-Generated.....	188
Administrative Advice/0620—Member-Generated.....	189
Administrative Advice Response/0630.....	190
Network Management Request/0800—Sign-On/Sign-Off.....	191
Network Management Request/0800—Network Connection Status, Member-Generated.....	193
Network Management Request/0800—Network Connection Status, System-Generated.....	193
Network Management Request/0800—Host Session Activation/Deactivation.....	194
Network Management Request/0800—PEK Exchange.....	195
Network Management Request/0800—PEK Exchange On Demand.....	196
Network Management Request Response/0810—Sign-On/Sign-Off.....	197

Network Management Request Response/0810—Network Connection Status, Member-Generated.....	198
Network Management Request Response/0810—Network Connection Status, System-Generated.....	199
Network Management Request Response/0810—Host Session Activation/Deactivation .....	200
Network Management Request Response/0810—PEK Exchange.....	200
Network Management Request Response/0810—PEK Exchange-On Demand.....	201
Network Management Advice/0820—PEK Exchange.....	202

## 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 transaction 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	

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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 and if DE 42 does not uniquely identify the terminal.
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).
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.

---

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
56 Payment Account Data	•	X	C	When Mastercard is the BIN Controller (as defined by EMVCo) DE 56 will be present and contain the PAR value when one is associated with the PAN.
61 Point-of-Service (POS) Data	M	•	M	
62 Intermediate Network Facility (INF) Data	O	•	O	
63 Network Data	•	X	M	
108 MoneySend Reference Data	C	•	C	Mandatory for originating institution to submit DE 108 on all Mastercard® MoneySend™ Payment Transactions. Optional for originating institution to submit DE 108 on all MoneySend Funding Transactions.
				Mandatory for originating institution to submit DE 108 on all Mastercard™ Merchant Presented QR Payment and Funding Transactions. Optional on Mastercard Merchant Presented QR Refund Payment Transactions.
112 Additional Data (National Use)	C	•	C	Contains applicable subelement data.
120 Record Data	C	X	C	
124 Member-defined Data	C	•	C	Must contain customer-defined data; required for Mastercard MoneySend Payment 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>4</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>4</sup>
7 Transmission Date and Time	ME	•	ME	Must be the same value as in the original Authorization Request/0100.

<sup>4</sup> 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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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>4</sup>
10 Conversion Rate, Cardholder Billing	C	•	C	Must be the same value as in the original Authorization Request/0100. <sup>4</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>4</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 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. Refer to the data element details for list of values by message type. <sup>5</sup>

---

<sup>5</sup> 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).

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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>4</sup>
51 Currency Code, Cardholder Billing	C	•	C	Must be the same value as in the original Authorization Request/0100. <sup>4</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.
56 Payment Account Data	C	X	C	When Mastercard is the BIN Controller (as defined by EMVCo), the issuer is not required to provide DE 56 in the response message. If a PAR value is associated with the PAN, Mastercard will insert DE 56 containing the PAR value in the response message before forwarding the message to the acquirer. When the issuer is the BIN Controller and has associated a PAR value with the PAN, the issuer must include DE 56 containing the PAR value in the response message.
62 Intermediate Network Facility (INF) Data	CE	•	CE	Must be the same value as in the original Authorization Request/0100 message, if present.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
108 MoneySend Reference Data	C	•	C	Mandatory for originating institution to submit DE 108 on all MoneySend Payment Transactions, optional for originating institution to submit DE 108 on all MoneySend Funding Transactions.
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: Applicable only to Swedish Domestic Authorization Switching Service (SASS) or Peru domestic POS transactions.</b>				
124 Member-defined Data	C	•	C	May contain issuer-defined data; required for Mastercard MoneySend Payment Transactions.
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 (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 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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.
28 Amount, Transaction Fee	C	•	C	Contains an online transaction fee as permitted by the operating rules of a bank card product.
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.

---

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
38 Authorization ID Response	C	•	C	Must be either the same value as in the original Authorization Request Response/0110, if present, or a value provided by the acquirer if the acquirer or merchant processed and approved the transaction. 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.
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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
56 Payment Account Data	•	X	C	When Mastercard is the BIN Controller, the PAR value is inserted when available.
60 Advice Reason Code	M	•	M	DE 60, subfield 1 (Advice Reason Code) must contain the value 190 (APS approved), value 191 (Acquirer Processing System [APS] Completed Authorization Transaction), or value 192 (M/Chip Offline Advice to Issuer).
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.
112 Additional Data (National Use)	C	•	C	Contains applicable subelement data.
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, if present.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
124 Member-defined Data	C	•	C	May contain acquirer-defined data; required for Mastercard MoneySend Payment Transactions.
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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.

---

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.
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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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 customer-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.

## 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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.

---

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.

---

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.
56 Payment Account Data	•	X	C	When Mastercard is the BIN Controller, the PAR value is inserted when available.
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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
108 MoneySend Reference Data	•	C	C	Must be the same value as in the original Authorization Request/0100, if present.  Optional for Mastercard Merchant Presented QR Transactions.
112 Additional Data (National Use)	•	C	C	Contains applicable subelement data.
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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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 Authorization Advice/0120 message, if present.
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.

Data Element ID and Name	Org	Sys	Dst	Comments
56 Payment Account Data	C	X	C	When Mastercard is the BIN Controller, issuers are not required to send PAR. Mastercard will insert the PAR in the message before sending to the acquirer, when available.
				When Mastercard is not the BIN Controller, the issuer may provide the PAR in the response message when available. Mastercard will pass this value to the acquirer.
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 Response or an Authorization Advice Request 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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.
28 Amount, Transaction Fee	CE	CE	•	Must be the same value as in the Authorization Advice/0120 message, 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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
37 Retrieval Reference Number	CE	•	CE	Must be the same value as in the Authorization Advice/0120—Acquirer-generated, if present.
39 Response Code	ME	•	ME	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.
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.
56 Payment Account Data	C	X	C	<p>When Mastercard is the BIN Controller, issuers are not required to send PAR. Mastercard will insert the PAR in the message before sending to the acquirer, when available.</p> <p>When Mastercard is not the BIN Controller, the issuer may provide the PAR in the response message when available. Mastercard will pass this value to the acquirer.</p>
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.

Data Element ID and Name	Org	Sys	Dst	Comments
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.

## Authorization Advice Response/0130—System-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, 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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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 Authorization Advice/0120 message, if present.
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.
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.
56 Payment Account Data	C	C	•	When Mastercard is the BIN Controller, the PAR value is inserted when available.
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—System-Generated (Responding to an Issuer-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—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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
15 Date, Settlement	•	ME	ME	Must be the same value as in the Authorization Advice/0120—Issuer-generated.
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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.

## Authorization Response Acknowledgement/0180

---

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—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	

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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 of this manual.
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.

## Issuer File Update Request/0302

---

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—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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
56 Payment Account Data	O	•	C	DE 56 is optional when DE 101 (File Name) is MCC111 (PAN-PAR Mapping File).
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	O	•	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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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	•	CE	CE	Must be the same value as in the original Issuer File Update Request/0302, if present.

---

## 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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
7 Transmission Date and Time	M	•	M	Transaction time stamp; UTC date and time that this transaction was entered into interchange.
9 Conversion Rate, 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.
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.

<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	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.
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, 34, 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.

<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	<p>Must contain the transaction category code (TCC) from the original Authorization Request/0100.</p> <p>Subelement 63 (Trace ID) must be present. Subelement 58 (ATM Additional Data) and subelement 77 (Funding/Payment Transaction Type Indicator) may be present based on the usage condition defined for each of these subelements in the Data Element Definitions.</p> <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>
				<p><b>NOTE: 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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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. If the original authorization was a Purchase with Cash Back request (subfield 2 value 40) and the cash back portion of the request was not approved by the issuer (Response Code 87 (Purchase Only Approval)), DE 54 should not be included in the reversal request.
56 Payment Account Data	•	X	C	When Mastercard is the BIN Controller, the PAR value is inserted when available.
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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
108 MoneySend Reference Data	C	•	C	Mandatory for originating institution to submit DE 108 on all MoneySend Payment Transactions. Optional for originating institution to submit DE 108 on all MoneySend Funding Transactions.  Optional for Mastercard Merchant Presented QR Transactions.
112 Additional Data (National Use)	C	•	C	Contains applicable subelement data.
124 Member-defined Data	C	•	C	Member-defined data element, available for message initiator and recipient optional use; required for Mastercard MoneySend Payment Transactions.
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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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>6</sup>
6 Amount, Cardholder Billing	CE	X	C	Must be the same value as in the original Reversal Request/0400 message. <sup>6</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>6</sup>
10 Conversion Rate, Cardholder Billing	CE	X	C	Must be the same value as in the original Reversal Request/0400 message. <sup>6</sup>
11 Systems Trace Audit Number	ME	•	ME	Must be the same value as in the original Reversal Request/0400 message.
15 Date, Settlement	ME	•	M	Must be the same value as in the original Reversal Request/0400 message.
16 Date, Conversion	CE	X	C	Must be the same value as in the original Reversal Request/0400 message. <sup>6</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.

<sup>6</sup> This data will be present, as defined, except when the Authorization Platform has declined a Reversal Request/0400 message and was unable to complete currency conversion processing.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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>6</sup>
51 Currency Code, Cardholder Billing	CE	X	C	Must be the same value as in the original Reversal Request/0400 message. <sup>6</sup>
56 Payment Account Data	C	X	C	When Mastercard is the BIN Controller, issuers are not required to send PAR. Mastercard will insert the PAR in the message before sending to the acquirer, when available.  When Mastercard is not the BIN Controller, the issuer may provide the PAR in the response message when available. Mastercard will pass this value to the acquirer.
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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
108 MoneySend Reference Data	C	•	C	Mandatory for originating institution to submit DE 108 on all MoneySend Payment Transactions, optional for originating institution to submit DE 108 on all MoneySend Funding Transactions.  If DE 108 is submitted but the acquirer is not ready to receive, the transaction may fail on the acquirer side.
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 customer-defined data; required for MoneySend Payment Transactions.
127 Private Data	O	X	CE	Private data for message initiator's use.

## 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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.

<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	<p>Must contain the transaction category code (TCC) from the original Authorization Request/0100 or Reversal Request/0400 message. The following subelements may be present in the Reversal Advice if they were present in the original Authorization Request/0100:</p> <ul style="list-style-type: none"> <li>• 20 (Cardholder Verification Method)</li> <li>• 33 (PAN Mapping File Information)</li> <li>• 38 (Account Category)</li> <li>• 58 (ATM Additional Data)</li> <li>• 63 (Trace ID)</li> <li>• 71 (On-behalf Services)</li> <li>• 77 (Funding/Payment Transaction Type Indicator)</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>• 95 (Mastercard Promotion Code)</li> <li>• 96 (Visa Market-Specific Data Identifier [Visa Only])</li> </ul>
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.
56 Payment Account Data	•	X	C	When Mastercard is the BIN Controller, the PAR value is inserted when available.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.

---

## Reversal Advice Response/0430

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—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.

---

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
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.

---

---

<b>Data Element ID and Name</b>		<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
56	Payment Account Data	O	•	•	Issuers may optionally provide DE 56.
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.

---

## 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

---

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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	M	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.
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.

---

## Administrative Request Response/0610

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

---

<b>Date Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- Message Type Identifier (MTI)	M	•	M	Constant—0610 (Administrative Request Response).

---

---

<b>Date Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
- 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.
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.

---

<b>Date Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
127 Private Data	•	X	CE	May contain message initiator information.

## 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.
42 Card Acceptor ID Code	•	M	M	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.
48 Additional Data—Private Use	•	C	C	If DE 60 = 600, DE 48 will not be present in the message.
56 Payment Account Data	•	X	C	When Mastercard is the BIN Controller (as defined by EMVCo) DE 56 will be present and contain the PAR value when one is associated with the PAN. DE 56 is only present when DE 60 = 0251.
60 Advice Reason Code	•	M	M	Indicates specific type of message.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.
120 Record Data	•	C	C	If DE 60 = 600, contains rejected message.  DE 120 will also be present if DE 60 = 0250, 0251, or 0252.
127 Private Data	•	O	O	Private use data element, available for optional use by message initiator.

---

## Administrative Advice/0620—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—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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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	•	X	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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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	O	X	•	Private use data element, available for optional use by message initiator.

---

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

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 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.

---

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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 the details for this data element in the Data Element Definitions chapter of this manual.
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.

---

## **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.

## **Network Management Request/0800—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—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 the DE 70 data element definition 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.

<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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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 the DE 70 data element definition for a list of applicable values by message type.

---

## Network Management Request/0800—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—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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
33 Forwarding Institution ID Code	•	M	M	Constant—002202; identifies the Authorization Platform.
48 Additional Data—Private Use	•	O	C	Key Exchange Data Block for variant 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
110 Additional Data-2	•	O	C	Key Exchange Data Block for TR-31 Key Block key change function; the KEK is used to encrypt the PEK.

## **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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
63 Network Data	•	X	•	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: <ul style="list-style-type: none"><li>• 162 = Solicitation for key exchange request</li><li>• 163 = Solicitation for Encryption Key Exchange - TR-31 Keyblock</li></ul>
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.

---

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

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—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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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—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—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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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.

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

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.
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.
110 Additional Data—2	O	M	•	Must be the same value as in the original Network Management Request/0800.

## **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).

---

<b>Data Element ID and Name</b>		<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
-	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—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.

---

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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: <ul style="list-style-type: none"> <li>• 161 = Encryption key exchange request</li> <li>• 164 = Encryption TR-31 Block Key Exchange Confirmation of Success</li> <li>• 165 = Encryption TR-31 Block Key Exchange Advice of Failure</li> </ul>
110 Additional Data—2	•	M	M	Echoes the Key Check Value (DE 110, subelement 10) from the Network Management Request/0800—PEK Exchange message.

---

## 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.....	223
Subelement Layout.....	223
Subfield Layout.....	224
Position Layout.....	224
List of Data Elements (Numeric Order).....	224
List of Data Elements (Alphabetic Order).....	229
Message Type Identifier.....	233
Message Types and Applicable Program or Service.....	236
About Primary and Secondary Bit Maps.....	237
Primary Bit Map.....	237
DE 1—Bit Map, Secondary.....	239
DE 2—Primary Account Number (PAN).....	241
About Primary Account Number.....	243
DE 3—Processing Code.....	244
Subfield 1—Cardholder Transaction Type Code.....	246
Subfield 2—Cardholder "From Account" Type Code.....	248
Subfield 3—Cardholder "To Account" Type Code.....	249
DE 4—Amount, Transaction.....	250
DE 5—Amount, Settlement.....	254
DE 6—Amount, Cardholder Billing.....	255
DE 7—Transmission Date and Time.....	257
Subfield 1—Date.....	259
Subfield 2—Time.....	260
DE 8—Amount, Cardholder Billing Fee.....	260
DE 9—Conversion Rate, Settlement.....	260
Subfield 1—Decimal Indicator.....	262
Subfield 2—Conversion Rate.....	262
DE 10—Conversion Rate, Cardholder Billing.....	263
Subfield 1—Decimal Indicator.....	264
Subfield 2—Cardholder Billing Conversion Rate.....	264
DE 11—System Trace Audit Number (STAN).....	265
DE 12—Time, Local Transaction.....	267
DE 13—Date, Local Transaction.....	268

---

DE 14—Date, Expiration.....	269
DE 15—Date, Settlement.....	270
DE 16—Date, Conversion.....	271
DE 17—Date, Capture.....	272
DE 18—Merchant Type.....	273
DE 19—Acquiring Institution Country Code.....	274
DE 20—Primary Account Number (PAN) Country Code.....	275
DE 21—Forwarding Institution Country Code.....	276
DE 22—Point-of-Service (POS) Entry Mode.....	276
Subfield 1—POS Terminal PAN Entry Mode.....	278
Subfield 2—POS Terminal PIN Entry Mode.....	279
Authorization Platform Edits.....	280
Mastercard Electronic Card Transactions.....	280
Mastercard Consumer Presented QR Transactions.....	280
Chip Transactions.....	281
Magnetic Stripe or Chip-Read Transactions for Mastercard Electronic Card.....	283
Contactless Magnetic Stripe Transactions.....	284
Credential on File Transactions.....	285
DE 23—Card Sequence Number.....	285
DE 24—Network International ID.....	287
DE 25—Point-of-Service (POS) Condition Code.....	288
DE 26—Point-of-Service (POS) Personal ID Number (PIN) Capture Code.....	288
DE 27—Authorization ID Response Length.....	289
DE 28—Amount, Transaction Fee.....	290
Subfield 1—Debit/Credit Indicator.....	291
Subfield 2—Amount.....	292
DE 29—Amount, Settlement Fee.....	292
Subfield 1—Debit/Credit Indicator.....	293
Subfield 2—Amount.....	293
DE 30—Amount, Transaction Processing Fee.....	293
Subfield 1—Debit/Credit Indicator.....	294
Subfield 2—Amount.....	294
DE 31—Amount, Settlement Processing Fee.....	294
Subfield 1—Debit/Credit Indicator.....	295
Subfield 2—Amount.....	295
DE 32—Acquiring Institution ID Code.....	296
DE 33—Forwarding Institution ID Code.....	297
DE 34—Primary Account Number (PAN), Extended.....	299
DE 35—Track 2 Data.....	300

---

DE 36—Track 3 Data.....	301
DE 37—Retrieval Reference Number.....	302
Subfield 1—Transaction Date and Initiator Discretionary Data.....	304
Subfield 2—Terminal Transaction Number.....	304
DE 38—Authorization ID Response.....	304
DE 39—Response Code.....	306
Authorization Request Response/0110 Response Codes.....	309
Authorization Advice/0120 Response Codes.....	311
Authorization Advice Response/0130 Response Codes.....	313
Authorization Advice Response/0180 Response Codes.....	314
Authorization Negative Acknowledgement/0190 Response Codes.....	314
Issuer File Update Request Response/0312 Response Codes.....	314
Reversal Request/0400 Message Response Codes.....	315
Reversal Request Response/0410 Response Codes.....	317
Reversal Advice/0420 Response Codes.....	318
Reversal Advice Response/0430 Message and Administrative Advice Response/0630 Response Codes.....	320
Administrative Request Response/0610 Response Codes.....	320
Network Management Request Response/0810 Response Codes.....	321
DE 40—Service Restriction Code.....	321
DE 41—Card Acceptor Terminal ID.....	322
DE 42—Card Acceptor ID Code.....	323
DE 43—Card Acceptor Name/Location for All Transactions.....	324
Subfield 1—Card Acceptor Name (or Payment Facilitator & Sub-Merchant Information, if applicable).....	325
Subfield 2—Space.....	327
Subfield 3—Card Acceptor City (or Sub-Merchant Information, if applicable).....	327
Subfield 4—Space.....	327
Subfield 5—Card Acceptor State or Country Code (or Sub-Merchant Information, if applicable).....	328
DE 43—Card Acceptor Name/Location for ATM Transactions.....	328
Subfield 1—ATM Owning Institution or Terminal/Merchant Address or Both.....	329
Subfield 2—Space.....	329
Subfield 3—ATM or Merchant Location City.....	330
Subfield 4—Space.....	330
Subfield 5—ATM or Merchant State, Province, or Country Code Location.....	330
DE 43—Card Acceptor Name/Location for Bankcard-Activated Public Phones.....	331
Subfield 1—Abbreviation "TEL" .....	332
Subfield 2—Phone Number Dialed.....	332

---

Subfield 3—Abbreviation "M".....	333
Subfield 4—Call Duration.....	333
Subfield 5—Space.....	333
Subfield 6—Call Origin City.....	334
Subfield 7—Space.....	334
Subfield 8—Call Origin State or Country Code.....	334
DE 44—Additional Response Data.....	335
DE 44 Values by Program or Service.....	336
Authorization Platform Edits.....	338
DE 45—Track 1 Data.....	339
DE 46—Expanded Additional Amounts.....	340
DE 47—Additional Data—National Use.....	341
DE 48—Additional Data—Private Use.....	341
DE 48 Transaction Category Code.....	343
DE 48 Subelement Encoding Scheme in Authorization Request/0100 Messages.....	344
DE 48 Subelement Encoding Scheme in Network Management Messages.....	345
List of DE 48 Subelements.....	345
Subelement 10—Encrypted PIN Block Key.....	349
Subelement 11—Key Exchange Block Data (Double-Length Keys).....	349
Subelement 11—Key Exchange Block Data (Triple-Length Keys).....	350
Subelement 12—Routing Indicator.....	352
Subelement 13—Mastercard Hosted Mobile Phone Top-Up Request Data.....	352
Subfield 1—Mobile Phone Number.....	353
Subfield 2—Mobile Phone Service Provider Name.....	353
Subelement 14—Account Type Indicator.....	353
Subelement 15—Authorization System Advice Date and Time.....	354
Subfield 1—Date.....	355
Subfield 2—Time.....	355
Subelement 16—Processor Pseudo ICA.....	356
Subelement 17—Authentication Indicator.....	356
Subelement 18—Service Parameters.....	357
Subfield 01—Canada Domestic Indicator.....	358
Subelement 20—Cardholder Verification Method.....	359
Subelement 21—Acceptance Data.....	359
Subfield 01—mPOS Acceptance Device Type.....	360
Subfield 02—Additional Terminal Capability Indicator.....	361
Subelement 23—Payment Initiation Channel.....	362
Subfield 1—Device Type.....	363
Subelement 25—Mastercard Cash Program Data.....	365

---

Subfield 01—Message Identifier.....	366
Subelement 26—Wallet Program Data.....	366
Subfield 1—Wallet Identifier.....	367
Subelement 27—Transaction Analysis.....	368
Subfield 1—Overview.....	369
Subfield 2—Test Results.....	370
Subelement 28—Cardless ATM Order ID.....	371
Subelement 29—Additional POS Terminal Locations.....	372
Subelement 30—Token Transaction Identifier.....	372
Subelement 32—Mastercard Assigned ID.....	373
Subelement 33—PAN Mapping File Information.....	374
Subfield 1—Account Number Indicator.....	375
Subfield 2—Account Number.....	376
Subfield 3—Expiration Date.....	376
Subfield 4—Product Code.....	377
Subfield 5—Token Assurance Level.....	377
Subfield 6—Token Requestor ID.....	378
Subfield 7—Primary Account Number, Account Range.....	379
Subfield 8—Storage Technology.....	379
Subelement 34—ATC Information.....	380
Subfield 1—ATC Value.....	381
Subfield 2—ATC Discrepancy Value.....	382
Subfield 3—ATC Discrepancy Indicator.....	382
Subelement 34 Subfield Data Examples.....	382
Subelement 35—Contactless Non-Card Form Factor Request/Response.....	383
Subelement 36—Visa MVV (Visa Only).....	384
Subfield 1—Merchant Verification Value (MVV).....	385
Subelement 37—Additional Merchant Data.....	385
Subfield 1—Payment Facilitator ID.....	386
Subfield 2—Independent Sales Organization ID.....	387
Subfield 3—Sub-Merchant ID.....	387
Subelement 38—Account Category.....	388
Subelement 39—Account Data Compromise Information.....	389
Subelement 40—Electronic Commerce Merchant/Cardholder Certificate Serial Number (Visa Only).....	391
Subfield 1—Merchant Certificate Serial Number.....	392
Subfield 2—Cardholder Certificate Serial Number.....	392
Subelement 41—Electronic Commerce Certificate Qualifying Information.....	392
Subfield 1—Reserved for Future Use.....	393

---

Subfield 2—Reserved for Future Use.....	393
Subfield 3—Reserved for Future Use.....	393
Subfield 4—Reserved for Future Use.....	394
Subfield 5—Reserved for Future Use.....	394
Subfield 6—Reserved for Future Use.....	394
Subfield 7—Reserved for Future Use.....	394
Subfield 8—Reserved for Future Use.....	395
Subfield 9—Reserved for Future Use.....	395
Subfield 10—Reserved for Future Use.....	395
Subfield 11—Citizen ID.....	395
Subfield 12—Reserved for Future Use.....	396
Subfield 13—Reserved for Future Use.....	396
Subfield 14—Reserved for Future Use.....	396
Subfield 15—Reserved for Future Use.....	396
Subfield 16—Reserved for Future Use.....	397
Subfield 17—Reserved for Future Use.....	397
Subfield 18—Reserved for Future Use.....	397
Subelement 42—Electronic Commerce Indicators.....	397
Subfield 1—Electronic Commerce Security Level Indicator and UCAF Collection Indicator...	399
Subfield 2—Original Electronic Commerce Security Level Indicator and UCAF Collection Indicator.....	402
Subfield 3—Reason for UCAF Collection Indicator Downgrade.....	403
Subelement 43—Universal Cardholder Authentication Field (UCAF).....	404
Subelement 43—3-D Secure for Mastercard <i>SecureCode</i> .....	405
Subelement 43—Digital Secure Remote Payment Universal Cardholder Authentication Field (UCAF).....	406
Subelement 43—Static AAV.....	407
Subelement 43—3-D Secure Electronic Commerce Verification Service (Visa, JCB, Diners Club and American Express Only).....	408
Subelement 44—3-D Secure Electronic Commerce Transaction Identifier (XID) (Visa and American Express).....	409
Subelement 45—3-D Secure Electronic Commerce Transaction Response Code (Visa and American Express).....	410
Subelement 46—Product ID (Visa Only).....	410
Subelement 47—Mastercard Payment Gateway Transaction Indicator.....	411
Subelement 48—Mobile Program Indicators.....	412
Subfield 1—Remote Payments Program Type Identifier.....	413
Subfield 2—Mastercard Mobile Remote Payment Transaction Type.....	413
Subfield 3—Mobile Phone Number.....	414

---

Subfield 4—Convenience Fee.....	414
Subelement 49—Time Validation Information.....	415
Subfield 1—Time Value.....	415
Subfield 2—Time Discrepancy Value.....	415
Subfield 3—Time Discrepancy Indicator.....	416
Subelement 51—Merchant On-behalf Services.....	416
Subfield 1—Merchant On-behalf (OB) Service.....	417
Subfield 2—Merchant On-behalf (OB) Result 1.....	417
Subelement 51—Valid Subfield 1 and Subfield 2 Value Combinations.....	418
Subfield 3—Additional Information.....	419
Subelement 52—Transaction Integrity Class.....	420
Subelement 53—E-ID Request Code.....	421
Subfield 1—E-ID Request Value.....	422
Subelement 55—Merchant Fraud Scoring Data.....	423
Subfield 1—Merchant Fraud Score.....	424
Subfield 2—Merchant Score Reason Code.....	424
Subfield 3—Reserved for Future Use.....	424
Subfield 4—Reserved for Future Use.....	425
Subfield 5—Reserved for Future Use.....	425
Subelement 56—Security Services Additional Data for Issuers.....	425
Subfield 1—Security Services Indicator.....	427
Subfield 2—Security Services Data.....	427
Subelement 56—Valid Subfield 1 and Subfield 2 Value Combinations.....	427
Subelement 57—Security Services Additional Data for Acquirers.....	433
Subfield 1—Security Services Indicator.....	434
Subfield 2—Security Services Data.....	434
Subelement 58—ATM Additional Data.....	434
Subfield 1—ATM Time.....	435
Subfield 2—ATM Date.....	435
Subfield 3—Watermark.....	436
Subfield 4—Mark 1.....	436
Subfield 5—Mark 2.....	436
Subfield 6—Mark 3.....	437
Subfield 7—Card Swallowed Status.....	437
Subfield 8—Posting Date.....	438
Subelement 61—POS Data Extended Condition Codes.....	438
Subfield 1—Partial Approval Terminal Support Indicator.....	439
Subfield 2—Purchase Amount Only Terminal Support Indicator.....	439
Subfield 3—Real-time Substantiation Indicator.....	439

---

Subfield 4—Merchant Transaction Fraud Scoring Indicator.....	440
Subfield 5—Final Authorization Indicator.....	441
Subelement 63—Trace ID.....	442
Subelement 64—Transit Program.....	444
Subfield 1—Transit Transaction Type Indicator.....	445
Subfield 2—Transportation Mode Indicator.....	445
Subelement 65—Terminal Compliant Indicator.....	446
Subfield 1—TLE Compliant.....	447
Subfield 2—UKPT/DUKPT Compliant.....	447
Subelement 66—Authentication Data.....	448
Subfield 1—Program Protocol.....	449
Subfield 2—Directory Server Transaction ID.....	449
Subelement 67—MoneySend Information.....	450
Subfield 1—Sanction Screening Score.....	451
Subelement 71—On-behalf Services.....	451
Subfield 1—On-behalf (OB) Service.....	452
Subfield 2—On-behalf Result 1.....	452
Subfield 3—On-behalf Result 2.....	453
Subelement 71—Valid Subfield 1 and Subfield 2 Value Combinations.....	453
Subelement 72—Issuer Chip Authentication.....	463
Subelement 74—Additional Processing Information.....	464
Subfield 1—Processing Indicator.....	465
Subfield 2—Processing Information.....	465
Valid Subfield 1 and Subfield 2 Value Combinations.....	466
Subelement 75—Fraud Scoring Data.....	466
Subfield 1—Fraud Score.....	468
Subfield 2—Score Reason Code.....	468
Subfield 3—Rules Score.....	469
Subfield 4—Rules Reason Code 1.....	469
Subfield 5—Rules Reason Code 2.....	470
Subelement 76—Mastercard Electronic Acceptance Indicator.....	471
Subelement 77—Funding/Payment Transaction Type Indicator.....	472
Subelement 78—Payment Service Indicators (Visa Only).....	474
Subfield 1—Spend Qualified Indicator.....	475
Subfield 2—Dynamic Currency Conversion Indicator.....	475
Subfield 3—U.S. Deferred Billing Indicator.....	476
Subfield 4—Visa Checkout Indicator.....	477
Subfield 5—Message Reason Code.....	477
Subfield 6—Reserved for Future Use.....	478

---

Subelement 79—Chip CVR/TVR Bit Error Results.....	478
Subfield 1—CVR or TVR Identifier.....	480
Subfield 2—Byte ID.....	480
Subfield 3—Byte Identifier.....	480
Subfield 4—Value of Bit in Error.....	481
Subelement 80—PIN Service Code.....	481
Subelement 82—Address Verification Service Request.....	482
Subelement 83—Address Verification Service Response.....	483
Subelement 84—Merchant Advice Code.....	485
Subelement 84—Visa Response Codes (Visa Only).....	486
Subelement 85—Account Status (Visa Only).....	486
Subelement 86—Relationship Participant Indicator (Visa Only).....	487
Subelement 87—Card Validation Code Result.....	488
Subelement 87—CVV2 Response (Visa Only).....	489
Subelement 88—Magnetic Stripe Compliance Status Indicator.....	490
Subelement 89—Magnetic Stripe Compliance Error Indicator.....	490
Subelement 90—Lodging and Auto Rental Indicator.....	491
Subelement 90—Custom Payment Service Request (Visa Only).....	492
Subelement 90—Custom Payment Service Request Response (Visa Only).....	493
Subelement 91—Acquirer Reference Data (American Express Only).....	494
Subelement 91—Custom Payment Service Request/Transaction ID (Visa Only).....	494
Subelement 91—Custom Payment Service Response/Transaction ID (Visa Only).....	495
Subelement 92—CVC 2.....	496
Subelement 92—CVV2 Data (Visa Only).....	497
Subelement 93—Fleet Card ID Request Data (Visa Only).....	498
Subfield 1—Fleet Card ID Request Indicator.....	498
Subfield 2—Optional Free-form Informational Text.....	499
Subelement 94—Commercial Card Inquiry Request (Visa Only).....	499
Subelement 94—Commercial Card Inquiry Response (Visa Only).....	500
Subelement 95—Mastercard Promotion Code.....	501
Subelement 95—American Express Customer ID Number (American Express Only).....	502
Subelement 96—Visa Market-Specific Data Identifier (Visa Only).....	502
Subelement 97—Prestigious Properties Indicator (Visa Only).....	503
Subelement 98—Mastercard Corporate Fleet Card ID/Driver Number.....	504
Subelement 99—Mastercard Corporate Fleet Card Vehicle Number.....	505
DE 48—Authorization Platform Edits.....	506
DE 48, Proper Formatting.....	506
DE 48, TCC.....	506
DE 48, TCC and DE 3.....	507

---

DE 48, Subelement 14.....	508
DE 48, Subelement 26.....	508
DE 48, Subelement 35.....	509
DE 48, Subelement 37.....	510
DE 48, Subelement 38.....	510
DE 48, Subelement 42 and Subelement 43.....	512
DE 48, Subelement 43 (Static AAV).....	514
DE 48, Subelement 42 and DE 61.....	515
DE 48, Subelement 61.....	516
DE 48, Subelement 66.....	517
DE 48, Subelement 77.....	518
DE 48, Subelement 78.....	518
DE 48, Subelement 82.....	519
DE 48, Subelement 84.....	519
DE 48, Subelement 86.....	520
DE 48, Subelement 95.....	520
DE 48, in Authorization Request Response.....	520
DE 49—Currency Code, Transaction.....	521
DE 50—Currency Code, Settlement.....	522
DE 51—Currency Code, Cardholder Billing.....	523
DE 52—Personal ID Number (PIN) Data.....	524
DE 53—Security-Related Control Information.....	525
Subfield 1—PIN Security Type Code.....	526
Subfield 2—PIN Encryption Type Code.....	526
Subfield 3—PIN Block Format Code.....	527
Subfield 4—PIN Key Index Number.....	527
Subfield 5—Reserved for Future Use.....	528
Subfield 6—Reserved for Future Use.....	528
DE 54—Additional Amounts.....	528
Subfield 1—Account Type.....	531
Subfield 2—Amount Type.....	532
Subfield 3—Currency Code.....	532
Subfield 4—Amount.....	533
DE 54—Authorization Platform Edits.....	533
DE 55—Integrated Circuit Card (ICC) System-Related Data.....	534
DE 55—Subelement Encoding Scheme.....	535
DE 55—Subelements.....	536
DE 55—Authorization Platform Edits.....	540
Authorization Platform Edits—Cardholder Authentication Service.....	542

---

DE 56—Payment Account Data.....	545
Subelement 01—Payment Account Data.....	546
Subfield 01—Payment Account Reference (PAR).....	546
DE 57—DE 59—Reserved for National Use.....	546
DE 60—Advice Reason Code.....	547
Subfield 1—Advice Reason Code.....	548
DE 60, Subfield 1 Values, in Authorization Advice/0120.....	548
DE 60, Subfield 1 Values, in Reversal Advice/0420.....	550
DE 60, Subfield 1 Values, in Administrative Request/0600.....	550
DE 60, Subfield 1 Values, in Administrative Request Response/0610.....	550
DE 60, Subfield 1 Values, in Administrative Advice/0620.....	551
Subfield 2—Advice Detail Code.....	551
DE 60, Subfield 2 Values, in Authorization Advice/0120—Issuer-Generated.....	552
DE 60, Subfield 2 Values, in Authorization Advice/0120—System-Generated.....	552
DE 60, Subfield 2 Values, in Administrative Advice/0620.....	553
DE 60, Subfield 2 Values, in Customer Service Messages.....	553
DE 60, Subfield 2 Values, in Dynamic CVC 3 Validation.....	554
DE 60, Subfield 2 Values, in Mastercard In Control Service.....	554
DE 60, Subfield 2 Values, in M/Chip On-Behalf Services.....	555
DE 60, Subfield 2 Values, in Mastercard Digital Enablement Service.....	555
DE 60, Subfield 2 Values, in Mastercard Merchant Presented QR Service.....	556
DE 60, Subfield 2 Values, in Pay with Rewards.....	557
DE 60, Subfield 2 Values, in PIN Validation.....	557
DE 60, Subfield 2 Values, in Private Label Processing.....	557
DE 60, Subfield 2 Values, in TCC, CAT Level, and Promotion Code in Failed Parameter Combinations (Country-Specific).....	557
DE 60, Subfield 2 Values, in TCC, CAT Level, and Promotion Code in Failed Parameter Combinations (Global).....	558
DE 60, Subfield 2 Values, in MCC, CAT Level, and Promotion Code in Failed Parameter Combinations (Country-Specific).....	558
DE 60, Subfield 2 Values, in MCC and Promotion Code in Failed Parameter Combinations (Country-Specific).....	559
DE 60, Subfield 2 Values, in MCC and Promotion Code in Failed Parameter Combinations (Global).....	559
DE 60, Subfield 2 Values, in TCC and Promotion Code in Failed Parameter Combinations (Country-Specific).....	560
DE 60, Subfield 2 Values, in TCC and Promotion Code in Failed Parameter Combinations (Global).....	560
DE 60, Subfield 2 Values, in MCC and CAT Level in Failed Parameter Combinations (Country-Specific).....	561

---

DE 60, Subfield 2 Values, in MCC and CAT Level in Failed Parameter Combinations (Global).....	561
DE 60, Subfield 2 Values, in TCC and CAT Level in Failed Parameter Combinations (Country-Specific).....	562
DE 60, Subfield 2 Values, in TCC and CAT Level in Failed Parameter Combinations (Global).....	562
DE 60, Subfield 2 Values, in MCC in Failed Parameter Combinations (Country-Specific)....	563
DE 60, Subfield 2 Values, in MCC in Failed Parameter Combinations (Global).....	563
DE 60, Subfield 2 Values, in TCC in Failed Parameter Combinations (Country-Specific).....	564
DE 60, Subfield 2 Values, in TCC in Failed Parameter Combinations (Global).....	564
DE 60, Subfield 2 Values, in Miscellaneous Processing.....	565
Subfield 3—Advice Detail Text.....	565
DE 61—Point-of-Service (POS) Data.....	566
Subfield 1—POS Terminal Attendance.....	567
Subfield 2—Reserved for Future Use.....	567
Subfield 3—POS Terminal Location.....	568
Subfield 4—POS Cardholder Presence.....	568
Subfield 5—POS Card Presence.....	569
Subfield 6—POS Card Capture Capabilities.....	569
Subfield 7—POS Transaction Status.....	569
Subfield 8—POS Transaction Security.....	570
Subfield 9—Reserved for Future Use.....	570
Subfield 10—Cardholder-Activated Terminal Level.....	571
Subfield 11—POS Card Data Terminal Input Capability Indicator.....	571
Subfield 12—POS Authorization Life Cycle.....	573
Subfield 13—POS Country Code (or Sub-Merchant Information, if applicable).....	573
Subfield 14—POS Postal Code (or Sub-Merchant Information, if applicable).....	573
Authorization Platform Edits.....	574
DE 62—Intermediate Network Facility (INF) Data.....	577
DE 63—Network Data.....	578
Subfield 1—Financial Network Code.....	580
Subfield 2—Banknet Reference Number.....	590
DE 64—Message Authentication Code.....	590
DE 65—Bit Map, Extended.....	591
DE 66—Settlement Code.....	591
DE 67—Extended Payment Code.....	592
DE 68—Receiving Institution Country Code.....	592
DE 69—Settlement Institution Country Code.....	593
DE 70—Network Management Information Code.....	593

---

Network Management Request/0800—Sign-On/Sign-Off.....	594
Network Management Request/0800—Network Connection Status, Member-Generated.....	595
Network Management Request/0800—Network Connection Status, System-Generated.....	595
Network Management Request/0800—Host Session Activation/Deactivation.....	595
Network Management Request/0800—PEK Exchange.....	596
Network Management Request/0800—PEK Exchange-On Demand.....	596
Network Management Request Response/0810—PEK Exchange.....	596
Network Management Advice/0820—PEK Exchange.....	596
DE 71—Message Number.....	597
DE 72—Message Number Last.....	597
DE 73—Date, Action.....	597
DE 74—Credits, Number.....	598
DE 75—Credits, Reversal Number.....	598
DE 76—Debits, Number.....	599
DE 77—Debits, Reversal Number.....	599
DE 78—Transfers, Number.....	600
DE 79—Transfers, Reversal Number.....	600
DE 80—Inquiries, Number.....	600
DE 81—Authorizations, Number.....	601
DE 82—Credits, Processing Fee Amount.....	601
DE 83—Credits, Transaction Fee Amount.....	602
DE 84—Debits, Processing Fee Amount.....	602
DE 85—Debits, Transaction Fee Amount.....	603
DE 86—Credits, Amount.....	603
DE 87—Credits, Reversal Amount.....	603
DE 88—Debits, Amount.....	604
DE 89—Debits, Reversal Amount.....	604
DE 90—Original Data Elements.....	605
Subfield 1—Original Message Type Identifier.....	606
Subfield 2—Original DE 11 (Systems Trace Audit Number).....	606
Subfield 3—Original DE 7 (Transmission Date and Time).....	606
Subfield 4—Original DE 32 (Acquiring Institution ID Code).....	607
Subfield 5—Original DE 33 (Forwarding Institution ID Code).....	607
DE 91—Issuer File Update Code.....	608
DE 92—File Security Code.....	608
DE 93—Response Indicator.....	609
DE 94—Service Indicator.....	609
Subfield 1—Reserved for Future Use.....	610
Subfield 2—Acquirer/Issuer Indicator.....	610

---

Subfield 3—Address Data Indicator.....	610
DE 95—Replacement Amounts.....	611
Subfield 1—Actual Amount, Transaction.....	612
Subfield 2—Actual Amount, Settlement.....	613
Subfield 3—Actual Amount, Cardholder Billing.....	613
Subfield 4—Zero Fill.....	613
DE 96—Message Security Code.....	614
DE 97—Amount, Net Settlement.....	614
Subfield 1—Debit/Credit Indicator.....	615
Subfield 2—Amount.....	615
DE 98—Payee.....	615
DE 99—Settlement Institution ID Code.....	616
DE 100—Receiving Institution ID Code.....	616
DE 101—File Name.....	617
DE 102—Account ID 1.....	618
DE 103—Account ID 2.....	619
DE 104—Transaction Description.....	619
DE 105—DE 107—Reserved for Mastercard Use.....	620
DE 108—MoneySend Reference Data.....	620
DE 108—Authorization Platform Edits.....	622
Subelement 01—Receiver/Recipient Data.....	623
Subfield 01—Receiver/Recipient First Name.....	625
Subfield 02—Receiver/Recipient Middle Name.....	626
Subfield 03—Receiver/Recipient Last Name.....	626
Subfield 04—Receiver/Recipient Street Address.....	627
Subfield 05—Receiver/Recipient City.....	628
Subfield 06—Receiver/Recipient State/Province Code.....	628
Subfield 07—Receiver/Recipient Country.....	629
Subfield 08—Receiver/Recipient Postal Code.....	629
Subfield 09—Receiver/Recipient Phone Number.....	630
Subfield 10—Receiver/Recipient Date of Birth.....	630
Subfield 11—Receiver/Recipient Account Number.....	631
Subfield 12—Receiver/Recipient Identification Type.....	632
Subfield 13—Receiver/Recipient Identification Number.....	632
Subfield 14—Receiver/Recipient Identification Country Code.....	633
Subfield 15—Receiver/Recipient Identification Expiration Date.....	633
Subfield 16—Receiver/Recipient Nationality.....	634
Subfield 17—Receiver/Recipient Country of Birth.....	634
Subelement 02—Sender Data.....	635

---

Subfield 01—Sender First Name.....	636
Subfield 02—Sender Middle Name.....	637
Subfield 03—Sender Last Name.....	638
Subfield 04—Sender Street Address.....	639
Subfield 05—Sender City.....	639
Subfield 06—Sender State/Province Code.....	640
Subfield 07—Sender Country.....	640
Subfield 08—Postal Code.....	641
Subfield 09—Sender Phone Number.....	641
Subfield 10—Sender Date of Birth.....	642
Subfield 11—Sender Account Number.....	642
Subfield 12—Sender Identification Type.....	643
Subfield 13—Sender Identification Number.....	644
Subfield 14—Sender Identification Country Code.....	645
Subfield 15—Sender Identification Expiration Date.....	645
Subfield 16—Sender Nationality.....	646
Subfield 17—Sender Country of Birth.....	646
Subelement 03—MoneySend Transaction Data.....	647
Subfield 01—Unique Transaction Reference.....	647
Subfield 02—Additional Message.....	648
Subfield 03—Funding Source.....	649
Subfield 04—Participation ID.....	650
Subfield 05—Transaction Purpose.....	651
Subelement 04—MoneySend Language Description.....	652
Subfield 01—Language Identification.....	652
Subfield 02—Language Data.....	653
Subelement 05—Digital Account Information.....	653
Subfield 01—Digital Account Reference Number.....	654
Subfield 02—Mastercard Merchant Presented QR Receiving Account Number.....	655
Subelement 06—QR Dynamic Code Data.....	656
DE 109—Reserved for ISO Use.....	657
DE 110—Additional Data—2.....	658
Subelement 9—ANSI X9 TR-31 Key Block Key (128-bit Key Block Protection Key).....	659
Subelement 9—ANSI X9 TR-31 Key Block Key (192-bit Key Block Protection Key).....	659
Subelement 10—Key Check Value.....	660
DE 111—Reserved for ISO Use.....	660
DE 112—Additional Data (National Use).....	661
DE 112—Encoding Scheme.....	662
DE 112—Authorization Platform Edits.....	663

---

All Regions—Installment Payment Transactions.....	664
Subelement 21—Installment Payment Data 1.....	664
Subelement 22—Installment Payment Data 2.....	665
Subelement 23—Installment Payment Data 3.....	668
Alternate Processing.....	669
Brazil—Payment Transactions.....	669
Subelement 012—Brazil Commercial and Financing Data.....	669
Subelement 013—Crediário First Simulation.....	672
Subelement 014—Crediário Second Simulation.....	675
Subelement 015—Crediário Third Simulation.....	678
Subelement 018—Brazil Post-Dated Transaction Data.....	680
Subelement 019—Original Purchase Amount.....	683
Brazil—Merchant Fraud Scoring Data.....	684
Subelement 028—Merchant Fraud Score Data.....	684
Chile—Payment Transactions.....	685
Subelement 010—Installment Payment Data.....	685
Colombia—Domestic Transactions.....	686
Subelement 035—Issuer Fee Inquiry Indicator.....	686
Subelement 036—Issuer Fee Amount.....	686
Colombia—Payment Transactions.....	687
Subelement 010—Installment Payment Data.....	687
Subelement 011—Customer ID.....	688
Cuotas—Payment Transactions.....	688
Subelement 001—Installment Payment Data.....	688
Subelement 003—Installment Payment Response Data.....	690
Subelement 027—ATM Credit Card Cash Advance Installments.....	690
Europe Region and Philippines—Payment Transactions.....	694
Subelement 009—Installment Payment Data.....	694
Subelement 020—Domestic Card Acceptor Tax ID.....	696
Greece—Payment Transactions.....	697
Subelement 006—Installment Payment Data.....	697
Subelement 008—Installment Payment Response Data.....	698
Japan—Payment Transactions.....	699
Subelement 030—Japan Domestic POS Data.....	699
Subelement 031—Japan Domestic Response Code.....	701
Subelement 032—Japan Payment Options.....	702
Mexcta—Payment Transactions.....	707
Subelement 004—Credit Line Usage Fee (CLUF).....	707
Subelement 005—Issuing Bank Name (AKA Doing Business As [DBA]).....	707

---

Subelement 006—Financial Institution ID (FIID).....	708
Subelement 007—Installment Payment Data.....	708
Subelement 008—Installment Payment Response Data.....	709
Netherlands—IBAN—Account Inquiry.....	710
Subelement 037—Additional Cardholder Information.....	710
Parcelas—Payment Transactions.....	712
Subelement 001—Installment Payment Data.....	713
Subelement 002—Installment Payment Response Data.....	713
Subelement 016—Additional Installment Payment Response Data.....	714
Percta—Payment Transactions.....	715
Subelement 007—Installment Payment Data.....	715
Subelement 008—Installment Payment Response Data.....	716
Spain—Domestic ATM Transactions.....	717
Subelement 017—ATM Domestic Fee.....	717
United Kingdom—Debt Repayment Transactions.....	719
Subelement 033—UK Recipient Details.....	719
DE 113—Reserved for National Use.....	721
Generic Data, Administrative Request/0600 Message.....	722
Banking Data, Administrative Request/0600 Message.....	723
DE 114—Reserved for National Use.....	724
Consumer Application Request Data Administrative Request/0600 Message.....	725
Consumer Status Inquiry or Preapproved Offer Inquiry Data Administrative Request/0600 Message.....	727
Consumer Account Maintenance Data Administrative Request/0600 Message.....	728
Consumer Application Response Data Administrative Request Response/0610 Message.....	731
Consumer Account Maintenance Data Administrative Request Response/0610 Message.....	732
DE 115—Reserved for National Use.....	736
Business Application Request Data Administrative Request/0600 Message.....	736
Business Application Status Inquiry Data or Business Preapproved Offer Inquiry Data Administrative Request/0600 Message.....	738
Business Account Maintenance Data Administrative Request/0600 Message.....	739
Business Application Response Data Administrative Request Response/0610 Message.....	742
Business Account Maintenance Data Administrative Request Response/0610 Message.....	743
DE 116—Reserved For National Use.....	747
Consumer User Lookup Inquiry Data Administrative Request/0600.....	748
Consumer Account Lookup Inquiry Data Administrative Request/0600 Message.....	749
Consumer Account Lookup Response Data Administrative Request Response/0610 Message.....	750
DE 117—Reserved for National Use.....	751
Business User Lookup Inquiry Data Administrative Request/0600 Message.....	752

---

Business Account Lookup Inquiry Data Administrative Request/0600 Message.....	753
Business Account Lookup Response Data Administrative Request Response/0610 Message....	754
DE 118—Reserved for National Use.....	755
Authorized User Data Administrative Request/0600 Message.....	756
Trade Reference Data Administrative Request/0600 Message.....	757
Authorized User Response Data Administrative Request/0610 Message.....	758
DE 119—Reserved for National Use.....	759
Using DE 113–119 in Administrative 06xx Messages.....	760
DE 120—Record Data.....	763
Subfield 01—AVS Service Indicator 1.....	765
Subfield 02—AVS Service Indicator 2.....	765
Subfield 03—AVS Service Indicator 3.....	766
Subfield 04—AVS Service Indicator 4.....	766
Online File Maintenance.....	767
MCC102—Stand-In Account File.....	768
MCC103—Electronic Warning Bulletin File.....	769
MCC104—Local Stoplist File.....	771
MCC105—Payment Cancellation File.....	775
MCC106—PAN Mapping File.....	778
MCC107—Enhanced Value File.....	783
MCC108—Product Graduation File.....	785
MCC109—Application Transaction Counter File.....	787
MCC111—PAN-PAR (Payment Account Reference) Mapping File.....	789
DE 120 Error Codes.....	790
DE 121—Authorizing Agent ID Code.....	806
DE 122—Additional Record Data.....	808
DE 123—Receipt Free Text.....	809
DE 124—Member-Defined Data.....	810
DE 124—Member-Defined Data (General Use).....	810
DE 124—Member-Defined Data (MoneySend Only).....	812
DE 124—Member-Defined Data (Brazil Maestro Only).....	812
Subfield 1—Unique Reference Number.....	812
Subfield 2—Sender/Payer/User ID.....	813
Subfield 3—Sender/Payer Address.....	813
Subfield 4—Additional Sender Information.....	814
Subfield 6—Discretionary Message on Sales Slip Supported.....	815
Subfield 7—Discretionary Message on Sales Slip Code.....	815
Subfield 8—Discretionary Message on Sales Slip Content.....	816
Subfield 9—Phoneshop (Phone Company ID).....	816

---

Subfield 10—Phoneshop (Cell Phone Number).....	816
Subfield 11—Phoneshop (Message Security Code).....	817
Subfield 12—Merchant CNPJ Number.....	817
Subfield 13—Total Annual Effective Cost.....	817
DE 124—Member-Defined Data (Colombia Domestic Use Only).....	818
Subfield 1—Card Issuer Data.....	818
Subfield 2—Tax (IVA).....	818
Subfield 3—Tax Amount Base.....	819
Subfield 4—Retailer Data.....	819
Subfield 5—Terminal Acquirer Data.....	820
Subfield 6—Acquirer Original Processing Code.....	820
Subfield 7—Bill Payment/Top up Data.....	820
Subfield 8—Local POS Data.....	821
Subfield 9—Local Response Codes.....	821
Subfield 10—Original Transaction Data.....	822
Subfield 11—IAC Tax Amount.....	822
DE 125—New PIN Data.....	823
DE 126—Private Data.....	823
DE 127—Private Data.....	824
DE 128—Message Authentication Code.....	825

## Data Element Layout

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

Attribute	Description
Data Representation:	Annotation and data length (fixed or variable in length)
Length Field:	2 or 3 if 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

### Usage

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.

•      •      •

### Values

Valid values and name of each value listed.

### Application Notes

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
Data Representation:	Annotation and data length (fixed or variable in length)
Length Field	2 or 3 if variable in length
Data Field:	Contents of subfields
Subfields:	Indicates number of subfields
Justification:	See subfields (may be subfield specific)

### Usage

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 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)
Data Representation:	Annotation and data length (fixed or variable in length)
Length Field:	2 if variable in length (omitted if not part of the data)
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.

<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>7</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>7</sup>	n-4
18	Merchant Type	n-4
19	Acquiring Institution Country Code <sup>7</sup>	n-3
20	Primary Account Number (PAN) Country Code	n-3
21	Forwarding Institution Country Code <sup>7</sup>	n-3
22	Point-of-Service (POS) Entry Mode	n-3
23	Card Sequence Number	n-3
24	Network International ID <sup>7</sup>	n-3
25	Point-of-Service (POS) Condition Code <sup>7</sup>	n-2
26	Point-of-Service (POS) Personal ID Number (PIN) Capture Code	n-2
27	Authorization ID Response Length <sup>7</sup>	n-1
28	Amount, Transaction Fee	an-9

<sup>7</sup> 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.

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
29	Amount, Settlement Fee <sup>7</sup>	an-9
30	Amount, Transaction Processing Fee <sup>7</sup>	an-9
31	Amount, Settlement Processing Fee <sup>7</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>7</sup>	ans...28; LLVAR
35	Track 2 Data	ans...37; LLVAR
36	Track 3 Data <sup>7</sup>	ans...104; LLLVAR
37	Retrieval Reference Number	an-12
38	Authorization ID Response	ans-6
39	Response Code	an-2
40	Service Restriction Code <sup>7</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>7</sup>	ans...999; LLLVAR
47	Additional Data—National Use <sup>8</sup>	ans...999; LLLVAR
48	Additional Data—Private Use	ans...999; LLLVAR
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
53	Security-Related Control Information	n-16
54	Additional Amounts	an...240; LLLVAR
55	Integrated Circuit Card (ICC) System-Related Data	b...255; LLLVAR

<sup>8</sup> 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.

<sup>9</sup> This data element is an ISO-designated “private use” data element redefined by Mastercard in accordance with provisions of the ISO 8583–1987 specification.

---

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
56	Payment Account Data	an...37; LLLVAR
57–59	Reserved for National Use <sup>8</sup>	ans...999; LLLVAR
60	Advice Reason Code <sup>10</sup>	ans...060; LLLVAR
61	Point-of-Service (POS) Data <sup>10</sup>	an...026; LLLVAR
62	Intermediate Network Facility (INF) Data <sup>10</sup>	ans...100; LLLVAR
63	Network Data <sup>10</sup>	an...050; LLLVAR
64	Message Authentication Code (MAC) <sup>7</sup>	b-8
65	Bit Map, Extended <sup>7</sup>	b-8
66	Settlement Code <sup>7</sup>	n-1
67	Extended Payment Code <sup>7</sup>	n-2
68	Receiving Institution Country Code <sup>7</sup>	n-3
69	Settlement Institution Country Code <sup>7</sup>	n-3
70	Network Management Information Code	n-3
71	Message Number <sup>7</sup>	n-4
72	Message Number Last <sup>7</sup>	n-4
73	Date, Action	n-6
74	Credits, Number <sup>7</sup>	n-10
75	Credits, Reversal Number <sup>7</sup>	n-10
76	Debits, Number <sup>7</sup>	n-10
77	Debits, Reversal Number <sup>7</sup>	n-10
78	Transfers, Number <sup>7</sup>	n-10
79	Transfers, Reversal Number <sup>7</sup>	n-10
80	Inquiries, Number <sup>7</sup>	n-10
81	Authorizations, Number <sup>7</sup>	n-10
82	Credits, Processing Fee Amount <sup>7</sup>	n-12
83	Credits, Transaction Fee Amount <sup>7</sup>	n-12
84	Debits, Processing Fee Amount <sup>7</sup>	n-12
85	Debits, Transaction Fee Amount <sup>7</sup>	n-12
86	Credits, Amount <sup>7</sup>	n-16

---

<sup>10</sup> Although this data element is designated as binary, it also may contain up to eight bytes of EBCDIC encoded data.

---

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
87	Credits, Reversal Amount <sup>7</sup>	n-16
88	Debits, Amount <sup>7</sup>	n-16
89	Debits, Reversal Amount <sup>7</sup>	n-16
90	Original Data Elements	n-42
91	Issuer File Update Code	an-1
92	File Security Code <sup>7</sup>	an-2
93	Response Indicator <sup>7</sup>	an-5
94	Service Indicator	an-7
95	Replacement Amounts	n-42
96	Message Security Code <sup>10</sup>	b-8
97	Amount, Net Settlement <sup>7</sup>	an-17
98	Payee	ans-25
99	Settlement Institution ID Code <sup>7</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>7</sup>	ans...100; LLLVAR
105–107	Reserved for Mastercard Use <sup>7</sup>	ans...999; LLLVAR
108	MoneySend Reference Data	ans...999; LLLVAR
109	Reserved for ISO Use <sup>7</sup>	ans...999; LLLVAR
110	Additional Data—2	ans...999; LLLVAR
111	Reserved for ISO Use <sup>7</sup>	ans...999; LLLVAR
112	Additional Data (National Use)	ans...100; LLLVAR
113–119	Reserved for National Use <sup>8</sup>	ans...999; LLLVAR
120	Record Data <sup>10</sup>	ans...999; LLLVAR
121	Authorizing Agent ID Code <sup>10</sup>	n...6; LLLVAR
122	Additional Record Data <sup>10</sup>	ans...999; LLLVAR
123	Receipt Free Text	ans...512; LLLVAR
124	Member-defined Data	ans...199; LLLVAR
125	New PIN Data	b-8

---

---

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
126	Private Data	ans...100; LLLVAR
127	Private Data <sup>10</sup>	ans...100; LLLVAR
128	Message Authentication Code (MAC) <sup>7</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>11</sup>	n-3
32	Acquiring Institution ID Code	n...6; LLVAR
54	Additional Amounts	an...240; LLLVAR
110	Additional Data—2	ans...999; LLLVAR
46	Additional Data—ISO Use <sup>11</sup>	ans...999; LLLVAR
47	Additional Data—National Use <sup>12</sup>	ans...999; LLLVAR
112	Additional Data (National Use)	ans...100; LLLVAR
48	Additional Data—Private Use <sup>13</sup>	ans...999; LLLVAR
122	Additional Record Data <sup>13</sup>	ans...999; LLLVAR
44	Additional Response Data	ans...25; LLVAR
60	Advice Reason Code <sup>13</sup>	ans...060; LLLVAR
6	Amount, Cardholder Billing	n-12
8	Amount, Cardholder Billing Fee <sup>11</sup>	n-8
97	Amount, Net Settlement <sup>11</sup>	an-17
5	Amount, Settlement	n-12

<sup>11</sup> 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.

<sup>12</sup> 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.

<sup>13</sup> This data element is an ISO-designated “private use” data element redefined by Mastercard in accordance with provisions of the ISO 8583–1987 specification.

---

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
29	Amount, Settlement Fee <sup>11</sup>	an-9
31	Amount, Settlement Processing Fee <sup>11</sup>	an-9
4	Amount, Transaction	n-12
28	Amount, Transaction Fee	an-9
30	Amount, Transaction Processing Fee <sup>11</sup>	an-9
38	Authorization ID Response	ans-6
27	Authorization ID Response Length <sup>11</sup>	n-1
81	Authorizations, Number <sup>11</sup>	n-10
121	Authorizing Agent ID Code <sup>13</sup>	n...6; LLLVAR
65	Bit Map, Extended <sup>11</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>11</sup>	n-16
74	Credits, Number <sup>11</sup>	n-10
82	Credits, Processing Fee Amount <sup>11</sup>	n-12
87	Credits, Reversal Amount <sup>11</sup>	n-16
75	Credits, Reversal Number <sup>11</sup>	n-10
83	Credits, Transaction Fee Amount <sup>11</sup>	n-12
51	Currency Code, Cardholder Billing	n-3
50	Currency Code, Settlement	n-3
49	Currency Code, Transaction	n-3
73	Date, Action	n-6
17	Date, Capture <sup>11</sup>	n-4
16	Date, Conversion	n-4
14	Date, Expiration	n-4
13	Date, Local Transaction	n-4

---

---

<b>Number</b>	<b>Name</b>	<b>Data Representation</b>
15	Date, Settlement	n-4
88	Debits, Amount <sup>11</sup>	n-16
76	Debits, Number <sup>11</sup>	n-10
84	Debits, Processing Fee Amount <sup>11</sup>	n-12
89	Debits, Reversal Amount <sup>11</sup>	n-16
77	Debits, Reversal Number <sup>11</sup>	n-10
85	Debits, Transaction Fee Amount <sup>11</sup>	n-12
67	Extended Payment Code <sup>11</sup>	n-2
101	File Name	ans...17; LLVAR
92	File Security Code <sup>11</sup>	an-2
21	Forwarding Institution Country Code <sup>11</sup>	n-3
33	Forwarding Institution ID Code	n...6; LLVAR
80	Inquiries, Number <sup>11</sup>	n-10
55	Integrated Circuit Card (ICC) System-Related Data	b...255; LLLVAR
62	Intermediate Network Facility (INF) Data <sup>13</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>11</sup>	b-8
128	Message Authentication Code (MAC) <sup>11</sup>	b-8
71	Message Number <sup>11</sup>	n-4
72	Message Number Last <sup>11</sup>	n-4
96	Message Security Code <sup>14</sup>	b-8
108	MoneySend Reference Data	ans...999; LLLVAR
63	Network Data <sup>13</sup>	an...050; LLLVAR
24	Network International ID <sup>11</sup>	n-3
70	Network Management Information Code	n-3
125	New PIN Data	b-8
90	Original Data Elements	n-42

---

<sup>14</sup> 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>
98	Payee <sup>11</sup>	ans-25
56	Payment Account Data	an...37; LLLVAR
52	Personal ID Number (PIN) Data	b-8
25	Point-of-Service (POS) Condition Code <sup>11</sup>	n-2
61	Point-of-Service (POS) Data <sup>13</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; LLVAR
20	Primary Account Number (PAN) Country Code	n-3
34	Primary Account Number (PAN), Extended <sup>11</sup>	ans...28; LLVAR
126	Private Data	ans...100; LLLVAR
127	Private Data <sup>13</sup>	ans...100; LLLVAR
3	Processing Code	n-6
123	Receipt Free Text	ans...512; LLLVAR
68	Receiving Institution Country Code <sup>11</sup>	n-3
100	Receiving Institution ID Code	n...11; LLVAR
120	Record Data <sup>13</sup>	ans...999; LLLVAR
95	Replacement Amounts	n-42
109	Reserved for ISO Use <sup>11</sup>	ans...999; LLLVAR
111	Reserved for ISO Use <sup>11</sup>	ans...999; LLLVAR
105–107	Reserved for Mastercard Use <sup>11</sup>	ans...999; LLLVAR
57–59	Reserved for National Use <sup>12</sup>	ans...999; LLLVAR
113–119	Reserved for National Use <sup>12</sup>	ans...999; LLLVAR
39	Response Code	an-2
93	Response Indicator <sup>11</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>11</sup>	an-3
66	Settlement Code <sup>11</sup>	n-1

---

Number	Name	Data Representation
69	Settlement Institution Country Code <sup>11</sup>	n-3
99	Settlement Institution ID Code <sup>11</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>11</sup>	ans...104; LLLVAR
104	Transaction Description <sup>11</sup>	ans...100; LLLVAR
78	Transfers, Number <sup>11</sup>	n-10
79	Transfers, Reversal Number <sup>11</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

### Usage

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—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
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—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—PEK Exchange	•	M	M
<b>Values</b>			
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
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.

<b>MTI</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</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	✓	✓	✓	✓	✓	✓
0130	Authorization Advice Response—System-generated	✓	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓

---

<b>MTI</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
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 consist 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.

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

Data Representation:	b-8
Length Field:	N/A
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	•
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—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—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
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—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

Data Representation: n...19; LLVAR

Length Field: 2

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
Authorization Request Response/0110	ME	•	ME
Authorization Advice/0120—Acquirer-generated	M	•	M

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

---

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	•
Network Management Request Response/0810—PEK Exchange—On Demand	•	ME	ME
<b>Values</b>			

---

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.

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

---

Data Representation: n-6

---

Length Field: N/A

---

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

Acquirers and prepaid card issuers in the U.S. region must support POS balance inquiry transaction type and functionality for all prepaid Mastercard credit and Debit Mastercard card account ranges.

The following cross edits occur for:

#### Authorization Request/0100

IF...	THEN...
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 01, 30, 91, or 92.

#### Reversal Request/0400 messages

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

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

IF...	THEN...
-------	---------

---

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

---

#### 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 [ASI]) and	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>
DE 3 (Processing Code) contains a value other than 00 (Purchase) or 28 (Payment)	

---

### 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
Justification:	N/A

---

#### Values

Cardholder Account Debits		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>						
20	=	Purchase Return/Refund	√	√	√	√
21	=	Deposit		√		
22	=	Credit Adjustment		√		
23	=	Check Deposit Guarantee		√		
24	=	Check Deposit		√		
28	=	Payment Transaction	√	√	√	√
<b>Cardholder Account Inquiries</b>						
30	=	Balance Inquiry	√	√	√	√
<b>Cardholder Account Transfers</b>						
40	=	Account Transfer	√	√		
<b>Reserved Values</b>						
90	=	Reserved for Future Use	√			
<b>PIN Management Transactions</b>						
91	=	PIN Unblock	√	√	√	√
92	=	PIN Change	√	√	√	√
<b>Token Requests and Token Maintenance Requests</b>						
93	=	Card on File Token Processing	√			
<b>Application Notes</b>						

---

---

Value 20 will be allowed for MDES related Authorization Request/0100 messages even if the account status is suspended or delete pending.

Effective with Release 19.Q2, value 20 will be allowed for Visa gateway transactions to support the authorization of returns or refunds.

The Dual Message System (Authorization) identifies refund transactions in DE 3, subfield 1 (Cardholder Transaction Type Code) with a value of 20 (Purchase Return/Refund). Mastercard requires that issuers receive and respond to refund transactions involving a Mastercard, Debit Mastercard, or Maestro card.

Values 21–24 are not currently supported for use on the Authorization Platform.

Value 30 is only applicable to eligible issuers.

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

Value 93 is used only for token requests and maintenance by the token requestor and will appear in the following messages:

- Authorization Request/0100
- Authorization Request Response/0110

**NOTE: Value 93 will be decommissioned in a future release.**

---

## 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:

Cardholder “From Account” Type Code		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	√

---

### 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:

---

Cardholder "To Account" Type Code	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

Data Representation:	n-12
Length Field:	N/A
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 and Reversal Request/0400—Balance Inquiry, except where ATM transaction fees are allowed
- Authorization Request/0100—Chargeback Period Extension Request
- 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
- Authorization Request/0100—Account Status Inquiry with Authentication Indicator

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

---

### **Application Notes**

DE 4 cannot exceed the region or country Mastercard® MoneySend™ Funding and Payment Transaction limit.

<b>WHEN...</b>	<b>THEN...</b>
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:**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The Authorization Request/0100 message contains DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI]) and  DE 4 (Amount, Transaction) contains a value greater than zero and DE 3 (Processing Code) contains a value of 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) = 004</li></ul>

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

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 (cancelling a previously approved authorization) from any acquirer as there is no Authorization Platform edit restricting such advices from Europe region acquirers.

### **For Card Activation Requests:**

<b>WHEN...</b>	<b>THEN...</b>
----------------	----------------

---

The Authorization Request/0100 message contains DE 48, subelement 77 = C09 (Card Activation) and DE 4 other than zero

Sends the acquirer an Authorization Request Response/0110 message where:

- DE 39 (Response Code) = 30
- DE 44 (Additional Response Data) = 004

Usage of value C09 is limited to Private Label Prepaid Cards issued in Europe.

#### **For Authorization Chargeback Protection Period Extension Requests:**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The acquirer sends an Authorization Chargeback Protection Period Extension Authorization Request/0100 message that contains the following:</p> <ul style="list-style-type: none"> <li>• DE 3 (Processing Code), subfield 1 (Transaction Type), value 00 (Purchase)</li> <li>• DE 4 (Transaction Amount), value 0</li> <li>• DE 48 (Additional Data), subelement 63 (Trace ID) is present</li> <li>• DE 61, subelement 4 (POS Cardholder Presence) is not equal to value 4 (Standing Order/Recurring)</li> <li>• DE 61 (POS Data), subelement 7 (POS Transaction Status), value 4 (Prauthorized)</li> </ul> <p>and the issuer is not available to respond to the request</p>	<p>Rejects the transaction where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 91 (Authorization System or issuer system inoperative)</li> </ul>
<p>The acquirer sends an Authorization Request/0100 message for an Authorization Chargeback Protection Period Extension request:</p> <ul style="list-style-type: none"> <li>• DE 3 (Processing Code), subfield 1 (Transaction Type), value 00 (Purchase)</li> <li>• DE 4 (Transaction Amount), value 0</li> <li>• DE 48 (Additional Data), subelement 63 (Trace ID) is NOT present</li> <li>• DE 61, subelement 4 (POS Cardholder Presence) is not equal to value 4 (Standing Order/Recurring), and</li> <li>• DE 61 (POS Data), subelement 7 (POS Transaction Status), value 4 (Prauthorized)</li> </ul>	<p>Rejects the transaction where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format Error)</li> <li>• DE 44 (Additional Response Data) = 0480nn (where nn is the subelement number)</li> </ul>

The acquirer sends an Authorization Request/0100 message for an Authorization Chargeback Protection Period Extension request:

- DE 3 (Processing Code), subfield 1 (Transaction Type), value 00 (Purchase)
- DE 4 (Transaction Amount), value 0
- DE 48 (Additional Data), subelement 63 (Trace ID) is present
- DE 61, subelement 4 (POS Cardholder Presence) is not equal to value 4 (Standing Order/Recurring)
- DE 61 (POS Data), subelement 7 (POS Transaction Status), value 4 (Preauthorized)

And if the values for Contactless Transit Aggregated, Transit Debt Recovery Transactions are present:

- DE 48 (Additional Data), subelement 64 (Transit Program), subfield 1 (Transit Transaction Type Individual) = 03 (Post-Authorized Aggregated), 04 (Authorized Aggregated Split Clearing), or 06 (Post-Authorized Aggregated Maestro)

Rejects the transaction where:

- DE 39 (Response Code) = 30 (Format Error)
- DE 44 (Additional Response Data) = 061 (Point-of-Service [POS] Data)

The acquirer sends an Authorization Request/0100 message for an Authorization Chargeback Protection Period Extension request:

- DE 3 (Processing Code), subfield 1 (Transaction Type), value 00 (Purchase)
- DE 4 (Transaction Amount), value 0
- DE 48 (Additional Data), subelement 63 (Trace ID) is present
- DE 61, subelement 4 (POS Cardholder Presence) is not equal to value 4 (Standing Order/Recurring)
- DE 61 (POS Data), subelement 7 (POS Transaction Status), value 4 (Preauthorized)

Rejects the transaction where:

- DE 39 (Response Code) = 30 (Format Error)
- DE 44 (Additional Response Data) = 004 (Transaction Amount)

And if the values for Transit Debt Recovery Transactions are present:

- DE 48 (Additional Data), subelement 64 (Transit Program), subfield 1 (Transit Transaction Type Individual) = 07 (Debt Recovery)

Or if the values for an installment payment transaction are present:

- DE 48 (Additional Data), subelement 95 (Promotion Code)

---

The acquirer sends an Acquirer-Generated Advice/0120 or Acquirer-Generated Reversal/0400 message for an Authorization Chargeback Protection Period Extension request where the message contains the following:

- DE 3 (Processing Code), subfield 1 (Transaction Type), value 00 (Purchase)
  - DE 4 (Transaction Amount), value 0
  - DE 48 (Additional Data), subelement 63 (Trace ID) is present
  - DE 61, subelement 4 (POS Cardholder Presence) is not equal to value 4 (Standing Order/Recurring)
  - DE 61 (POS Data), subelement 7 (POS Transaction Status), value 4 (Preauthorized)
- 

Rejects the transaction where:

- DE 39 (Response Code) = 30 (Format Error)
- DE 44 (Additional Response Data) = 004 (Transaction Amount)

## 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

---

Data Representation: n-12

---

Length Field: N/A

---

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	•	C
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.

### 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.

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

---

Data Representation:	n-12
Length Field:	N/A
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	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	CE	X	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)

Issuers must adhere to the following when providing a partial approval Authorization Request/0110 message:

- 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 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 Network. Date and time must be expressed in Coordinated Universal Time (UTC).

---

### Attributes

---

Data Representation:	n-10
Length Field:	N/A

---

---

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	•
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

#### **Values**

See subfields

#### **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. The transmission time provided in DE 7 must be within three minutes of the current time recorded by the Mastercard 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

---

Data Representation: n-8

---

Length Field: N/A

---

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

---

Data Representation:	n-8
Length Field:	N/A
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:

	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**

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 or Reversal Request/0400 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

---

Data Representation:	n-8
Length Field:	N/A
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
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	CE	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 or Reversal Request/0400 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
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

Data Representation: n-6

Length Field: N/A

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
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.

If the transaction time is not known at the time of authorization (for example, in the case of a preauthorization request), the acquirer must use the authorization time in this field.

### 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.

---

## 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

---

Data Representation: n-4

---

Length Field: N/A

---

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.

If the transaction date is not known at the time of authorization (for example, in the case of a preauthorization request), the acquirer must use the authorization date in this field.

---

### 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.

---

## 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

---

Data Representation: n-4

---

Length Field: N/A

---

Data Field: Contents of positions 1–4

---

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
<b>Values</b>	
This data element must consist of a year and a month in YYMM format.	
<b>Application Notes</b>	
This data element is defined and used identically within all Mastercard programs and services.	
<b>IF...</b>	<b>THEN...</b>
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.
An MDES transaction	DE 14 must be populated when provided by the merchant. It might contain a dynamic expiration date.

## 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	
Data Representation:	n-4
Length Field:	N/A
Data Field:	Contents of positions 1–4
Subfields:	N/A
Justification:	N/A
<b>Usage</b>	

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.

### 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 processing system (CPS) or intermediate network facility (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

Data Representation:	n-4
Length Field:	N/A
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	CE	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

---

Data Representation:	n-4
Length Field:	N/A
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

---

Data Representation:	n-4
Length Field:	N/A
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>
The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 or Reversal Request/0400 message for a MoneySend Payment Transaction where: <ul style="list-style-type: none"><li>• DE 3, subfield 1 contains value 28</li><li>• DE 18 does not contain MCC 6536 or MCC 6537</li><li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li><li>• DE 61, subfield 10 criteria is met for MoneySend<ul style="list-style-type: none"><li>– 0 = Not a CAT transaction</li><li>– 1 = Authorized Level 1 CAT: Automated dispensing machine with PIN</li><li>– 2 = Authorized Level 2 CAT: Self-service terminal</li><li>– 6 = Authorized Level 6 CAT: Electronic commerce</li></ul></li><li>• DE 124 is present</li></ul>	The Authorization Platform sends the OFI an Authorization Request Response/0110 or Reversal Request Response/0410 message where: <ul style="list-style-type: none"><li>• DE 39 = 30 (Format error)</li><li>• DE 44 = 018 (Merchant Type)</li></ul>

## 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

---

---

Data Representation:	n-3
Length Field:	N/A
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.

---

Attributes

Data Representation:	n-3
Length Field:	N/A
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.

## 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

Data Representation:	n-3
Length Field:	N/A
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) indicates the method used for PAN entry to initiate a transaction and the PIN entry capabilities.

#### Attributes

Data Representation:	n-3
----------------------	-----

---

Length Field:	N/A
Data Field:	Contents of subfields 1–2
Subfields:	2
Justification:	See subfields

### **Usage**

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 the method used for PAN entry to initiate a transaction.

### Attributes

Data Representation:	n-2
Data Field:	Contents of positions 1–2
Justification:	N/A

### Values

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 submit magnetic stripe transactions, 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
07	= PAN auto-entry via contactless M/Chip
09	= PAN TokenName via electronic commerce containing DSRP cryptogram in DE 55 (Integrated Circuit Card [ICC] System-Related Data).
10	= Credential on File

**NOTE: Mastercard is mandating support of the new DE 22, subfield 1, value 10 (Credential on File) effective as of 12 June 2018 for all issuers globally, and for all acquirers excluding Canada. Acquirers within Canada are mandated to support the new value effective as of 12 October 2018. However, acquirers in Canada can begin to support and use the new value effective as of 12 June 2018 (or anytime leading up to 12 October 2018) if they choose to do so, at which time they would become subject to the requirements defined herein.**

---

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 *M/Chip Requirements* for additional information.

---

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 TokenName entry via electronic commerce with optional SecureCode-AAV or DSRP cryptogram in UCAF.

---

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 transmitted by the acquirer within the authorization request in DE 35 (Track 2 Data) or DE 45 (Track 1 Data) and forwarded to the issuer without alteration or truncation.

---

95 = Visa only. Chip card with unreliable Card Verification Value (CVV) data.

## Subfield 2—POS Terminal PIN Entry Mode

DE 22 (Point-of-Service [POS] Entry Mode), subfield 2 (POS Terminal PIN Entry Mode) describes the capability of the terminal device to support/accept PIN entry.

---

### 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
3	=	mPOS Software-based PIN Entry Capability
8	=	Terminal has PIN entry capability but PIN pad is not currently operative

## Authorization Platform Edits

The Authorization Platform performs edits on specific programs and services.

Edits are performed on the following programs and services:

- Mastercard Electronic Card Transactions
- Mastercard Consumer Presented QR Transactions
- Chip Transactions
- Magnetic Stripe or Chip-Read Transactions for Mastercard Electronic Card
- Contactless Magnetic Stripe Transactions
- Credential on File Transactions

### 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

WHEN....	THEN...
DE 22, subfield 1 contains the value 81 (PAN)	DE 48, subelement 42 must be present. entry via electronic commerce, including chip)

### Mastercard Consumer Presented QR Transactions

The Authorization Platform performs the following system edits to help ensure that acquirers supporting merchants that choose to submit tokenized Mastercard Consumer Presented QR transactions are properly using value 03 (PAN auto-entry via barcode reader) in DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) in Authorization Request/0100 messages.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>An Authorization Request/0100 or Authorization Advice/0120—Acquirer-generated message contains DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), value 03 (PAN auto-entry via barcode reader)</p> <p>and</p> <p>DE 48 (Additional Data— Private Use), subelement 21 (Acceptance Data), subfield 2 (Additional Terminal Capability Indicator) is present and does not contain any of the valid value combinations of 00, 01, 10, or 11</p>	<p>Rejects the message and sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 048021 (indicating the data element in error)</li> </ul> <p><b>NOTE: If DE 48, subelement 21, subfield 2 is not present, the Authorization Platform will continue processing the message.</b></p>
<p>An Authorization Request/0100 message contains DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), value 03 (PAN auto-entry via barcode reader)</p> <p>and</p> <p>DE 18 (Merchant Type) contains MCC 6011 (Member Financial Institution—Automated Cash Disbursements) or DE 48 (Additional Data—Private Use), TCC (Transaction Category Code), contains value Z (ATM Cash Disbursement)</p>	<p>Rejects the message and sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 58 (Transaction not permitted to acquirer/terminal)</li> </ul>
<p>An Authorization Request/0100 message contains both of the following:</p> <ul style="list-style-type: none"> <li>• DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), value 03 (PAN auto-entry via barcode reader); and</li> <li>• DE 52 (Personal ID Number [PIN] Data)</li> </ul>	<p>Rejects the message and sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 58 (Transaction not permitted to acquirer/terminal)</li> </ul>

### **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

WHEN...	THEN the Authorization Platform...
The Authorization Request/0100 message contains DE 22, subfield 1 = 05 or 07 or 09 and DE 55 is present and Acquirer Chip testing level associated with the acquirer indicates the acquirer is approved for partial grade chip transaction	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) = 055</li> </ul>
The Authorization Request/0100 message contains DE 22, subfield 1 contains value 09 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 (Response Code) = 30 (Format error)</li> <li>• DE 44 = 055</li> </ul>
The Authorization Request/0100 message contains DE 22, subfield 1 contains value 05 or 07 or 09 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 where: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 022</li> </ul>
The Authorization Request/0100 message contains DE 22, subfield 1 contains value 09 and DE 61, subfield 4 does not contain value 5 and DE 61, subfield 10 does not contain value 6	Sends the acquirer an Authorization Request Response/0110 where: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 061</li> </ul>
The Authorization Request/0100 message contains DE 22, subfield 1 contains value 09 and DE 61, subfield 3 does not contain value 2 or 4	Sends the acquirer an Authorization Request Response/0110 where: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 061</li> </ul>
DE 55 is present in the Authorization Request/0100 message or the Authorization Advice/0120 message and DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 does not contain value 03, 05, 07, 09, or 81	Rejects the Authorization Request/0100 message or Authorization Advice/0120 message where: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 055</li> </ul>

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>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</p>	<p>Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30 (Format error)</li> <li>• DE 44 = 022</li> </ul>
<p>DE 22, subfield 1, contains value 80 and the service code in DE 35—Track 2 Data is not 2xx or 6xx, indicating that it is not a chip card</p>	<p>Replaces DE 22, subfield 1, value 80 with value 90 before forwarding the Authorization Request/0100 message to the issuer and</p> <p>Notifies the acquirer of this downgrade by populating DE 48, subelement 74 (Additional Processing Information) in 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**

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) contains value 80 and the service code in DE 35—Track 2 Data is not 2xx or 6xx, indicating that it is not a chip card</p>	<p>Replaces DE 22, subfield 1, value 80 with value 90 before forwarding the Authorization Advice/0120 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

WHEN...	THEN the Authorization Platform...
The Authorization Request/0100 message for a Mastercard Electronic card contains DE 22, subfield 1, value 02, 05, 07, 09, 80, 90, or 91 and the value in DE 18 is equal to a non-face-to-face environment	Determines whether the MCC in DE 18 (Merchant Type) is one of the following values that represent a non-face-to-face environment: <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> 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, 09, 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).

### Contactless Magnetic Stripe Transactions

The Authorization Platform will perform the following edit on authorization transactions that contain a contactless magnetic stripe account number that is participating in the Contactless Mapping Service.

## Authorization Request/0100 Message

WHEN...	THEN the Authorization Platform...
DE 22, subfield 1 is value 91 and DE 35 or DE 45 is not present	Rejects the transaction and sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 022</li></ul>

**NOTE: This edit is not performed on an Authorization Advice/0120 message or a Reversal Request/0400 message because track data is not expected for a Reversal Request/0400 message and is optional for an Authorization Advice/0120 message.**

## Credential on File Transactions

The Authorization Platform performs the following edits.

WHEN...	THEN the Authorization Platform...
An Authorization Request/0100 message contains: <ul style="list-style-type: none"><li>• DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) = 10 (Credential on File), and</li><li>• DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence) = 5 (Cardholder not present [Electronic order])</li></ul> And DE 48, subelement 42 is not present	Sends 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) = 048042</li></ul>

## DE 23—Card Sequence Number

DE 23 (Card Sequence Number) distinguishes among separate cards having the same DE 2 (Primary Account Number [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**

Data Representation:	n-3
Length Field:	N/A
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.

If the account range is registered for the Authentication Indicator Type 1 Service, then DE 23 should be present.

---

### 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

---

#### MDES Application Note

---

**NOTE: The following feature only applies to tokens that use a secure element or cloud token type.**

DE 23 is not provided unless the issuer opts to receive it.

For more information, refer to the *Mastercard Digital Enablement Service Issuer Implementation Guide*.

---

## DE 24—Network International ID

---

DE 24 (Network International ID) identifies a single international network of card issuers.

---

### Attributes

---

Data Representation: n-3

---

Length Field: N/A

---

Data Field: N/A

---

Subfields: N/A

---

Justification: N/A

---

### Usage

---

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

Data Representation:	n-2
Length Field:	N/A
Data Field:	N/A
Subfields:	N/A
Justification:	N/A

### Usage

The Authorization Platform currently does not use this data element. All Mastercard customers are required to use DE 61 for POS Condition Code information. 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

Data Representation:	n-2
Length Field:	N/A
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.**

---

## 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.

---

#### Attributes

---

Data Representation:	n-1
Length Field:	N/A
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

Data Representation:	an-9
Length Field:	N/A
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—Acquirer-generated	C	•	C
Authorization Advice/0120—System-generated	•	X	C
Authorization Advice Response/0130—Issuer-generated	CE	•	CE
Authorization Advice Response/0130—System-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.

---

**WHEN an acquirer sends an Authorization Advice/0120 message and... THEN the Authorization Platform...**

DE 28 is not provided in an Authorization Advice Response/0130 message, or is provided, but it contains a value different from the original request	Populates the DE 28 value from the Authorization Advice/0120 message in the response message before sending to the acquirer.
---	--

---

## **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

---

**Application Notes**

---

**WHEN an acquirer sends an Authorization Advice/0120 message and... THEN the Authorization Platform...**

---

DE 28, subfield 1 (Debit/Credit Indicator) contains a value other than C (Credit) or D (Debit)	Forwards to the acquirer an 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) = 028 (indicating the data element in error).</li></ul>
--	---

---

## 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

---

Data Representation: an-9

---

Length Field: N/A

---

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
Values	
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
Values	
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	
Data Representation:	an-9
Length Field:	N/A
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 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

---

Data Representation: an-9

---

Length Field: N/A

---

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.

---

### Attributes

---

Data Representation:	n...6; LLVAR
Length Field:	2
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 processing 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.

For bridged transactions acquired on the Single Message System, issuers will receive the 6-digit customer ID number assigned by Mastercard that identifies the institution acting as the “acquiring bank” or “merchant bank” for a transaction in DE 32 (Acquiring Institution Identification Code) of the authorization message instead of a Mastercard-assigned internal ICA.

**NOTE: Transactions that have passed between platforms (Single Message System to Dual Message System, Dual Message System to Single Message System) are referred to as bridged transactions.**

#### Visa transactions:

Acquirers must use their Mastercard-assigned customer ID in DE 32 of Visa-branded authorizations, and must also provide their Visa-assigned acquirer BIN to the Global Customer Service team.

---

## 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**

---

Data Representation:	n...6; LLVAR
----------------------	--------------

---

Length Field:	2
---------------	---

---

Data Field:	Contents of positions 1–6
-------------	---------------------------

---

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

---

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

---

#### **Usage**

---

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.

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

Data Representation:	ans...28; LLVAR
Length Field:	2
Data Field:	N/A
Subfields:	N/A

---

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

**Usage**

The Authorization Platform currently does not use this data element.

---

## 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**

---

Data Representation:	ans...37; LLVAR
----------------------	-----------------

---

Length Field:	2
---------------	---

---

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.

DE 35 is optional for 0120 AFD completion advice. See *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 <sup>15</sup>	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 <sup>15</sup>	F	n-1
8 Longitudinal Redundancy Check <sup>15</sup>	F	n-1

Refer to the *Security Rules and Procedures* for additional Track 2 data information.

## 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.

<sup>15</sup> These fields are encoded on the card but must be omitted within Track 2 data.

---

Attributes

---

Data Representation: ans...104; LLLVAR

---

Length Field: 2

---

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

---

Data Representation: an-12

---

Length Field: 2

---

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
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.)

**Visa Transactions:** Acquirers that use the Mastercard 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.

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.

---

#### 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.

---

#### 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

Data Representation:	ans-6
Length Field:	N/A
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, all high values, or all zeros.

### 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 special characters.
Visa	6	alphanumeric, with no special characters.
American Express	6	alphanumeric, trailing space(s).
Diners Club	6	numeric, trailing space(s).
Discover	6	numeric, trailing space(s).

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.

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)
- C—Level 1 (Small Business Spend Processing)
- D—Level 1 (Small Business Spend Processing and Product Graduation)
- E—Level 2 (Small Business Spend Processing)
- F—Level 2 (Small Business Spend Processing and Product Graduation)
- G—Level 3 (Small Business Spend Processing)
- H—Level 3 (Small Business Spend Processing and Product Graduation)
- J—Level 4 (Small Business Spend Processing)
- K—Level 4 (Small Business Spend Processing and Product Graduation)
- M—Enhanced Value (Enhanced Value and High Spend) and Product Graduation
- P—Product Graduation (or the Co-brand Proprietary card program)
- Q—Level 5 (Small Business Spend Processing)
- R—Level 5 (Small Business Spend Processing and Product Graduation)
- S—High Value and Premium High Spend
- T—High Value and Product Graduation
- W—Spend Shortfall
- Y—Spend Shortfall and Product Graduation
- 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.

---

## 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**

---

Data Representation:	an-2
----------------------	------

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

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

---

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 following information applies to purchase only, no cash back allowed responses from an issuer.

The issuer must provide...	The acquirer will receive...
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 (Additional Amounts) cash back amount and, if applicable, DE 28 (Amount, Transaction Fee) 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.	The purchase-only approval amount in the acquirer's transaction currency in DE 4  DE 38  DE 39, value 87  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.
DE 38 (Authorization ID Response)	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.
DE 39 value 87 (Purchase only, no cash back allowed)	
DE 51 (Currency Code, Cardholder Billing) with the issuer's cardholder billing currency code	
IF the issuer provides a response code value of...	THEN the Authorization Platform...
87 (Purchase Amount Only, No Cash Back Allowed) in the Authorization Request Response/0110 (applies to Mastercard only)	Requires that the amounts in DE 28 (Amount, Transaction Fee) and DE 54 (Additional Amounts) are subtracted from DE 6 (Amount, Cardholder Billing).
IF the issuer provides a response code value of...	THEN the Issuer Processing System (IPS)...

---

30 (Format Error) in the Authorization Request Response/0110 message	Also provides DE 44 with six positions for data element and subelement format errors (For example, 0480nn for DE48 subelement nn), or three positions if no subelements are present (For example, 022 for DE 22).
--	---

---

The Authorization Platform responds as indicated for Mastercard transactions only.

---

<b>IF the issuer provides a response code value of...</b>	<b>THEN the Authorization Platform...</b>
91, 92, or 96 in the Authorization Request Response/0110 (applies to Mastercard only)	Automatically invokes Stand-In processing. The Stand-In System 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.
<b>Invalid values in DE 39 for a Mastercard ATM transaction...</b>	<b>Instead, the issuer should use the following response code...</b>
01, 03, 08, 12, 15, 63, 76, 77, or 87	57
78	14
84 or 94	Any valid response code
<b>WHEN the acquirer or issuer...</b>	<b>THEN the Authorization Platform...</b>
Sends a Network Management/0800 group sign-off message (DE 70 = 062 or 064) within three minutes of the previous 0800 message for the same sign-on Member Group ID (DE 2 —Primary Account Number [PAN])	Generates the Network Management Response/0810 message where DE 39 (Response Code) = 96 (System error).

---

## Authorization Request Response/0110 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	✓	✓	✓	✓	✓

<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	✓	✓		✓	✓

<sup>16</sup> Issuers should use this response code only when no other reason code applies.

<sup>17</sup> Issuers should use this response code when their host blocks transactions based on specific transaction processing or fraud rules.

<sup>18</sup> Issuers may also use this response code for transaction types other than ATM.

<sup>19</sup> Issuers may also use this response code for transaction types other than ATM transactions. Issuers that opt to decline a contactless or card-not-present transaction and obtain a cardholder verification through a second transaction may use this response code. Refer to the *M/Chip Requirements for Contact and Contactless* manual for more details on contactless transactions and how to use response code 65. E-commerce merchants should trigger an authentication using Mastercard Identity Check/Mastercard SecureCode following an authorization decline with response code 65.

<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	✓	✓	✓	✓	✓
81	=	Domestic Debit Transaction Not Allowed (Regional use only)	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 System 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.

<sup>20</sup> Refer to the Canada Region Debit Mastercard Merchant Acceptance section in the Program and Service Format Requirements chapter of this manual for details on the use of this response code for Canada-acquired transactions.

<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	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓

<sup>21</sup> Issuers may also use this response code for transaction types other than ATM transactions. Issuers that opt to decline a contactless or card-not-present transaction and obtain a cardholder verification through a second transaction may use this response code. Refer to the *M/Chip Requirements for Contact and Contactless* manual for more details on contactless transactions and how to use response code 65. E-commerce merchants should trigger

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
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		✓			
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 System 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.

<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	—	✓	✓	✓	✓	✓
12	=	Invalid transaction	—	✓	✓	✓	✓	✓
14	=	Invalid card number	—	✓			✓	✓

an authentication using Mastercard Identity Check/Mastercard SecureCode following an authorization decline with response code 65.

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
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.

<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	= Completed successfully	—	✓	✓	✓	✓	✓	✓

### Authorization Negative Acknowledgement/0190 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>
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.

<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	= Issuer File Update action completed successfully	—	✓	✓	✓	✓	✓	✓
25	= Unable to locate record on file (no action taken)	—	✓	✓	✓	✓	✓	✓
26	= Record not in active status	—	✓	✓	✓	✓	✓	✓
27	= Issuer File Update field edit error	—	✓	✓	✓	✓	✓	✓
28	= Record permanently deleted	—	✓	✓	✓	✓	✓	✓

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
29	=	Delete request less than 540 days	—	✓	✓	✓	✓	✓
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.

<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 (/0400 only)	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 (/0400 only)	Decline	✓			✓	✓
30	=	Format error	Decline	✓	✓	✓	✓	✓
32	=	Partial reversal (/0400 only)	Decline	✓			✓	✓
34	=	Suspect Fraud (/0400 only)	Decline	✓	✓		✓	
41	=	Lost card	Capture	✓	✓	✓	✓	✓

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
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 (/0400 only)	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	✓	✓		✓	✓

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
91	=	Authorization System 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.

<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	✓	✓	✓	✓	✓
76	=	Invalid/nonexistent "To Account" specified	Decline	✓	✓	✓	✓	✓
77	=	Invalid/nonexistent "From Account" specified	Decline	✓	✓	✓	✓	✓
91	=	Authorization System or issuer system inoperative	Decline	✓	✓	✓	✓	✓
92	=	Unable to route transaction	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>
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	✓	✓	✓	✓	✓	✓
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	✓	✓	✓		✓	✓

<b>Values</b>		<b>Action</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
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	✓	✓		✓	✓
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	✓	✓		✓	✓
		Valid for zero amount transactions.						
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 System or issuer system inoperative	Decline	✓	✓	✓	✓	✓
92	=	Unable to route transaction	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>
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.

<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 System or issuer system inoperative	Resubmit request	✓	✓			
92	=	Unable to route transaction	Determine error and resubmit request	✓	✓			

Values	Action	MC	NP	VI	TE	MS	CI
96 = System error	Resubmit request	✓	✓				

## Network Management Request Response/0810 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	—	✓	✓	✓	✓	✓	✓
30 = Format error	—	✓	✓	✓	✓	✓	✓
63 = Security violation	—	✓	✓	✓	✓	✓	✓
79 = Key Exchange Validation failed	—	✓	✓	✓	✓	✓	✓
91 = Authorization System 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

Data Representation: an-3

Length Field: N/A

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

Data Representation: ans-8

Length Field: N/A

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.

---

## 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

---

Data Representation: ans-15

---

Length Field: N/A

---

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
Administrative Advice/0620	•	C	C

### 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).

#### American Express Authorizations:

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 10-digit SE number in character format should be left justified and followed by trailing spaces. This 10-digit number also should pass the Modulus 9 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	Sends the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or a Reversal Request Response/0410 message where: <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

---

Data Representation: ans-40 (supports extended character sets)

---

Length Field: N/A

---

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	•
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.

---

### **Subfield 1—Card Acceptor Name (or Payment Facilitator & Sub-Merchant Information, if applicable)**

DE 43 (Card Acceptor Name/Location for All Transactions), subfield 1 (Card Acceptor 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 Mastercard® rePower transaction must have the value: MC rePower following the carrier name.

---

### Application Notes

---

The following are rules for DE 43, subfield 1 (Card Acceptor Name [or Payment Facilitator & Sub-Merchant Information, if applicable]):

- The Card Acceptor Name should contain the same name as imprinted or printed on the transaction information document (TID)—the name most recognizable to the cardholder.
  - Acquirers must identify a merchant chain/franchise by providing either DE 48, subelement 32 (Mastercard Assigned ID) with the ID assigned to the chain/franchise, or by providing the chain/franchise name in DE 43, subfield 1 (Card Acceptor Name). If the merchant is part of a chain/franchise name, acquirers must provide the recognizable name in DE 43, subfield 1 and must provide DE 48, subelement 32 to reflect the chain or franchise identification. Whenever an acquirer has been provided a Mastercard Assigned ID for a merchant customer, they must identify that merchant by providing DE 48, subelement 32.
  - The Card Acceptor Name must contain the chain/franchise merchant name at the beginning of this subfield. If a chain is listed in the 3000–3999 range of card acceptor business codes (MCCs), use the exact chain name. If the merchant is part of a chain/franchise and the cardholder would not recognize the chain/franchise name, populate the recognizable name in DE 43, subfield 1, and provide DE 48, subelement 32 (Mastercard Assigned ID). A chain/franchise merchant is one of multiple merchant outlets selling the same line of goods or services, or authorized to sell a company’s goods or services in a particular place. This mandate will not be associated with any edits in Authorization System; instead, it will be monitored and edited in the Authorization Data Integrity Monitoring Program.
  - The Card Acceptor Name should contain a unique identifier at the end of this subfield following the Card Acceptor Name/DBA Name if the merchant has more than one property in a city.
- 

**NOTE: The acquirer must ensure that the name of the payment facilitator appears in DE 43, subfield 1 in conjunction with the name of the sub-merchant. The payment facilitator name, in full or in abbreviated form, must be followed by an asterisk and the sub-merchant name. DE 43, subfields 3 and 5 must contain the location information of the sub-merchant, not the payment facilitator.**

---

---

## 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
<b>Value</b>	
Delimiter (space).	

## Subfield 3—Card Acceptor City (or Sub-Merchant Information, if applicable)

DE 43 (Card Acceptor Name/Location for All Transactions), subfield 3 (Card Acceptor City) indicates the city of the merchant.

Attributes	
Data Representation:	ans-13
Data Field:	Contents of positions 24–36
Justification:	Left
<b>Values</b>	
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
<b>Value</b>	
Delimiter (space).	

---

### Subfield 5—Card Acceptor State or Country Code (or Sub-Merchant Information, if applicable)

DE 43 (Card Acceptor Name/Location for All Transactions), subfield 5 (Card Acceptor State or Country Code [or Sub-Merchant Information, if applicable]) 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

---

Data Representation: ans-40 (supports extended character sets)

---

Length Field: N/A

---

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	•
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

Justification: N/A

**Value**

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

---

#### Values

---

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

---

#### Value

---

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

---

#### Values

---

U.S. 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 *Quick Reference Booklet* 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

---

Data Representation: ans-40 (supports extended character sets)

---

Length Field: N/A

---

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
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 initiating the transaction.

---

### **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
<b>Values</b>	
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
<b>Values</b>	
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
<b>Values</b>	
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, DE 44 will contain either a three- or six-digit value that indicates the data element number (three digits) only or the data element plus subelement numbers (six digits) in which the format error occurred. If the format error occurred in a data element that does not have subelements, DE 44 will contain a three-digit numeric value.

### Attributes

Data Representation: ans...25; LLVAR

Length Field: 2

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
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—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.

---

<b>IF DE 39</b>		<b>is...</b>	<b>THEN DE 44...</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
00	N/A								
01			Contains the phone number for “call issuer” response codes. Applies to Authorization Request Response/0110 messages.	√	√	√	√	√	√
08			Contains the ID information for “approve with ID” response codes for example: <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> Applies to Authorization Request Response/0110 messages.	√	√	√	√	√	√

---

<b>IF DE 39</b>	<b>is... THEN DE 44...</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
12	Should be accessed when the value 12 is present in DE 39 for Mastercard Corporate Fleet Card® transactions only as follows: <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> Applies to Authorization Request Response/0110 messages.	✓					
25	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.	✓	✓	✓	✓	✓	✓
27	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.	✓	✓	✓	✓	✓	✓
30	Contains either the data element/subelement when a format error is detected (for example, 022 for DE 22, or 0480nn for DE48 [subelement nn]). Applies to all response messages.	✓	✓	✓	✓	✓	✓
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.	✓	✓	✓	✓	✓	✓

---

<b>IF DE 39 is...</b>	<b>THEN DE 44...</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
85	Contains the date and time used in electronic commerce transactions, after which a cardholder may re-apply for a certificate. Format is YYYYMMDDHH. HH is the 24-hour military clock.	√	√		√		

---

## Authorization Platform Edits

The Authorization Platform will perform the following system edit.

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
An Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or Reversal Request/0400 message contains one or both of the following: <ul style="list-style-type: none"> <li>• DE 48 (Additional Data—Private Use), DE 108 (MoneySend Reference Data), or DE 112 (Additional Data [National Use]) with subelements that have incorrect length and/or incorrect format (Data Representations)</li> <li>• Multiple instances of the same subelement (when not permitted) in DE 48</li> </ul>	Rejects the message and forwards the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 message where DE 44 is 6 positions for subelement format errors: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Message format error)</li> <li>• DE 44 (Additional Response Data) = 0480nn, or 1080nn, or 1120nn (where nn is the subelement number)</li> </ul> (DE 44 is three positions for Dual Message System (Authorization) if no subelements are present, for example, for DE 22 format error: DE 44 = 022)

---

Examples:

- When an edit error occurs on DE 48, the DE 44 data will be populated as these examples below:
  - Error on DE 48 subelement 42, subfield 1: 048042 (no subfield information is provided)
  - Error on DE 48 subelement 61: 048061
- DE 48 TCC format error will be responded with DE 44 = 048000.

For non-DE 48/DE 108/DE 112 format errors, DE 44 will only have DE info and no subelement information. For example, the format error in DE 22 will have DE 44 as 022.

## 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

Data Representation: ans...76; LLVAR

Length Field: 2

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. Refer to *AFD Completion* for more information.

Field ID and Name	F = Fixed V = Variable	Maximum Length
1 Start Sentinel <sup>8</sup>	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 <sup>8</sup>	F	n-1
11	Longitudinal Redundancy Check <sup>8</sup>	F	n-1

---

Refer to the *Security Rules and Procedures* for additional Track 1 data information.

---

## 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

---

Data Representation:	ans...999; LLLVAR
Length Field:	3
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

---

Data Representation:	ans...999; LLLVAR
	Although this data element is ans, some subelements deviate from ans and contain binary data. 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.

---

---

Length Field:	3
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.
- For subelements defined with a CE (conditional echo) presence notation for an Org (originator) entity Mastercard will not reject a message from the message originator if the original subelement data is not returned as defined in a response message. Based on the presence notation for the Dst (destination) entity Mastercard will forward the subelement data as received from the message originator if it is present in a response message.

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	X	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
Reversal Request Response/0410	ME	•	ME
Reversal Advice/0420	•	C	C
Administrative Advice/0620	•	C	C
Network Management Request/0800—PEK Exchange	•	O	C
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 for POS transactions as defined in the *Quick Reference Booklet*.

<b>TCC</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
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	√	√	√	√	√	
H	Hotel/Motel	√	√	√	√	√	
O	Hospitalization, College	√	√	√	√	√	
P	Payment Transaction	√	√			√	√
R	Retail Sale	√	√	√	√	√	√

TCC	Description	MC	NP	VI	TE	MS	CI
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 Network may choose to have the Authorization Platform assign the TCC in authorization messages on their behalf, if TCC is submitted with a <space> value.**

Refer to the *Quick Reference Booklet* for a complete definition of all TCC values.

## 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.

<b>"VAR"—999 maximum bytes (TCC + Subelement Data)</b>							
LLL	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	<b>First Subelement (SE) Data</b>		<b>Second Subelement (SE) Data</b>			
		SE ID	SE Length	SE Variable Length Data	SE ID	SE Length	SE Variable Length Data
<b>mandatory</b>							
<b>1002 maximum bytes (LLL + TCC + Subelement Data)</b>							

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

Number of Bytes	Attribute	Description
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 following table 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	<b>First Subelement (SE) Data</b>			<b>Second Subelement (SE) Data</b>		
	SE ID	SE Length	SE Variable Length Data	SE ID	SE Length	SE Variable Length Data
<b>1002 maximum bytes (LLL + Subelement Data)</b>						

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.

Subelement ID and Name	Data Representation
10      Encrypted PIN Block Key	an...16
11      Key Exchange Block Data (Double-length Keys)	an-54
11      Key Exchange Block Data (Triple-length Keys)	an-70

---

<b>Subelement ID and Name</b>	<b>Data Representation</b>
12 Routing Indicator	a-1
13 Mastercard Hosted Mobile Phone Top-up Request Data	ans-47
14 Account Type Indicator	ans-1
15 Authorization Platform Advice Date and Time	n-10
16 Processor Pseudo ICA	n-7
17 Authentication Indicator	n-1
18 Service Parameters	ans...99
19 Reserved for Future Use	N/A
20 Cardholder Verification Method	a-1
21 Acceptance Data	n-5; LLVAR
22 Reserved for Future Use	N/A
23 Payment Initiation Channel	an-2
25 Mastercard Cash Program Data	ans...14
26 Wallet Program Data	an-3
27 Additional Transaction Analysis	an...97
28 Cardless ATM Order ID	an-10
29 Additional POS Terminal Locations	an-1
30 Token Transaction Identifier	ans...64
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 Contactless Non-Card Form Factor Request/Response	an-1
36 Visa MVV (Visa Only)	an-14
37 Additional Merchant Data	ans...49
38 Account Category	an-1
39 Account Data Compromise 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

<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 and American Express)	b-20
45 Visa 3-D Secure Electronic Commerce Transaction Response Code (Visa and American Express)	an-1
46 Product ID (Visa Only)	an-2
47 Mastercard Payment Gateway Indicator	ans...8
48 Mobile Program Indicators	n-1
49 Time Validation Information	n-15
50 Reserved for Future Use	N/A
51 Merchant On-behalf Services	ans...99
52 Transaction Integrity Class	an-2
53 E-ID Request Code	ans...99; LLVAR
54 Reserved for Future Use	N/A
55 Merchant Fraud Scoring Data	an...32
56 Security Services Additional Data for Issuers	an...99
57 Security Services Additional Data for Acquirers	an...99
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 Reserved for Future Use	N/A
66 Authentication Data	ans...45; LLVAR
67–70 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

<b>Subelement ID and Name</b>	<b>Data Representation</b>
76 Mastercard Electronic Acceptance Indicator	a-1
77 Funding/Payment Transaction Type Indicator	an-3
78 Payment Service Indicators (Visa Only)	ans-6
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
84 Merchant Advice Code	an-2
84 Visa Response Codes (Visa Only)	an-2
85 Account Status (Visa Only)	a-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)	ns-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

<b>Subelement ID and Name</b>		<b>Data Representation</b>
98	Mastercard Corporate Fleet Card® ID/Driver Number	n...6; LLVAR
99	Mastercard Corporate Fleet Card® Vehicle Number	n...6; LLVAR

## **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
Data Representation:	an...16
Length Field:	2
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 (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
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

---

Data Representation: an-70

---

Length Field: 2

---

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 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
Data Representation:	a-1
Length Field:	2
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
Data Representation:	ans-47
Length Field:	2
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 (Mobile Phone Number) 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.

---

**Subfield 2—Mobile Phone Service Provider Name**

DE 48, subelement 13, subfield 2 (Mobile Phone Service Provider Name) 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 14—Account Type Indicator**

DE 48, subelement 14 (Account Type Indicator) contains values that identify the cardholder's intention to process the transaction as Credit or Debit. Subelement 14 must only be included on Brazil Combo card transactions.

---

### Attributes

Subelement ID	14
Data Representation	ans-1
Length of Field	2
Data Field	Contents of position 1
Subfields	N/A
Justification	N/A

---

### Usage

Following is the usage of subelement 14 (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
Authorization Advice/0120	C	•	C
Reversal Request/0400	C	•	C

---

### Values

C = Credit Transaction

D = Debit Transaction

---

### Application Notes

Subelement 14 (Account Type Indicator) is used in Brazil to identify the transaction as:

- Credit: (Credit/Mastercard). The transaction will be processed by the Dual Message System with a Mastercard credit brand/product.
- Debit: (Debit/Mastercard). The transaction will be processed by the Dual Message System as a Debit Mastercard transaction with a Mastercard debit brand/product.

The Mastercard Network will use the combination of the Account type indicator contained in DE 48, subelement 14 and the “from account type” value contained in DE 3 (Processing Code), subfield 2 (Cardholder “From” Account Type Code) to determine the issuer host destination for the authorization request messages.

---

## 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 that 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

---

Data Representation: n-10

---

Length Field: 2

---

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 message 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 message 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

---

Data Representation:

n-7

---

Length Field:

2

---

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 17—Authentication Indicator**

DE 48, subelement 17 (Authentication Indicator) is defined by the Authorization Platform and is passed to the issuer to indicate that the transaction qualified for Authentication service.

	<b>Attribute</b>	<b>Value</b>
Subelement ID	n-2	17
Subelement Length	n-2	01
Data Representation	n-1	
Number of Subfields	N/A	

### **Usage**

Following is the usage of subelement 17 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Authorization Request/0100	•	X	C
Authorization Request Response/0110	•	X	C
Authorization Advice/0120—Acquirer-generated	•	X	C
Authorization Advice/0120—System-generated	•	X	C
Authorization Advice Response/0130—Issuer-generated (Responding to Acquirer-generated 0120)	•	X	C

<b>Value</b>	<b>Description</b>
1	Transaction qualified for Authentication Service Type 1
2	Transaction qualified for Authentication Service Type 2

### **Application Notes**

#### **Cardholder Authentication Service**

Acquirers must support receiving subelement 17 in authorization response messages.

Issuers that have registered for or are already participating in the Cardholder Authentication Service must be prepared to receive the valid cardholder authentication result in subelement 17.

## **Subelement 18—Service Parameters**

DE 48, subelement 18 (Service Parameters) defines the service parameters of the transaction.

<b>Attributes</b>	
Subelement ID:	18
Data Representation:	ans...99; LLVAR

Length Field:	2
Data Field:	Contents of subfield 01
Subfields:	01
Justification:	N/A

### Usage

Following is the usage of subelement 18 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages.

Org      Sys      Dst

Authorization Request/0100	C	X	•
----------------------------	---	---	---

### Values

Contains the Canada Domestic Indicator value in subfield 01.

### Application Notes

Refer to the Canada Region Debit Mastercard Merchant Acceptance section in the Program and Service Format Requirements chapter of this manual for additional details on the use of subelement 18 for Canada-acquired transactions.

## Subfield 01—Canada Domestic Indicator

DE 48, subelement 18, subfield 01 (Canada Domestic Indicator) indicates the merchant accepts Canada domestic Debit Mastercard cards.

### Attributes

Subfield ID:	01
Data Representation:	an-1
Length Field:	2
Data Field:	Contents of subfield 01
Justification:	N/A

### Values

Y = Yes, the merchant accepts Canada domestic Debit Mastercard cards.

Example: 18050101Y—subelement 18 (Service Parameters), length 05, subfield 01 (Canada Domestic Indicator), length 01, value Y.

**NOTE: The remaining 94 characters are reserved for future use.**

## 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 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	•
Reversal Advice/0420	•	M	M

### Values

P	=	Online PIN verification
S	=	Can signify signature, “Offline PIN verification” (for chip transactions), “M-PIN” (for Mobile Device with PIN entry capability) or “No CVM used”

## Subelement 21—Acceptance Data

DE 48 (Additional Data—Private Use), subelement 21 (Acceptance Data) indicates the merchant terminal’s capability to support specific programs and services.

Attribute	Value
Subelement ID	n-21
Subelement Length	n-2
Data Representation	n...11; LLVAR
Data Field	Contents of subfields

<b>Attribute</b>	<b>Value</b>
Number of Subfields	2

### **Usage**

Following is the usage of subelement 21 (whether it is mandatory, conditional, optional, system-provided, or not required) in applicable messages.

<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Authorization Request/0100	O	•	C
Authorization Advice/0120—Acquirer-generated	O	•	C

### **Values**

See Subfield

### **Application Notes**

The subelement should be provided to indicate the merchant terminal's capabilities in supporting specific programs and services.

### **Subfield 01—mPOS Acceptance Device Type**

DE 48 (Additional Data—Private Use), subelement 21 (Acceptance Data), subfield 01 (mPOS Acceptance Device Type) identifies the type of device used by the merchant as the terminal for accepting mPOS transactions.

<b>Attribute</b>	<b>Description</b>
Subfield ID	01
Data Representation	n-1
Length Field	2
Data Field	Contents of subfield 1
Justification	N/A

<b>Values</b>	<b>Description</b>
0	Dedicated mPOS Terminal with PCI compliant dongle (with or without key pad)
1	Off the Shelf Mobile Device
2–9	Reserved for Future Use

### **Subfield 02—Additional Terminal Capability Indicator**

DE 48, subelement 21, subfield 2 (Additional Terminal Capability Indicator) identifies Mastercard Consumer Presented QR and barcode terminal capabilities. This subfield is optional. Customers that have opted to submit or process tokenized Mastercard Consumer Presented QR transactions are expected to support this subfield.

<b>Attribute</b>	<b>Value</b>
Subfield ID	n-2 02
Subfield Length	n-2 02
Data Representation	n...2; LLVAR
Data Field	Contents of positions 1–2
Justification	N/A
Position 1	Mastercard Consumer Presented QR Capability Support Indicator
Position 2	Mastercard Consumer Presented Barcode Capability Support Indicator

<b>Values</b>	<b>Description</b>
0	Not Supported
1	Supported

### **Subfield 2—Valid Position 1 and Position 2 Value Combinations**

<b>Valid Combinations</b>	<b>QR Capability</b>	<b>Barcode Capability</b>
00	Not supported	Not supported

Valid Combinations	QR Capability	Barcode Capability
01	Not supported	Supported
10	Supported	Not supported
11	Supported	Supported

### **Subelement 23—Payment Initiation Channel**

DE 48, subelement 23 (Payment Initiation Channel) provides information about the device type used to identify mobile-initiated (m-commerce) or other EMV Contact, Magnetic stripe Contactless, or M/Chip Contactless transactions.

Attribute	Description
Subelement ID:	23
Data Representation:	an-2
Length Field:	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	C	•	C
Authorization Advice/0120	C	•	C
Reversal Request/0400	C	•	C

#### **Values**

See subfield 1.

#### **Application Notes**

Acquirers in regions where it is mandated must ensure that each newly deployed or re-deployed contactless-enabled POS terminal used by their merchants transmits the device type indicator value, if present on the card or non-card form factor, in data element DE 48 (Additional Data—Private Use), subelement 23 (Payment Initiation Channel), subfield 1 (Device Type) of authorization messages.

---

### Subfield 1—Device Type

DE 48, subelement 23, subfield 1 (Device Type) indicates the type of device used at the terminal. In the scope of chip transactions it must be populated using the device type field value of chip tag 9F6E.

**NOTE: Effective immediately, new values in DE 48, subelement 23, subfield 1 contain an indication of the form factor. Existing values from 00–19 may continue to be used, and their meanings remain unchanged; however, Mastercard will not send these values in future communication as part of DE 48, subelement 23, subfield 1. New values from 20–99 exclusively indicate the form factor only without also indicating the storage technology. Mastercard has introduced new device type values from 20–33 in anticipation of new form factors for payments, with values 34–99 reserved for future use. For information on storage technology of device types (such as Trusted Execution Environment [TEE] or Secure Element), refer to the description of DE 48, subelement 33 (PAN Mapping File Information), subfield 8 (Storage Technology).**

Attribute	Description
Data Representation:	an-2
Data Field:	Contents of positions 1–2
Justification:	N/A
Values	

**NOTE: Some values from 00–19 may indicate not only the physical form factor but also other attributes such as device technology and payment app specifications.**

00 = Card

01 = Mobile Network Operator (MNO) controlled removable secure element (SIM or UICC) personalized for use with a mobile phone or smartphone

02 = Key Fob

03 = Watch using a contactless chip or a fixed (non-removable) secure element not controlled by the MNO

04 = Mobile Tag

05 = Wristband

06 = Mobile Phone Case or Sleeve

07 = Mobile phone or smartphone with a fixed (non-removable) secure element controlled by the MNO, for example, code division multiple access (CDMA)

08 = Removable secure element not controlled by the MNO, for example, memory card personalized for used with a mobile phone or smartphone

09 = Mobile Phone or smartphone with a fixed (non-removable) secure element not controlled by the MNO

10 = MNO controlled removable secure element (SIM or UICC) personalized for use with a tablet or e-book

11 = Tablet or e-book with a fixed (non-removable) secure element controlled by the MNO

12 = Removable secure element not controlled by the MNO, for example, memory card personalized for use with a tablet or e-book

13 = Tablet or e-book with fixed (non-removable) secure element not controlled by the MNO

14 = Mobile phone or smartphone with a payment application running in a host processor

15 = Tablet or e-book with a payment application running in a host processor

16 = Mobile phone or smartphone with a payment application running in the Trusted Execution Environment (TEE) of a host processor

17 = Tablet or e-book with a payment application running in the TEE of a host processor

18 = Watch with a payment application running in the TEE of a host processor

19 = Watch with a payment application running in a host processor

**NOTE: Values from 20–99 exclusively indicate the form factor only without also indicating the storage technology.**

Value	Meaning	Example
-------	---------	---------

---

20	Card	
21	Phone	Mobile phone
22	Tablet/e-reader	Tablet computer or e-reader
23	Watch/Wristband	Watch or wristband, including a fitness band, smart strap, disposable band, watch add-on, and security/ID band
24	Sticker	
25	PC	PC or laptop
26	Device Peripheral	Mobile phone case or sleeve
27	Tag	Key fob or mobile tag
28	Jewelry	Ring, bracelet, necklace, and cuff links
29	Fashion Accessory	Handbag, bag charm, and glasses
30	Garment	Dress
31	Domestic Appliance	Refrigerator, washing machine
32	Vehicle	Vehicle, including vehicle attached devices
33	Media/Gaming Device	Media or gaming device, including a set top box, media player, and television
34–99	Reserved for future form factors. Any value in this range may occur within form factor and transaction data without prior notice.	

---

## **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	
Subelement ID:	25
Data Representation:	ans...14; LLVAR
Length Field:	2
Data Field:	Contents of subfields
Subfields:	1
Justification:	See subfields
<b>Usage</b>	

---

---

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.

Attribute	Description
Subfield ID:	01
Data Representation:	ans...10; LLVAR
Length Field:	2
Data Field:	Contents of positions 1–2, positions 3–10 undefined
Justification:	N/A

#### **Values**

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 26—Wallet Program Data**

DE 48 (Additional Data—Private Use), subelement 26 (Wallet Program Data) contains the subfield that will identify transactions submitted using wallets on the Mastercard Digital Enablement Service (MDES) or Masterpass platform. Subelement 26 must be present in all Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, and Authorization Advice/0120—System-generated messages for transactions processed using wallets on MDES or the Masterpass™ by Mastercard® platform.

Attribute	
Subelement ID:	26
Data Representation:	an-3
Length Field:	2

---

Data Field:	Contents of subfield 1
-------------	------------------------

Subfields:	1
------------	---

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

### **Usage**

Following is the usage of subelement 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—System-generated	•	C	C
--	---	---	---

### **Values**

---

See subfield 1
----------------

### **Subfield 1—Wallet Identifier**

DE 48, subelement 26, subfield 1 (Wallet Identifier) provides information about transactions initiated through the Masterpass Online platform or through the Mastercard Digital Enablement Service (MDES) and indicates who the Wallet Provider was for the transaction.

---

Attribute	Description
-----------	-------------

Data Representation:	an-3
----------------------	------

Data Field:	Provides the Wallet Identifier
-------------	--------------------------------

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

### **Values**

---

Value	Description
-------	-------------

**Note: The following values apply to both Masterpass and MDES transactions.**

101	Masterpass by Mastercard
-----	--------------------------

**Note: The following values only apply to MDES transactions.**

103	Apple Pay
-----	-----------

216	Google Pay
-----	------------

217	Samsung Pay
-----	-------------

327	Merchant tokenization program
-----	-------------------------------

---

### **Application Notes**

---

The Wallet ID is now required in Masterpass transactions submitted from certain regions or countries. The Wallet ID cannot contain all zeros, spaces, or special characters.

The Authorization Platform inserts the Wallet Identifier for MDES transactions when available, which identifies the wallet that the transaction came from.

New Wallet Identifier values may be provided in this field without prior written notice.

---

The following table indicates the presence of the Wallet Identifier in Masterpass and MDES transactions.

<b>Masterpass Messages</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Authorization Request/0100	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C

#### **Application Notes**

If the card in Masterpass is an MDES token, then MDES would add the correct Wallet ID to the transaction.

---

<b>MDES Messages</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Authorization Request/0100	•	X	C
Authorization Advice/0120—Acquirer-generated	•	X	C
Authorization Advice/0120—System-generated	•	X	C
Reversal Request/0400	•	X	C
Reversal Advice/0420	•	X	C

#### **Application Notes**

For MDES, Mastercard inserts the Wallet Identifier for the wallet that the token was supplied to.

---

### **Subelement 27—Transaction Analysis**

DE 48, subelement 27 (Transaction Analysis) contains information about transaction analysis.

<b>Attribute</b>	<b>Value</b>
Subelement ID	n-2

---

Subelement Length	n-2	13...97
Data Representation	an...97; LLVAR	
Data Field	Contents of subfields 1–2	
Number of Subfields	2	

### Usage

Following is the usage of subelement 27 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

Message	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Advice/0120—System-generated	C	•	C

### Application Notes

DE 48, subelement 27 and subfields 1 and 2 are set up in Tag, Length, Value format:  
27LL01LLVV02LLVVVVVVV... For example, see as follows:

Subfield 1	Subfield 2
0102CI	0206SNAOVP

### Subfield 1—Overview

DE 48, subelement 27, subfield 1 (Overview) provides issuers with a code that represents the overall disposition of the transaction based on the applicable transaction validation results and corresponding decision matrix.

---

Attributes	
Subfield ID	01
Data Representation	an-2
Subfield Length	2
Data Field	Contents of subfield 1
Justification	N/A

---

Values	Description
CI	Continue processing with information
CW	Continue processing with warning
DI	Decline issuer decision

<b>Values</b>	<b>Description</b>
DS	Decline suspicious

### **Subfield 2—Test Results**

DE 48, subelement 27, subfield 2 (Test Results) provides the list of failed validations. If several failed validations generate the same test result code, the code will only be reported one time in subfield 2.

<b>Attribute</b>	<b>Value</b>
Subfield ID	02
Data Representation	an...87; LLVAR; The LL length field of LLVAR will be an integral multiple of 3, not to exceed 87.
Subfield Length	2
Data Field	Contents of subfield 2
Justification	N/A

<b>Values</b>	<b>Description</b>
CAM	Invalid Card Authentication
CCH	Cross channel
CRN	Consent requirement not fulfilled
CVF	Cardholder verification (on terminal) was not successful
CVU	CVM requirements not fulfilled
CVX	Status CVM unknown
DAF	ODA failed
DAU	ODA was not performed
DMM	Data mismatch
DNC	Data not consistent with application or product
EXP	Token expired
FER	Format error
FUZ	Fuzzing
ICT	Not a valid cryptogram type
NMK	No matching key file/KDI combination

<b>Values</b>	<b>Description</b>
OVE	CDCVM retry exceeded—token suspended
OVF	CDCVM failed
OVP	CDCVM (was possible but) not performed
OVU	CDCVM not performed
PKC	ODA compromised
PPP	PIN Pad Problem
PTB	PIN on terminal bypass
PWE	Possible wedge attack
REP	ATC replay—Same UN
SKC	Key compromised
SNA	Request service not allowed for this product
UTP	Unable to process
WOC	Wallet overrule of Mastercard decision on CDCVM

### **Subelement 28—Cardless ATM Order ID**

Subelement 28 (Cardless ATM Order ID) is defined by the ATM operator, sent by the acquirer participating in the Cardless ATM program and passed to the issuer participating in the Cardless ATM program.

Attributes	
Subelement ID:	28
Data Representation:	an-10
Length Field:	2
Data Field:	Fixed length, contents of positions 1–10
Subfields:	N/A
Justification:	N/A

#### **Usage**

Following is the usage of subelement 28 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	X	C

#### **Values**

---

Cannot contain all spaces or all zeros.

---

### **Subelement 29—Additional POS Terminal Locations**

Subelement 29 is required when DE 61 (Point-of-Service [POS] Data), subfield 3 (POS Terminal Location) is present with the value of 8 (Additional Terminal Operating Environments).

---

#### Attributes

---

Subelement ID:	29
Data Representation:	an-1
Length Field:	2
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

---

#### Usage

---

Following is the usage of subelement 29 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	C	•	C

---

#### Values

---

A =	Transaction has been initiated remotely and completed at a physical terminal on premises of the card acceptor facility.
B =	Transaction has been initiated remotely and completed at a physical terminal off premises of the card acceptor facility.

---

### **Subelement 30—Token Transaction Identifier**

DE 48, subelement 30 (Token Transaction Identifier) will contain, when available, the calculated Token Transaction Identifier to identify the transaction. The Token Transaction Identifier is to be retained and used to provide the transaction details associated with an original purchase and subsequent reversal messages. The Token Transaction Identifier is only sent to issuers participating in the Mastercard Digital Enablement Service.

Attribute	Description	Value
Subelement ID	n-2	30
Subelement Length	n-2	44 or 64
Data Representation	ans...64; LLVAR	Variable
Number of Subfields	N/A	

### Usage

Following is the usage of subelement 30 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

Message	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Advice/0120—System-generated	•	X	C

### Values

A 44 byte base 64 value will be sent for Mastercard BIN ranges.

A 64 byte value will be sent for Visa BIN ranges.

### Application Notes

DE 48, subelement 30 will not be present when DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) contains a value of 20 (Purchase Return/Refund).

## Subelement 32—Mastercard Assigned ID

Subelement 32 (Mastercard Assigned ID) contains the merchant ID assigned by Mastercard.

### Attributes

Subelement ID:	32
Data Representation:	an-6
Length Field:	2
Data Field:	Contents of positions 1–6
Subfields:	N/A
Justification:	N/A

### Usage

Following is the usage of subelement 32 (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—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C
Reversal Advice/0420	•	C	C

### Values

The Mastercard Assigned ID must be a value assigned by Mastercard, and is the same value in both the Authorization and Clearing Platforms. Mastercard assigns one ID to the merchant regardless if the merchant is participating in multiple programs. This ID can also be assigned for transaction data integrity purposes. For all card acceptors that have been issued a Mastercard Assigned ID, all submitted authorization requests, reversals, and advices must contain the Mastercard Assigned ID in DE 48, subelement 32.

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]).

Participating merchants must submit the Mastercard Assigned ID for e-commerce transactions that are processed under 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
Data Representation:	an...93; LLVAR
Length Field:	2
Data Field:	Contents of subfields 1-8
Subfields:	8
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	C	X	C
Authorization Request Response/0110	C	X	C
Authorization Advice/0120—Acquirer-generated	C	X	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-generated	•	X	C
Authorization Advice Response/0130—Issuer-generated	CE	•	CE
Reversal Request/0400	C	X	C
Reversal Request Response/0410	CE	X	CE

---

Reversal Advice/0420	•	X	C
----------------------	---	---	---

### Values

See subfields

### Application Notes

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.

Acquirers will receive subelement 33 in contact M/Chip, contactless magnetic stripe, or contactless M/Chip transactions when the issuer is participating in the Contactless Mapping Service. Acquirers will also receive subelement 33 in contactless M/Chip, contactless magnetic stripe, magnetic stripe, or Digital Secure Remote Payment transactions when the issuer is participating in the Mastercard Digital Enablement Service. Acquirers do not receive subelement 33 for the Mastercard In Control™ Purchase Control Service or Mastercard In Control Virtual Card Spend Control Service.

Issuers that issue contactless cards or devices that provide a primary account number (PAN) within a transaction different from what is embossed on the card, must ensure that the following is provided in Authorization Request Response/0110 messages when responding to MCC 4111, 4131, 4784, 7523 transactions.

- The value E in DE 48, subelement 33, subfield 1 (Account Number Indicator)
- The embossed number in DE 48, subelement 33, subfield 2 (Account Number)
- The card expiration date of the embossed number in DE 48, subelement 33, subfield 3 (Expiration Date)

Acquirers processing transactions for merchant categories 4111, 4131, 4784, and 7523 must pass the PAN Mapping information back to the merchants.

---

### 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

Data Representation: an-1

Length Field: 2

Data Field: Contents of subfield 1

Justification: N/A

---

Values	Description
--------	-------------

---

C = Mastercard Digital Enablement Service Secure Element Token  
E = Embossed Account Number Provided by Issuer  
F = Mastercard Digital Enablement Service Card on File Token  
H = Mastercard Digital Enablement Service Cloud-based Payments Token  
L = Pay with Rewards Loyalty Program Operator [LPO] Card  
M = Primary Account Number  
P = Contactless 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 number.

---

#### **Attributes**

Subfield ID:	02
Data Representation:	n...19, LLVAR
Length Field:	2
Data Field:	Contents of subfield 2
Justification:	N/A

---

#### **Values                          Description**

Acquirer message = Contains primary account number

For Visa authorization transactions, subfield 2 contains the last four digits of the cardholder's primary account number (PAN) and will be provided when the transaction was initiated with a Visa token and the data is provided on the response from Visa.

---

Issuer message = Contains virtual number or token

For Mastercard Digital Enablement Service transactions, subfield 2 is the token rather than the primary account number, if subfield 1 value is C, H, or F.

---

### **Subfield 3—Expiration Date**

DE 48, subelement 33, subfield 3 (Expiration Date) indicates the expiration date of the PAN mapping account.

---

#### **Attributes**

---

Subfield ID:	03
Data Representation:	n-4; format YYMM
Length Field:	2
Data Field:	Contents of subfield 3
Justification:	N/A

---

#### Values

Acquirer message =	Will contain the expiration date when <ul style="list-style-type: none"> <li>• The issuer provided one for a PAN mapping record added to the MCC106 PAN Mapping File, or</li> <li>• A transit transaction response contains MCC 4111, 4131, 4784, and 7523, or</li> <li>• The Mastercard Digital Enablement Service was applied</li> </ul>
Issuer message =	May contain virtual card number or token expiration date only if acquirer provided in DE 14 of the authorization message.  For contactless 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.

---

#### Attributes

Subfield ID:	04
Data Representation:	an-3
Length Field:	2
Data Field:	Contents of subfield 4
Justification:	N/A

---

#### Values

Subfield 4 may contain product code for subfield 2 account number.

---

#### Subfield 5—Token Assurance Level

DE 48, subelement 33, subfield 5 (Token Assurance Level) contains a value indicating the confidence level of the token to PAN/cardholder binding.

---

Attributes

---

Subfield ID: 05

---

Data Representation: n-2

---

Length Field: 2

---

Data Field: Contents of subfield 5

---

Justification: N/A

---

**Values**

---

Contains a value indicating the confidence level of the token to PAN/cardholder relationship.

---

**Application Notes**

---

Subfield 5 is optional but should be included in messages sent to Mastercard by the acquirer if provided to the acquirer by the merchant. Acquirers may receive the value back in an Authorization Request Response/0110 message.

---

**Subfield 6—Token Requestor ID**

DE 48, subelement 33, subfield 6 (Token Requestor ID) contains the ID assigned by the Token Service Provider to the Token Requestor.

---

---

Attributes

---

Subfield ID: 06

---

Data Representation: n-11

---

Length Field: 2

---

Data Field: Contents of subfield 6

---

Justification: N/A

---

**Values**

---

Contains the ID assigned by the Token Service Provider to the Token Requestor. The Token Requestor ID is required for Card-on-File Token Request messages and is optional for all others.

---

**Application Notes**

---

Subfield 6 is optional but should be included in messages sent to Mastercard by the acquirer if provided to the acquirer by the merchant. Acquirers may receive the value back in an Authorization Request Response/0110 message.

---

### **Subfield 7—Primary Account Number, Account Range**

DE 48, subelement 33, subfield 7 (Primary Account Number, Account Range) carries either the first nine digits of the cardholder PAN, or the full Visa cardholder PAN in the authorization response for a transaction initiated with a Visa token.

---

#### **Attributes**

---

Subfield ID: 07

---

Data Representation: n...19; LLVAR

---

Length Field: 2

---

Data Field: Contents of subfield 7

---

Justification: N/A

---

#### **Values**

---

The first nine digits of the Visa cardholder PAN, or the full Visa cardholder PAN. Acquirers must be aware that this information must not be forwarded to their merchants.

---

### **Subfield 8—Storage Technology**

DE 48, subelement 33, subfield 8 (Storage Technology) describes the Storage Technology of a requested or created token.

---

#### **Attributes**

---

Subfield ID: 08

---

Data Representation: an-2

---

Length Field: 2

---

Data Field: Contents of subfield 8

---

Justification: N/A

---

#### **Usage**

---

Following is the usage of DE 48, subelement 33, subfield 8 (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—System-generated	•	X	C
Reversal Request/0400	•	X	C
Reversal Advice/0420	•	X	C

Authorization Request/0100—Tokenization Eligibility Request (TER)	•	X	C
Authorization Request/0100—Tokenization Authorization Request (TAR)	•	X	C
Authorization Request/0100—Tokenization Complete Notification (TCN)	•	X	C
Values	Description		
01	Device Memory		
02	Device Memory protected by Trusted Platform Module (TPM)		
03	Server		
04	Trusted Execution Environment (TEE)		
05	Secure Element (SE)		
06	Virtual Execution Environment (VEE)		

#### Application Notes

Subfield 8 is optional but should be included in messages sent to Mastercard by the acquirer if provided to the acquirer by the merchant. Acquirers may receive the value back in an Authorization Request Response/0110 message.

### Subelement 34—ATC Information

Subelement 34 (ATC Information) supports On-behalf Services.

#### Attributes

Subelement ID:	34
Data Representation:	an-11
Length Field:	2
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 Dynamic CVC 3 Pre-validation Service (OBS 15), Dynamic CVC 3 Validation in Stand-In Processing Service (OBS 16), M/Chip Cryptogram Pre-validation Service (OBS 02), or M/Chip Cryptogram Validation in Stand-In Processing Service (OBS 03) was performed on the transaction and the validation result was V (Valid), A (Valid AC; ATC outside allowed range), E (Valid AC; ATC Replay), T (Valid ARQC/TC and ATC; TVR/CVR invalid), or G (Application Cryptogram is valid but not an ARQC; status of TVR/CVR unknown).

#### **Chip Services**

- V = Valid ARQC/TC and ATC and TVR/CVR
- A = Valid Application Cryptogram; ATC out of range
- E = Valid Application Cryptogram; ATC replay
- T = Valid ARQC/TC and ATC; TVR/CVR invalid
- G = Application Cryptogram valid but not an ARQC; ATC valid; status of TVR/CVR unknown

#### **CVC Services**

- V = Valid CVC3 and ATC and TVR/CVR
- A = Valid CVC3; ATC out of range
- E = Valid CVC; 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.

The following ATC information will be provided in Dual Message (Authorization) and Single Message financial transaction requests and advices to issuers for MDES transactions initiated with a token, when available. ATC information will not be provided in declined advices.

- DE 48, subelement 34, subfield 1 (ATC Value)
  - DE 48, subelement 34, subfield 2 (ATC Discrepancy Value)
  - DE 48, subelement 34, subfield 3 (ATC Discrepancy Indicator)
- 

#### **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 Field: Contents of subfield 3

---

Justification: N/A

---

#### **Values**

---

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—Contactless Non-Card Form Factor Request/Response**

Subelement 35 (Contactless Non-Card Form Factor Request/Response) supports Contactless Mapping Service.

---

#### Attributes

Subelement ID:	35
Data Representation:	an-1
Length Field:	2
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
Authorization Request/0100	•	X	C
Authorization Request Response/0110	C	C	•

#### Values

The contactless issuer will receive the Authorization Request/0100 message containing DE 48, subelement 35, value R (Cardholder request for device).

The contactless 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 Contactless Mapping Service “Processing and Issuance of devices” participation option (Passive Participation) will receive an Authorization Request/0100 message when a cardholder requests a contactless device from the issuer-branded, secure website hosted by Mastercard. The issuer may then decide if the cardholder should receive the contactless device.

The Authorization Platform will use the value in DE 48, subelement 35 of the Authorization Request Response/0110 message to issue the contactless device or to decline the cardholder’s request.

If an issuer chooses not to support subelement 35, the issuer-branded website will evaluate the responses provided for AVS and CVC 2 and approve or decline the cardholder request based on those values.

---

### Subelement 36—Visa MVV (Visa Only)

DE 48, subelement 36 (Visa MVV [Visa Only]) supports the Visa-assigned Merchant Verification Value (MVV).

Attribute	Description

---

Subelement ID:	36
Data Representation:	a-14
Length Field:	2
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 (MVV)

DE 48, subelement 36, subfield 1 (Merchant Verification Value) contains the merchant verification value for subelement 36.

---

Attribute	Description
Subfield ID:	01
Data Representation:	an-10
Length Field:	2
Data Field:	Contents of subfield 1.
Justification:	N/A

---

Attribute	Description
Subfield ID:	01

---

### Values

0–9 and A–F

## Subelement 37—Additional Merchant Data

DE 48, subelement 37 (Additional Merchant Data) contains subfields representing the ID of the participating service provider in a transaction and the sub-merchant ID. The service provider can be a payment facilitator or independent sales organization.

---

Attribute	Description
Subelement ID:	37

---

---

Data Representation:	ans...49; LLVAR
Length Field:	2
Data Field:	Contents of subfields 1–3
Subfields:	3
Justification:	see subfields

---

### Usage

Following is the usage of subelement 37 (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

Specific application notes, conditions, and cross-edits where applicable.

### Valid Combinations of DE 48, subelement 37, subfields 1, 2, and 3:

- 
- Subfields 1 and 3 only
  - Subfield 2 only
  - Subfields 1, 2, and 3
- 

### Subfield 1—Payment Facilitator ID

DE 48, subelement 37, subfield 1 (Payment Facilitator ID) contains the Payment Facilitator ID assigned by Mastercard.

---

Attribute	Description
Subfield ID:	01
Data Representation:	n-11
Length Field:	2
Data Field:	Contents of subfield 1
Justification:	Right justified with leading zeros

---

### Values

---

The Payment Facilitator ID must always be a value assigned by Mastercard and must be the same value in both the Authorization and Clearing Platforms. This ID is the Company ID that will be assigned during the time of registration with Mastercard for a Service Provider as "Payment Facilitator."

The value must be provided by the acquirer when a registered payment facilitator is involved in a transaction and should be right justified with leading zeros. For example, if the Company ID is 123456, DE 48, SE 37, SF 1 should be 00000123456.

---

### **Subfield 2—Independent Sales Organization ID**

DE 48, subelement 37, subfield 2 (Independent Sales Organization ID) contains the Independent Sales Organization ID assigned by Mastercard.

Attribute	Description
Subfield ID:	02
Data Representation:	n-11
Length Field:	2
Data Field:	Contents of subfield 2
Justification:	Right justified with leading zeros

#### **Values**

The Independent Sales Organization ID must always be a value assigned by Mastercard and is the same value in both the Authorization and Clearing Platforms. This ID is the "Company ID" that is assigned during the time of registration via Mastercard Connect of a service provider as "Independent Sales Organization."

This value must be provided by the acquirer when a registered independent sales organization is involved in a transaction and should be right justified with leading zeros. For example, if the Company ID is 123456, DE 48, SE 37, SF 2 should be 00000123456.

---

### **Subfield 3—Sub-Merchant ID**

DE 48, subelement 37, subfield 3 (Sub-Merchant ID) contains the Merchant ID of the sub-merchant.

Attribute	Description
Subfield ID:	03
Data Representation:	ans-15
Length Field:	2
Data Field:	Contents of subfield 3
Justification:	Left justified, trailing spaces

---

### Values

The Sub-Merchant ID must always be the merchant ID of the sub-merchant whenever a payment facilitator is involved in a transaction. This value, which is assigned by the payment facilitator or their acquirer, must be provided by the acquirer whenever the Payment Facilitator ID is provided in the DE 48, SE 37 (Additional Merchant Data), SF 1 (Payment Facilitator ID).

## Subelement 38—Account Category

Subelement 38 (Account Category) supports Account Level Management.

---

### Attributes

Subelement ID:	38
Data Representation:	an-1
Length Field:	2
Data Field:	Contents of position 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
Reversal Advice/0420	•	C	C

---

### Values

B	=	Enhanced Value (Enhanced Value and High Spend)
C	=	Level 1 (Small Business Spend Processing)
D	=	Level 1 (Small Business Spend Processing and Product Graduation)
E	=	Level 2 (Small Business Spend Processing)
F	=	Level 2 (Small Business Spend Processing and Product Graduation)
G	=	Level 3 (Small Business Spend Processing)
H	=	Level 3 (Small Business Spend Processing and Product Graduation)
J	=	Level 4 (Small Business Spend Processing)
K	=	Level 4 (Small Business Spend Processing and Product Graduation)

---

M	=	Enhanced Value (Enhanced Value and High Spend) and Product Graduation
P	=	Product Graduation (or the Co-brand Proprietary card program)
Q	=	Level 5 (Small Business Spend Processing)
R	=	Level 5 (Small Business Spend Processing and Product Graduation)
S	=	High Value (High Value, Small Business Spend Processing and Premium High Spend)
T	=	High Value (High Value, Small Business Spend Processing and Premium High Spend) and Product Graduation
W	=	Spend Shortfall
Y	=	Spend Shortfall and Product Graduation
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.

---

Refer to the *Account Level Management User Manual* for additional information.

---

### **Subelement 39—Account Data Compromise Information**

DE 48, subelement 39 (Account Data Compromise Information) contains confirmed or suspected account data compromise event information for account ranges.

---

#### Attributes

Subelement ID:	39
Data Representation:	ans-30
Length Field:	2
Data Field:	Contents of positions 1–30
Subfields:	N/A
Justification:	Left

---

#### Usage

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 (Reserved for Future Use)

Data Representation:	n-3
----------------------	-----

---

---

Data Field: Contents of positions 1–3

Values: 000 = Not available

**Positions 4–6 (Reserved for Future Use)**

Data Representation: n-3

Data Field: Contents of positions 4–6

Values: N/A

**Positions 7–12 (Case Key Code number 1)**

Data Representation: ans-6

Data Field: Contents of positions 7–12

Values: Unique Key to Identify Case

**Positions 13–18 (Case Key Code number 2)**

Data Representation: ans-6

Data Field: Contents of positions 13–18

Values: Unique Key to Identify Case

**Positions 19–24 (Case Key Code number 3)**

Data Representation: ans-6

Data Field: Contents of positions 19–24

Values: Unique Key to Identify Case

**Position 25 (Account Number)**

Data Representation: n-1

Data Field: Contents of position 25

Values: 0–9 = Number of events in which the account number has been exposed

**Position 26 (Expiration Date)**

Data Representation: n-1

Data Field: Contents of position 26

Values: 0–9 = Number of events in which expiration date has been exposed

**Position 27 (CVC 2)**

Data Representation: n-1

Data Field: Contents of position 27

Values: 0–9 = Number of events in which the CVC 2 has been exposed

**Position 28 (PIN)**

---

Data Representation:	n-1
Data Field:	Contents of position 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 position 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 position 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
Data Representation:	n...40 (also contains binary data. See subfields.); LLVAR
Length Field:	2
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

---

Data Representation: b...16

---

Length Field: 2

---

Data Field: Merchant Certificate Serial Number in binary data.

---

Justification: 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.

---

Attributes

---

Subfield ID: 02

---

Data Representation: b...16

---

Length Field: 2

---

Data Field: Cardholder Certificate Serial Number in binary data.

---

Justification: 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

---

Data Representation:	ans...95; LLVAR
Length Field:	2 (value in the range of 05–95)
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
Data Representation:	ans...26
Length Field:	2

### Subfield 2—Reserved for Future Use

DE 48, subelement 41, subfield 2 (Reserved for Future Use) is for future use.

Attributes	
Subfield ID:	02
Data Representation:	n-6
Length Field:	2

### Subfield 3—Reserved for Future Use

DE 48, subelement 41, subfield 3 (Reserved for Future Use) is for future use.

Attributes	
------------	--

---

Subfield ID:	03
Data Representation:	n-3
Length Field:	2

---

#### **Subfield 4—Reserved for Future Use**

DE 48, subelement 41, subfield 4 (Reserved for Future Use) is for future use.

---

Attributes	
Subfield ID:	04
Data Representation:	an...22
Length Field:	2

---

#### **Subfield 5—Reserved for Future Use**

DE 48, subelement 41, subfield 5 (Reserved for Future Use) is for future use.

---

Attributes	
Subfield ID:	05
Data Representation:	ans...20
Length Field:	2

---

#### **Subfield 6—Reserved for Future Use**

DE 48, subelement 41, subfield 6 (Reserved for Future Use) is for future use.

---

Attributes	
Subfield ID:	06
Data Representation:	a...13
Length Field:	2

---

#### **Subfield 7—Reserved for Future Use**

DE 48, subelement 41, subfield 7 (Reserved for Future Use) is for future use.

---

Attributes	
Subfield ID:	07
Data Representation:	a-3

---

---

Length Field:	2
---------------	---

---

### **Subfield 8—Reserved for Future Use**

DE 48, subelement 41, subfield 8 (Reserved for Future Use) is for future use.

---

Attributes

---

Subfield ID:	08
--------------	----

---

Data Representation:	a...10
----------------------	--------

---

Length Field:	2
---------------	---

---

### **Subfield 9—Reserved for Future Use**

DE 48, subelement 41, subfield 9 (Reserved for Future Use) is for future use.

---

Attributes

---

Subfield ID:	09
--------------	----

---

Data Representation:	a...22
----------------------	--------

---

Length Field:	2
---------------	---

---

### **Subfield 10—Reserved for Future Use**

DE 48, subelement 41, subfield 10 (Reserved for Future Use) is for future use.

---

Attributes

---

Subfield ID:	10
--------------	----

---

Data Representation:	n-9
----------------------	-----

---

Length Field:	2
---------------	---

---

### **Subfield 11—Citizen ID**

DE 48, subelement 41, subfield 11 (Citizen ID) indicates the citizen ID.

---

Attributes

---

Subfield ID:	11
--------------	----

---

Data Representation:	a...20
----------------------	--------

---

Length Field:	2
---------------	---

---

Data Field:	National ID
-------------	-------------

---

---

Justification:	N/A
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
Data Representation:	ans...20
Length Field:	2

---

### **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 Representation:	ans...20
Length Field:	2

---

### **Subfield 14—Reserved for Future Use**

DE 48, subelement 41, subfield 14 (Reserved for Future Use) is for future use.

---

Attributes	
Subfield ID:	14
Data Representation:	ans...20
Length Field:	2

---

### **Subfield 15—Reserved for Future Use**

DE 48, subelement 41, subfield 15 (Reserved for Future Use) is for future use.

---

Attributes	
Subfield ID:	15
Data Representation:	ans...10
Length Field:	2

---

---

### **Subfield 16—Reserved for Future Use**

DE 48, subelement 41, subfield 16 (Reserved for Future Use) is for future use.

Attributes	
Subfield ID:	16
Data Representation:	n-2
Length Field:	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
Data Representation:	a-1
Length Field:	2

### **Subfield 18—Reserved for Future Use**

DE 48, subelement 41, subfield 18 (Reserved for Future Use) is for future use.

Attributes	
Subfield ID:	18
Data Representation:	a...20
Length Field:	2

## **Subelement 42—Electronic Commerce Indicators**

DE 48, subelement 42 (Electronic Commerce Indicators) contains the electronic commerce indicators representing the security level and cardholder authentication associated with the transaction.

<b>Attributes</b>	
Subelement ID:	42
Data Representation:	n-7 (except n-19 for acquirer Authorization Request Response/ 0110 messages if SecureCode downgrade or MDES SLI modification occurred)
Length Field:	2

Data Field:	Contents of subfield 1 (except contents of subfields 1, 2, and 3 for acquirer Authorization Request Response/0110 messages if <i>SecureCode</i> downgrade or MDES SLI modification occurred)
-------------	--

Subfields:	3
------------	---

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	X	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C
Reversal Request/0400	C	•	C

### **Values**

If *SecureCode* downgrade or MDES SLI modification did not occur, 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.

If *SecureCode* downgrade or MDES SLI modification occurred, contains contents of subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), subfield 2 (Original Electronic Commerce Security Level Indicator and UCAF Collection Indicator), and subfield 3 (Reason for UCAF Collection Indicator Downgrade) for acquirer Authorization Request Response/0110 messages.

### **Application Notes**

A Mastercard *SecureCode* transaction is downgraded to a non-*SecureCode* transaction if an Accountholder Authentication Value (AAV) is not present or is invalid in DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]).

---

For transactions initiated with Mastercard Digital Enablement Service (MDES) Tokens, Mastercard provides Authorization Platform edits that validate and when necessary, modify the Security Level Indicator (SLI) in DE 48, subelement 42, subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection indicator) in Authorization Request/0100 messages.

Mastercard sends the correct SLI to the issuer in Authorization Request/0100 messages for MDES transactions.

Mastercard notifies acquirers when the SLI has been corrected by inserting two additional DE 48, subelement 42 indicators, as follows. All acquirers must be ready to receive DE 48, subelement 42, subfield 2 (Original Electronic Commerce Security Level Indicator and UCAF Collection Indicator), and subfield 3 (Reason for UCAF Collection Indicator Downgrade) in the Authorization Request Response/0110 messages.

---

### **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
Data Representation:	n-3
Length Field:	2
Data Field:	Indicates the electronic commerce security level and UCAF collection in positions 1, 2, and 3
Justification:	N/A

---

#### **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	= eCommerce / SecureCode
2	= Processed through Masterpass
3	= Reserved for future use
4	= Tokenized payment
5–9	= 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™)

22 = Masterpass-generated transaction

24 = Digital Secure Remote Payment transaction

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 or a SecureCode merchant has chosen not to undertake SecureCode on this transaction
1	= UCAF data collection is supported by the merchant, and UCAF data must be present (DE 48, subelement 43 must be present and contain an attempt AAV for Mastercard SecureCode)
2	= UCAF data collection is supported by the merchant, and UCAF data must be present (DE 48, subelement 43 must contain a fully authenticated AAV)

---

---

3 = UCAF data collection is supported by the merchant, and UCAF (Mastercard assigned Static Accountholder Authentication Value) data must be present.

**NOTE: DE 48, subelements 32 and 43 are required for Static AAV transactions.**

Identifies participation in one of the following programs:

- Maestro Recurring Payments Program
- Mastercard Utility Payment Program
- Maestro Low Risk Merchant Program
- Maestro Static AAV for Masterpass

---

4 = Merchant has chosen to share authentication data within authorization; UCAF data collection not supported

---

5 = Issuer Risk Based Decisioning

---

6 = Merchant Risk Based Decisioning

**NOTE: Issuers and acquirers must support the security level indicator (SLI) value of 246 for Digital Secure Remote Payment (DSRP) transactions participating in the MDES for Merchants and MDES for Commerce Platforms.**

---

7 = Partial shipment or recurring payment (DE 48, subelement 43 not required). Liability will depend on the original UCAF values provided and matching with the initial transaction.

---

8–9 = Reserved for future use

---

**Application Notes**

---

For Visa Gateway 3-D Secure transactions the following mapping applies:

- Position 3 "0" maps to Field 60 SLI = 07 (Not Authenticated)
- Position 3 "1" maps to Field 60 SLI = 06 (3-D Secure merchant, not authenticated)
- Position 3 "2" maps to Field 60 SLI = 05 (Authenticated with CAVV)

For American Express Gateway 3-D Secure transactions the following mapping applies:

- Position 3 "0" maps to Field 61 SLI = 07 (Not Authenticated)
- Position 3 "1" maps to Field 61 SLI = 06 (Attempted with AEVV)
- Position 3 "2" maps to Field 61 SLI = 05 (Authenticated with AEVV)

SLI is the level of security used when a cardmember provides payment information to the merchant during authentication.

JCB and Diners Club use the same Position 3 values (0, 1, and 2) as defined for Mastercard *SecureCode*.

---

### **Subfield 2—Original Electronic Commerce Security Level Indicator and UCAF Collection Indicator**

DE 48, subelement 42, subfield 2 (Original Electronic Commerce Security Level Indicator and UCAF Collection Indicator) describes the original Security Level Indicators sent by the acquirer in the Authorization Request/0100 message before the *SecureCode* downgrade or MDES SLI modification occurred.

---

#### **Attributes**

---

Subfield ID:	02
Data Representation:	n-3
Length Field:	2
Data Field:	Contents of subfield 2
Justification:	N/A

---

<b>Position</b>	<b>Description</b>
1	Security Protocol
2	Cardholder Authentication
3	UCAF Collection Indicator

---

#### **Application Notes**

---

---

A Mastercard *SecureCode* transaction is downgraded to a non-*SecureCode* transaction if an Accountholder Authentication Value (AAV) is not present or is invalid in DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]).

DE 48, subelement 42, subfields 2 and 3 are only present in the Authorization Request Response/0110 message provided by Mastercard to the acquirer if a *SecureCode* downgrade or MDES SLI modification occurred.

For an acquirer-generated Reversal Request/0400 message, the contents of DE 48, subelement 42 (if present) should be the same as that which the acquirer sent in the Authorization Request/0100 message regardless of whether or not the Authorization Request Response/0110 message contains DE 48, subelement 42 with all three subfields due to the *SecureCode* downgrade or MDES SLI modification.

The message format sent in the acquirer Authorization Request Response/0110 message will be in the format 0103xxx0203yyy0301z only if the *SecureCode* downgrade occurs. Otherwise, the message format will remain as it is today which is 0103xxx.

**NOTE: DE 48, subelement 42, subfields 2 and 3 will always be submitted together.**

---

### **Subfield 3—Reason for UCAF Collection Indicator Downgrade**

DE 48, subelement 42, subfield 3 (Reason for UCAF Collection Indicator Downgrade) describes the reason why the Authorization Request/0100 message was downgraded or modified. Refer to Application Notes for details on *SecureCode* downgrade or MDES SLI modification.

---

#### **Attributes**

---

Subfield ID: 03

---

Data Representation: n-1

---

Length Field: 2

---

Data Field: Contents of subfield 3

---

Justification: N/A

---

---

#### **Values                          Description**

---

0                          Missing Universal Cardholder Authentication Field (UCAF)

---

1                          Invalid Universal Cardholder Authentication Field (UCAF)

---

---

#### **Application Notes**

---

A Mastercard *SecureCode* transaction is downgraded to a non-*SecureCode* transaction if an Accountholder Authentication Value (AAV) is not present or is invalid in DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]).

DE 48, subelement 42, subfields 2 and 3 are only present in the Authorization Request Response/0110 message provided by Mastercard to the acquirer if a *SecureCode* downgrade or MDES SLI modification occurred.

For an acquirer-generated Reversal Request/0400 message, the contents of DE 48, subelement 42 (if present) should be the same as that which the acquirer sent in the Authorization Request/0100 message regardless of whether or not the Authorization Request Response/0110 message contains DE 48, subelement 42 with all three subfields due to the *SecureCode* downgrade or MDES SLI modification.

The message format sent in the acquirer Authorization Request Response/0110 message will be in the format 0103xxx0203yyy0301z only if the *SecureCode* downgrade occurs. Otherwise, the message format will remain as it is today which is 0103xxx.

**NOTE: DE 48, subelement 42, subfields 2 and 3 will always be submitted together.**

---

### **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 *SecureCode* fully authenticated or attempts transactions, data for Visa, JCB, Diners Club, or American Express transactions associated with the 3-D Secure Electronic Commerce Verification Service (if collected), or the Static AAV assigned by Mastercard for Maestro Recurring Payments Program, Mastercard Utility Payment Program, or Maestro Low Risk Merchant Program.

Subelement 43 (UCAF) is also used to support Digital Secure Remote Payments (DSRP) submitted as Electronic Commerce (POS entry mode DE 22, subfield 1, value of 81) transactions. In this case, this UCAF field will contain an encoded list of data constructed according to a UCAF format. Refer to the *Digital Secure Remote Payments—UCAF Formats* manual for information on the UCAF formats supported by Mastercard.

---

#### **Attributes**

---

Subelement ID:	43
Data Representation:	ans...32; LLVAR
Length Field:	2
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](#)
- [3-D Secure Electronic Commerce Verification Service \(Visa or American Express\)](#)
- [Digital Secure Remote Payments](#)

### **Application Notes**

Effective 12 June 2018, a cryptogram in subelement 43 (UCAF) is not required for electronic commerce (POS entry mode DE 22, subfield 1, value of 81) Payment Transactions identified by DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 28 (Payment Transaction) initiated with tokens.

## **Subelement 43—3-D Secure for Mastercard SecureCode**

DE 48 (Additional Data—Private Use), 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**

Transaction specific. Position 1 of the Mastercard 3-D Secure SPA AAV is a control byte indicating the Mastercard Identity Check/Mastercard SecureCode platform that created the field contents.

<b>SPA1 Value</b>	<b>SPA2 Value</b>
j	kA, kB, kC, kD, kG, KH, kJ, KK, KO, kP

---

h	kE, kF, kL, kM, kN
---	--------------------

---

**NOTE: Values i, l, m, and n are reserved for future use.**

---

#### Application Notes

---

**NOTE: Issuers must pass the correct security level indicator (SLI) value with the corresponding AAV control byte during cardholder authentication. Mastercard 3DS protocol, SecureCode Program Rules, and DW Integrity Edits do not allow sending Fully Authenticated AAVs for Attempted Authentications nor Attempted AAVs for Fully Authenticated Authentications.**

The following is an example of a properly coded DE 48, subelement 43 for Mastercard SecureCode for Fully Authenticated Authorization including AVS request.

T420701032124328jJLtQa+lws8AREAEbjsA1MAAAA=

Refer to the *Mastercard SecureCode—Issuer Implementation Guide* and *Mastercard SecureCode—Acquirer Implementation Guide* for more information.

Mastercard supports attempts AAV, the acquirer should forward to Mastercard any attempts AAV it receives so that Mastercard can pass to the issuer.

**NOTE: Issuers should not perform SecureCode validation on static AAVs in DE 48, subelement 43 nor on attempts AAV generated by Mastercard.**

---

The UCAF field (DE 48, subelement 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.

---

## Subelement 43—Digital Secure Remote Payment Universal Cardholder Authentication Field (UCAF)

Subelement 43 contains UCAF data and is described here for Mastercard Digital Secure Remote Payments (DSRP).

---

#### Attributes

---

Subelement ID:	43
Data Representation:	ans-28; (base 64 encoded)
Length Field:	2
Data Field:	Mastercard Digital Secure Remote Payment UCAF format
Subfields:	N/A
Justification:	N/A

---

#### Values

---

Transaction specific.

Refer to the *Digital Secure Remote Payments—UCAF Formats* manual for detailed information on the UCAF formats supported by Mastercard.

---

An MDES transaction might not contain DE 48, subelement 43 when the acquirer has submitted a dynamic expiration date (DE 14) and a dynamic token verification code (DE 48, subelement 92) in order to perform MDES validation services.

---

A Digital Secure Remote Payment transaction submitted for Mastercard Digital Enablement Service processing that involves an authorization request for a partial shipment or a recurring payment must contain the partial shipment verbiage in subelement 43 as follows:

PARTIALSHIPMENTbbbbbbbbbbb or PARTIALSHIPMENT00000000000000 unless subelement 42 = 247 in which case subelement 43 is not required. This field contains 28 positions where b represents a space.

---

### **Application Notes**

---

The format is version dependent.

---

## **Subelement 43—Static AAV**

DE 48, subelement 43 is the Mastercard implementation of the Static AAV for Maestro Recurring Payments Program, Mastercard Utility Payment Program, Maestro Low Risk Merchant Program, or Maestro Static AAV for Masterpass.

---

### **Attributes**

---

Data Representation: ans-28

---

Data Field: The Mastercard assigned Static AAV

---

### **Values**

---

Position 1 = one of the following values:

- 3 = Transaction processed under the Maestro Recurring Payments Program
- 5 = Transaction processed under the Mastercard Utility Payment Program
- 5 = Maestro Basic Static AAV (Maestro e-commerce transaction initiated through Masterpass)

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).

---

---

For the Maestro Low Risk Merchant Program (Europe region only), for subsequent transactions after the first Maestro e-commerce transaction with the same Maestro card, approved merchants will use DE 48, subelement 43 in the Authorization Request/0100 message with the Mastercard-assigned static Accountholder Authentication Value (AAV) **5MARPPROGRAM9999999999999999** (28 positions).

---

#### **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—3-D Secure Electronic Commerce Verification Service (Visa, JCB, Diners Club and American Express Only)**

Subelement 43 (3-D Secure Electronic Commerce Verification Service [Visa, JCB, Diners Club, and American Express]) is for 3-D Secure Electronic Commerce Verification Service (Visa, JCB, Diners Club, and American Express).

---

#### **Attributes**

---

##### **Position 1 (3-D Secure Electronic Commerce Transaction Indicator)**

---

Subelement ID:	43
Data Representation:	n-1
Length Field:	2
Data Field:	Indicates a 3-D Secure Electronic Commerce transaction
Subfields:	N/A
Justification:	N/A
Values:	8 = Non-Mastercard 3-D Secure Electronic Commerce transaction (Visa, JCB, Diners Club or American Express)

---

##### **Position 2–21 (3-D Secure Electronic Commerce Cardholder Authentication Verification Value [CAVV] Visa Field 126.9 and American Express Verification Value [AEVV] AMEX field 61)**

---

Data Representation:	b-20
Data Field:	The 3-D Secure Electronic Commerce Visa, JCB, Diners Club, CAVV or American Express AEVV value in binary format for usage 2 and 3.
Values:	Transaction specific

---

#### **Application Notes**

---

---

For American Express Gateway 3-D Secure transactions, position 1 is information-only and will not be passed.

For recurring payment transactions, DE 48, subelement 43 will contain the partial shipment verbiage as follows: PARTIALbSHIPMENTbbbbbbbbbbb or PARTIALSHIPMENT000000000000000 where b represents a space. Zeros are literal and must be included as indicated. This field contains 28 positions.

For partial shipment transactions, DE 48, subelement 43 will contain the cryptographic data from the original transaction.

---

## **Subelement 44—3-D Secure Electronic Commerce Transaction Identifier (XID) (Visa and American Express)**

Subelement 44 (3-D Secure Electronic Commerce Transaction Identifier [XID][Visa and American Express]) contains the 3-D Secure Electronic Commerce Transaction Identifier (XID).

---

### **Attributes**

Subelement ID:	44
Data Representation:	b-20
Length Field:	2
Data Field:	The Visa or American Express 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. Visa field 126.8 or the American Express XID value in binary—AMEX field 61.

---

### **Application Notes**

---

The Visa XID value is optional in authorization messages for Visa usage 3 TransStain.

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—3-D Secure Electronic Commerce Transaction Response Code (Visa and American Express)**

Subelement 45 (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) or the American Express Verification Value (AEVV) results code.

---

### **Attributes**

Subelement ID:	45
Data Representation:	an-1
Length Field:	2
Data Field:	Visa 3-D Secure CAVV or American Express 3-D Secure AEVV results code
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**

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.

Refer to the American Express Technical Specifications manual for AMEX field 61, position 9, American Express Verification Value (AEVV Results Code) for a complete list of values available for this field.

---

## **Subelement 46—Product ID (Visa Only)**

DE 48, subelement 46 (Product ID) contains the Visa Product ID value (Visa Only).

---

### **Attributes**

Subelement ID:	46
----------------	----

---

---

Data Representation: an-2

Length Field: 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 (Product ID).

---

### **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**

DE 48, subelement 47 (Mastercard Payment Gateway Transaction Indicator) indicates that the transaction is a Mastercard Payment Gateway transaction.

---

### **Attributes**

---

Subelement ID: 47

---

Data Representation: ans-8

---

Length Field: 2

---

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	•	•
<b>Values</b>			
MC-MPG/W			
<b>IF...</b>	<b>THEN the Authorization Platform...</b>		
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) = 048047</li> </ul>		

## Subelement 48—Mobile Program Indicators

DE 48, subelement 48 (Mobile Program Indicators) identifies the service manager of the Mastercard Mobile Remote Payments Program.

Attribute	Description
Subelement ID:	48
Data Representation:	ans...73; LLVAR
Length Field:	2
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.

Attribute	Description
Subfield ID:	01
Data Representation:	n...1; LLVAR
Length Field:	2
Data Field:	Contents of subfield 1
Justification:	N/A

**Values**

---

1 = Issuer domain
2 = Acquirer domain

### **Subfield 2—Mastercard Mobile Remote Payment Transaction Type**

DE 48, subelement 48, subfield 2 (Mastercard Mobile Remote Payment Transaction Type) describes the available transaction types for Mastercard Mobile Remote Payments.

Attribute	Description
Subfield ID:	02
Data Representation:	n...1; LLVAR
Length Field	2 positions, value = 01
Data Field:	Contents of subfield 2
Justification:	N/A

**Values                      Description**

---

1	Remote Purchase (Consumer Initiated)—Face-to-Face
2	Remote Purchase (Consumer Initiated)—e-Commerce
3	Remote Purchase (Consumer Initiated)—MOTO
4	Bill Pay (Consumer Initiated)

5	Top-up (Consumer Initiated)
6	Cash-out (Consumer Initiated)
7	Cash-out (ATM/Agent Triggered)—DE 61, SF 10 can differentiate between ATM or non-CAT (Agent) transaction
8	Remote Purchase (Merchant Triggered)—Face-to-Face
9	Remote Purchase (Merchant Triggered)—e-Commerce

### **Subfield 3—Mobile Phone Number**

DE 48, subelement 48 (Mobile Program Indicators), subfield 3 (Mobile Phone Number) contains the customer mobile phone number.

Attribute	Description
Subfield ID:	03
Data Representation:	n...15; LLVAR
Length Field:	2
Data Field:	Contents of subfield 3
Justification:	N/A

**Values**

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
Data Representation:	ans...40; LLVAR
Length Field:	2
Data Field:	Contents of subfield 4
Justification:	N/A

**Values**

Customer convenience fee data.
--------------------------------

**Application Note**

--

---

The Convenience Fee amount that is present in subfield 4 must not be included in DE 4 (Amount, Transaction).

---

### **Subelement 49—Time Validation Information**

DE 48, subelement 49 (Time Validation Information) contains time data used to calculate time validation and the results of validation when performed.

	<b>Attribute</b>	<b>Value</b>
Subelement ID	n-2	49
Subelement Length	n-2	15
Data Representation	n-15	Fixed
Number of Subfields	3	Subfield 1—Time Value Subfield 2—Time Discrepancy Value Subfield 3—Time Discrepancy Indicator

#### **Usage**

Following is the usage of subelement 49 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Authorization Request/0100	•	X	C
Authorization Advice/0120—System-generated	•	X	C

#### **Subfield 1—Time Value**

DE 48, subelement 49, subfield 1 (Time Value) contains the time data derived from the acquirer transaction to be used in the time validation.

<b>Attributes</b>	
Data Representation	n-8
Data Field	Contents of subfield 1
Justification	Right-justified, leading zeros

#### **Subfield 2—Time Discrepancy Value**

DE 48, subelement 49, subfield 2 (Time Discrepancy Value) contains a positive value representing the differential in minutes between the transaction time data and service-calculated time.

---

#### **Attributes**

Data Representation	n-5
Data Field	Contents of subfield 2
Justification	Right-justified, leading zeros

#### **Subfield 3—Time Discrepancy Indicator**

DE 48, subelement 49, subfield 3 (Time Discrepancy Indicator) contains a value that indicates if the time discrepancy value is below, above, or within the minimum and maximum values for the time validation window or that indicates time validation was not performed.

---

#### **Attributes**

Data Representation	n-2
Data Field	Contents of subfield 3
Justification	Left-justified

---

<b>Values</b>	<b>Description</b>
---------------	--------------------

01	Positive value within time validation window
02	Positive value outside time validation window
03	Negative value within time validation window
04	Negative value outside time validation window
05	Unknown (time validation not performed)

#### **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
Data Representation:	ans...99; LLVAR  The “LL” length field of LLVAR must be an integral multiple of 4, not to exceed 96.
Length Field:	2
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**

See "Valid Subfield 1 and Subfield 2 Value Combinations."

---

**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**

See "Valid Subfield 1 and Subfield 2 Value Combinations."

### **Subelement 51—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 described here.

<b>Attributes</b>	<b>Subfield 1 (Merchant On-behalf [OB] Service)</b>	<b>Subfield 2 (Merchant On-behalf [OB] Result 1)</b>
Data Representation	an-2	an-1
Data Field	Contents of positions 1-2	Contents of position 3
Justification	Left-justified	N/A

#### **Values**

See the following table.

#### **Application Notes**

If the value of subfield 1 and subfield 2 is 90C, then DE 48, SE 55, subfield 1 and subfield 2 will be populated.

Subfield 2 will have values that identify the results from the EMS Real-time Fraud Scoring Service for Merchants processing result.

---

<b>DE 48, Subelement 51, Subfield 1 (Merchant On-behalf [OB] Service) Values (an-2)</b>	<b>DE 48, Subelement 51, Subfield 2 (Merchant On-behalf [OB] Result 1) Values (an-1)</b>
---	--

---

53 = Mastercard Digital Enablement Service Card on File PAN Mapping	C = Conversion of token to PAN completed successfully.
	F = Format error; Incorrect POS Entry Mode (not equal to 81 or 82) applicable to Authorization Request/0100, Authorization Advice/0120 Acquirer-generated, and Reversal Request/0400 messages.
	F = Format error; Token Requestor ID required (based on Token Requestor ID validation bypass parameter), not present (DE 48, subelement 33 not present), or not formatted correctly (DE 48, subelement 33 not formatted correctly).
	I = Invalid; Token suspended or deactivated.
	I = Invalid; Token not found on mapping table.
	T = Invalid; Token Requestor ID/Token combination invalid.

---

---

<b>DE 48, Subelement 51, Subfield 1 (Merchant On-behalf [OB] Service) Values (an-2)</b>	<b>DE 48, Subelement 51, Subfield 2 (Merchant On-behalf [OB] Result 1) Values (an-1)</b>
---	--

---

	U = Unable to process—Mapping Table unreachable/unavailable.
	U = Unable to process—Token expired.
56 = Mastercard Digital Enablement Service Card on File Tokenization and Maintenance	C = Tokenization request completed successfully.
<b>NOTE: Value 56 will be decommissioned in a future release.</b>	C = Token maintenance / inquiry request completed successfully.
	F = Format error; Incorrect POS Entry Mode (not equal to 01) applicable to Authorization Request/0100—Token Request and Authorization Request/0100—Token Requestor Card on File Token Maintenance/Inquiry messages.
	F = Format error; Token Requestor ID required (based on Token Requestor ID validation bypass parameter), not present (DE 48, subelement 33 not present), or not formatted correctly (DE 48, subelement 33 not formatted correctly).
	I = Invalid; Token Requestor ID invalid.
	I = Invalid; Token not found on mapping table.
	T = Invalid; Token Requestor ID/Token combination invalid.
	U = Unable to process—Mapping Table unreachable/unavailable.
	W = PAN listed in Electronic Warning Bulletin (EWB).
90 = EMS Real-time Fraud Scoring Service for Merchants	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.

---

### **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 52—Transaction Integrity Class**

DE 48, subelement 52 (Transaction Integrity Class) contains the Mastercard-provided Transaction Integrity Classification for Point of Sale (POS) Purchase and Purchase with Cash Back transactions initiated on the Authorization Platform.

<b>Attribute</b>	<b>Value</b>
Subelement ID	n-2
Subelement Length	02
Data Representation	an-2
Data Field	Contents of positions 1–2
Number of Subfields	N/A

**Usage**

Following is the usage of subelement 52 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Authorization Request/0100	•	X	C
Authorization Response/0110	OE	X	C
Authorization Advice/0120—System-generated	•	X	C
<b>Classification</b>	<b>Description</b>		<b>Value</b>
Card and Cardholder Present	EMV/Token in a Secure, Trusted Environment		A1
Card and Cardholder Present	EMV/Chip Equivalent		B1

---

Card and Cardholder Present	Mag Stripe	C1
Card and Cardholder Present	Key Entered	E1
Card and Cardholder Present	Unclassified	U0
Card and/or Cardholder Not Present	Digital Transactions	A2
Card and/or Cardholder Not Present	Authenticated Checkout	B2
Card and/or Cardholder Not Present	Transaction Validation	C2
Card and/or Cardholder Not Present	Enhanced Data	D2
Card and/or Cardholder Not Present	Generic Messaging	E2
Card and/or Cardholder Not Present	Unclassified	U0

#### **Application Notes**

The Transaction Integrity Class may optionally be provided in the designated clearing messages when provided by Mastercard via the Authorization Platform for Point of Sale (POS) Purchase and Purchase with Cash Back transactions destined for all issuers in the U.S. region of Mastercard® credit and Debit Mastercard® cards.

Issuers in the U.S. region must support receiving DE 48 (Additional Data), new subelement 52 (Transaction Integrity Class) in Authorization Request/0100 messages and optionally provide it in the Authorization Request Response/0110 messages. Issuers in the U.S. region must also support receiving DE 48 (Additional Data), new subelement 52 (Transaction Integrity Class) in Authorization Advice/0120—System-generated messages.

The Transaction Integrity Class is not sent to non-U.S. region issuers in authorization or clearing messages.

---

#### **Subelement 53—E-ID Request Code**

DE 48, subelement 53 (E-ID Request Code) enables the issuer to identify that additional cardholder information is being requested by the acquirer. This request code is sent by an acquirer to an issuer in an Account Status Inquiry (ASI) message.

---

<b>Attribute</b>	<b>Value</b>
Subelement ID:	n-2
Subelement Length:	53
Data Representation:	n-2
Data Field:	02
Number of Subfields:	ans...99; LLVAR
Number of Subfields:	1
<b>Usage</b>	

---

---

Following is the usage of subelement 53 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

Message	Org	Sys	Dst
Authorization Request/0100	C	•	C
<b>Values</b>			
See subfields.			
<b>Application Notes</b>			
Acquirers that support E-ID will include this subelement in an ASI, queuing the issuer to perform further processing outside of the Mastercard Network. This subelement is valid for Europe region activity only.			
Subelement 53 (and associated subfield 1) is effective as of 12 June 2018.			
For card-not-present transactions, the acquirer should not send subelement 53.			

### **Subfield 1—E-ID Request Value**

DE 48, subelement 53, subfield 1 (E-ID Request Value) informs the issuer of the proposed action on the cardholder account.

---

#### **Attributes**

Data Representation: ans-02

Data Field: Contents of positions 1–2

Justification: N/A

---

#### **Values      Description**

01      Informs the issuer to pull cardholder personal data for E-ID/Health ID Verification Purposes.

02      Informs the issuer to verify and send the age of the cardholder.

03–99    Reserved for Future Use

---

#### **Application Notes**

Issuers must:

- Validate that a valid value is present in the message; and
- Send this cardholder information through a network separate from the Mastercard Network.

---

Subelement 53 and subfield 1 are effective as of 12 June 2018.

## 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.

Attribute	Description
Subelement ID:	55
Data Representation:	an...32; LLVAR
Length Field:	2
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.

Mastercard will require all issuing and acquiring processors to code for, support, and integrate into their systems the data elements, subelements, and values associated with this item.

The following provides the Global Safety and Security Standards effective dates for each region.

- USA: 21 Apr 2017
- EUR: 13 Oct 2017; Ukraine: 1 Apr 2018
- LAC: 13 Oct 2017
- MEA: 13 Oct 2017
- AP: 13 Apr 2018
- CAN: 13 Apr 2018

For additional information about the requirement please refer to the *Global Safety and Security Standards Roadmap*.

**NOTE: Mastercard does not require issuers or acquirers to enroll in these optional products and services, but they must code their systems to support these fields to leverage such products and services in a timely manner in the event of a security issue.**

---

### **Subfield 1—Merchant Fraud Score**

DE 48, subelement 55, subfield 1 (Merchant Fraud Score) indicates the transaction risk score.

<b>Attribute</b>	<b>Description</b>
Subfield ID:	01
Data Representation:	an-3
Length Field:	2
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**

DE 48, subelement 55, subfield 2 (Merchant Score Reason Code) indicates the key factors that influenced the fraud score.

<b>Attribute</b>	<b>Description</b>
Subfield ID:	02
Data Representation:	an-2
Length Field:	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**

DE 48, subelement 55, subfield 3 (Reserved for Future Use) is reserved for future use.

Attribute	Description
Subfield ID:	03

Data Representation:	an-3
Length Field:	2
Data Field:	Contents of positions 1–3
Justification:	N/A
<b>Values</b>	
Reserved for Future Use	

#### **Subfield 4—Reserved for Future Use**

DE 48, subelement 55, subfield 4 (Reserved for Future Use) is reserved for future use.

Attribute	Description
Subfield ID:	04
Data Representation:	an-2
Length Field:	2
Data Field:	Contents of positions 1–2
Justification:	N/A
<b>Values</b>	
Reserved for Future Use	

#### **Subfield 5—Reserved for Future Use**

DE 48, subelement 55, subfield 5 (Reserved for Future Use) is reserved for future use.

Attribute	Description
Subfield ID:	05
Data Representation:	an-2
Length Field:	2
Data Field:	Contents of positions 1–2
Justification:	N/A
<b>Values</b>	
Reserved for Future Use	

#### **Subelement 56—Security Services Additional Data for Issuers**

DE 48, subelement 56 (Security Services Additional Data for Issuers) supports Mastercard embedded security services for issuers. Issuers can receive up to 16 instances of subelement

56. Each instance has the same format for each service. Issuers must code to receive the 16 instances that the service supports.

<b>Attribute</b>	<b>Description</b>
Subelement ID:	56
Data Representation:	an...99; LLVAR The “LL” length field of LLVAR must be an integral multiple of 6, not to exceed 96.
Length Field:	2
Data Field:	Contents of subfields
Subfields:	2
Justification:	N/A

#### **Usage**

Following is the usage of subelement 56 (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**

See subfields.

#### **Application Notes**

Mastercard will require all issuing and acquiring processors to code for, support, and integrate into their systems the data elements, subelements, and values associated with this item.

The following provides the Global Safety and Security Standards effective dates for each region.

- USA: 21 Apr 2017
- EUR: 13 Oct 2017; Ukraine: 1 Apr 2018
- LAC: 13 Oct 2017
- MEA: 13 Oct 2017
- AP: 13 Apr 2018
- CAN: 13 Apr 2018

For additional information about the requirement please refer to the *Global Safety and Security Standards Roadmap*.

**NOTE: Mastercard does not require issuers or acquirers to enroll in these optional products and services, but they must code their systems to support these fields to leverage such products and services in a timely manner in the event of a security issue.**

---

### **Subfield 1—Security Services Indicator**

DE 48, subelement 56, subfield 1 (Security Services Indicator) provides the security services indicator for issuers.

Attribute	Description
Data Representation:	an-3
Data Field:	Contents of positions 1–3
Justification:	N/A
<b>Values</b>	
A three-character code identifying the real-time monitoring service used.	

### **Subfield 2—Security Services Data**

DE 48, subelement 56, subfield 2 (Security Services Data) contains additional data supporting the issuer fraud score.

Attribute	Description
Data Representation:	an-3
Data Field:	Contents of positions 4–6
Justification:	N/A
<b>Values</b>	
A three-character value will be populated.	

### **Subelement 56—Valid Subfield 1 and Subfield 2 Value Combinations**

Following is the valid DE 48, subelement 56, subfield 1 (Security Services Indicator) and subfield 2 (Security Services Data) value combinations.

### **Service Data Content for Decision Intelligence Service—Digital Transaction Insights Feature**

Following is the Service Data Content for the Digital Transaction Insights feature of the Decision Intelligence service.

Subfield 2 (an-3)			
Subfield 1 (an-3)	Position 1	Position 2	Position 3
Security Services Indicator	Risk Level	Reason Code 1	Reason Code 2
AIQ—Digital Transaction Insights	0–9 where higher values indicate higher degree of risk.	The following codes apply to <b>both</b> Reason Code fields 1 and 2, where: <ul style="list-style-type: none"> <li>• Position 2 = a Mastercard-determined reason code</li> <li>• Position 3 = a merchant-determined reason code</li> </ul>	
<b>NOTE: This information is subject to change.</b>			
Reason Code	Description		
A	Risk Event - Suspicious Account Activity		
B	Risk Event - Unknown Device/Account Relationship		
C	Risk Event - Device or Profile information associated with fraud		
D	Risk Event - Recent High Risk change to Device or Profile information		
E	Risk Event - Recent change to Device or Profile Information		
F	Risk Event - PAN associated with fraud event		
G	New Account or Insufficient Data		
H	Merchant/Acquirer: Merchant (fraud) risk high (assessed by Mastercard)		
I	Merchant/Acquirer: Merchant (fraud) risk low (assessed by Mastercard)		
J	Environment: Good/Known IP		
K	Cardholder: Billing address - prior history established		
L	Cardholder: Email address - prior history established		
M	Cardholder: Phone Number - prior history established		

Subfield 2 (an-3)			
Subfield 1 (an-3)	Position 1	Position 2	Position 3
Security Services Indicator	Risk Level	Reason Code 1	Reason Code 2
	N	Cardholder: Shipping address - prior history established	
	O	Cardholder: Card number (PAN) behavior established high trust in the current transaction	
	P	Environment: Device known	
	Q	Environment: Account established on Device	
	R	Environment: Session - Trusted/normal/innocent session (no man in the middle attack/no bot, not suspicious account activity)	
	S	More than one Cardholder category established	
	T	More than one Merchant/Acquirer category established	
	U	More than one Environment category established	
	V	Co-occurring established link between cardholder and Merchant/Acquirer	
	W	Co-occurring established link between cardholder and Environment	
	X	Co-occurring established link between Merchant/Acquirer and Environment	
	Y	All three categories established	
	Z	VIP, Known Customer (Merchant Submitted)	

**NOTE: The above codes depict a potential list of reason codes and an appropriate ordering from negative to positive. This list may be further refined. Reason codes A–H reflect riskier, or less information while reason codes I–Z reflect positive information.**

### Service Data Content for Decision Intelligence Service—Authorization IQ Feature

Following is the Service Data Content for the Authorization IQ feature of the Decision Intelligence service. Customers that support Decision Intelligence will receive AQV (GDV-based

Spend Ranking), AQF (Frequency-based Spend Ranking), and AQS (Segment Qualifier) on all transactions.

**NOTE: Positions 2 and 3 use the same reason code definitions.**

Subfield 2 (an-3)			
Subfield 1 (an-3)	Position 1	Position 2	Position 3
<b>Spending Dimension Insights</b>	<b>Overall Account Spending Insights</b>	<b>Channel Spending Insights</b>	<b>Account Transaction Insights</b>
AQV—GDV-based Spend Ranking	<b>New</b> (card activity on the network less than 60 days old)	<b>New</b> (card activity on the network less than 60 days old)	0
Or		Or	
AQF—Frequency-based Spend Ranking		<b>None</b> (No network activity in the last 12 months or Dormant Card Number)	
	High = 1		High = 1
	Med-1 = 4		Med-1 = 4
	Med-2 = 5		Med-2 = 5
	Med-3 = 6		Med-3 = 6
	Low = 9		Low = 9
AQS—Segment Qualifier	Refer to the Segment Definitions table that follows.		

### Segment Definitions for Decision Intelligence Service—Authorization IQ Feature

The Authorization IQ feature of the Decision Intelligence service supports the following series of segments under which each transaction is qualified for dimension analysis.

**NOTE: New segments may be added to the Authorization IQ feature of the Decision Intelligence service at any time.**

Segment	Segment Qualifier ID
<b>Channel: Card Present—Domestic Segments</b>	000—Card activity on network less than 60 days old
Travel	001
Retail	002
Gaming	003

<b>Segment</b>	<b>Segment Qualifier ID</b>
Gambling	004
Education/Healthcare	005
Cash (for example: ATM)	006
Fuel	007
Utilities	008
Leisure and Entertainment	009
Digital Goods	010
Professional Services	011
Reserved for Future Use	012–198
Other Card Present—Domestic	199
<b>Channel: Card Present—Cross-Border Segments</b>	200—Card activity on network less than 60 days old
Travel	201
Retail	202
Gaming	203
Gambling	204
Education/Healthcare	205
Cash (for example: ATM)	206
Fuel	207
Utilities	208
Leisure and Entertainment	209
Digital Goods	210
Professional Services	211
Reserved for Future Use	212–398
Other Card Present—Cross-Border	399
<b>Channel: Card Not Present—Domestic Segments</b>	400—Card activity on network less than 60 days old
Travel	401
Retail	402
Gaming	403
Gambling	404

<b>Segment</b>	<b>Segment Qualifier ID</b>
Education/Healthcare	405
Cash (for example: ATM)	406
Utilities	407
Leisure and Entertainment	408
Digital Goods	409
Professional Services	410
Reserved for Future Use	411–598
Other Card Not Present—Domestic	599
<b>Channel: Card Not Present—Cross-Border Segments</b>	600—Card activity on network less than 60 days old
Travel	601
Retail	602
Gaming	603
Gambling	604
Education/Healthcare	605
Cash (for example: ATM)	606
Utilities	607
Leisure and Entertainment	608
Digital Goods	609
Professional Services	610
Reserved for Future Use	611–798
Other Card Not Present—Cross-Border	799
Reserved for Future Use	800–899
Dormant Card Number	900—Previously active card with no activity on the network in the last 120 days
Reserved for Future Use	901–999

### **Service Data Content for Consumer Controls**

Following is the Service Data Content for Consumer Controls.

Subfield 1 (an-3)	Subfield 2 (an-3)	
Service Code	Reason Code	Description
INC—Consumer Controls	AAL	Alert All Transactions
	ABD	Alert Budget
	ACB	Alert Cross-border
	ACH	Alert Transaction Channel
	AFL	Alert Filter
	AGE	Alert Transaction Geography
	AMC	Alert Merchant Category Code
	ATA	Alert Transaction Amount
	DBD	Decline Budget
	DCB	Decline Cross-border
	DCD	Decline Card Disabled
	DCH	Decline Transaction Channel
	DFL	Decline Filter
	DGE	Decline Transaction Geography
	DMC	Decline Merchant Category Code
	DTA	Decline Transaction Amount
	NAT	No Action Taken

### Subelement 57—Security Services Additional Data for Acquirers

DE 48, subelement 57 (Security Services Additional Data for Acquirers) supports Mastercard embedded security services for acquirers.

Attribute	Description
Subelement ID:	57
Data Representation:	an...99; LLVAR  The “LL” length field of LLVAR must be an integral multiple of 6, not to exceed 96.
Length Field:	2
Data Field:	Contents of subfields

Subfields:	2
Justification:	N/A

**Usage**

Following is the usage of subelement 57 (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—Security Services Indicator**

DE 48, subelement 57, subfield 1 (Security Services Indicator) provides the security services indicator for acquirers.

Attribute	Description
Data Representation:	an-3
Data Field:	Contents of positions 1–3
Justification:	N/A

**Values**

A three-character code identifying the real-time monitoring service used.

**Subfield 2—Security Services Data**

DE 48, subelement 57, subfield 2 contains additional data supporting the Merchant fraud score.

Attribute	Description
Data Representation:	an-3
Data Field:	Contents of positions 4–6
Justification:	N/A

**Values**

A three-character value will be populated.

**Subelement 58—ATM Additional Data**

DE 48, 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
Data Representation:	ans-33
Length Field:	2
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
Reversal Advice/0420	•	C	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

---

### 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

---

#### Attributes

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
-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**

DE 48, subelement 61 (POS Data, Extended Condition Codes) indicates whether the merchant terminal supports a specific program or service.

---

**Attributes**

Subelement ID:	61
Data Representation:	n-5
Length Field:	2
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

---

**Values**

---

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

---

**Values**

---

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 Expert Monitoring for Merchants.

---

**Attributes**

---

Data Representation: an-1

---

Data Field: Contents of position 4

---

Justification: N/A

---

**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.

---

Mastercard will require all issuing and acquiring processors to code for, support, and integrate into their systems the data elements, subelements, and values associated with this item.

The following provides the Global Safety and Security Standards effective dates for each region.

- USA: 21 Apr 2017
- EUR: 13 Oct 2017; Ukraine: 1 Apr 2018
- LAC: 13 Oct 2017
- MEA: 13 Oct 2017
- AP: 13 Apr 2018
- CAN: 13 Apr 2018

For additional information about the requirement please refer to the *Global Safety and Security Standards Roadmap*.

**NOTE: Mastercard does not require issuers or acquirers to enroll in these optional products and services, but they must code their systems to support these fields to leverage such products and services in a timely manner in the event of a security issue.**

---

### **Subfield 5—Final Authorization Indicator**

DE 48, subelement 61, subfield 5 (Final Authorization Indicator) is used to identify final authorization messages.

---

#### **Attributes**

---

Data Representation: n-1

---

Data Field: Contents of position 5

---

Justification: N/A

---

#### **Values**

---

0 = Normal Authorization/Undefined Finality

---

1 = Final Authorization

---

#### **Application Notes**

---

Final authorization is an authorization request for an amount greater than zero, which meets the following conditions:

- Authorization is requested for the final transaction amount.
- The transaction is not expected to be canceled after the authorization request is approved in full (excluding non-completion for technical reasons such as telecommunications failure or terminal failure).

Any transaction corresponding to an authorization identified as a final authorization must be presented within seven calendar days of the authorization approval date. An authorization request is properly identified as a final authorization when DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains value 0 and DE 48 (Additional Data), subelement 61 (POS Data Extended Condition Codes), subfield 5 contains value 1.

Coding authorization messages as “final” or “preauthorized” is mandatory for acquirers of Asia/Pacific, Europe, and Middle East/Africa card acceptors and optional for acquirers in other regions.

---

When submitting an Acquirer-generated Authorization Advice/0120, subfield 5 (Final Authorization Indicator) should be populated with the same value as provided in the original Authorization Request/0100 message.

---

Normal authorization/undefined finality is an authorization request for an amount greater than zero where a final amount may or may not be known and the transaction is not expected to be canceled after the authorization request is approved in full.

An authorization request is identified as normal or undefined finality authorization when DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains value 0 and DE 48 (Additional Data), subelement 61 (POS Data Extended Condition Codes), subfield 5 contains value 0 or is not present.

---

When DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains value 4 (Preauthorized request), DE 48 (Additional Data), subelement 61 (POS Data Extended Condition Codes), subfield 5 must either contain value 0 (Normal Authorization/Undefined Finality) or not be present.

---

## **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
Data Representation:	ans-15
Length Field:	2
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 six 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 048063. DE 48, subelement 63 may contain a value of zeros in Reversal Request/0400 messages or Reversal Advice/0420 messages only when an Authorization Request Response/0110 was not successfully received or processed by the acquirer.

DE 48, subelement 63 must be provided in Authorization Request/0100 messages to identify an incremental preauthorization and a zero amount Authorization Chargeback Protection Period Extension request.

DE 48, subelement 63 has been added to the acquirer-generated authorization advice/0120 layout to further assist issuers in matching an AFD completion advice to the original preauthorization. For additional details, refer to Clearing AFD Transactions in the Automated Fuel Dispenser Completion section of the Program and Service Format Requirements chapter.

---

## **Subelement 64—Transit Program**

DE 48, subelement 64 (Transit Program) is used to identify transit transactions in authorization messages.

**NOTE: Transit Program field is not limited to MCC 4111, MCC 4131, and MCC 4784.**

---

### Attributes

Subelement ID:	64
Data Representation:	n-4
Length Field:	2
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.

**NOTE: Values 3, 4, and 6 for Transit Transaction Type Indicators subelement 64, subfield 1 are limited to MCC 4111, MCC 4131, and MCC 4784.**

Attributes		
Data Representation:	n-2	
Data Field:	Contents of positions 1–2	
Justification:	N/A	
<b>Values</b>		
01	=	Prefunded
02	=	Real-time Authorized
03	=	Post-Authorized Aggregated
04	=	Authorized Aggregated Split Clearing
05	=	Other
06	=	Post-authorized Aggregated Maestro
07	=	Debt Recovery
08–99	=	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	
<b>Values</b>		
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
18	=	Trailer
19	=	Regional Train
20	=	Inter City
21	=	Funicular Train
22	=	Cable Car
23–99	=	Reserved for Future Use

---

### **Subelement 65—Terminal Compliant Indicator**

DE 48 (Additional Data—Private Use), subelement 65 (Terminal Compliant Indicator) contains two subfields that identify whether or not a POS terminal from which the transaction originated is Terminal Line Encryption (TLE) and Unique Key Per Terminal (UKPT)/Derived Unique Key Per Terminal (DUKPT) compliant. This field must be present in card-present, POS transactions acquired in India.

---

Attributes	
Subelement ID:	65
Data Representation:	n-2
Length Field:	2
Data Field:	Contents of subfields 1–2

---

---

Subfields:	2
Justification:	See subfields

### Usage

Following is the usage of subelement 65 (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 Terminal Compliant Indicator values in subfields 1 and 2.

#### Subfield 1—TLE Compliant

DE 48, subelement 65, subfield 1 indicates whether or not the POS terminal from which the transaction occurred is Terminal Line Encryption (TLE)-certified.

##### Attributes

Data Representation:	n-1
Data Field:	Contents of subfield 1
Justification:	N/A

##### Values

1	=	Not Certified
2	=	Certified

#### Subfield 2—UKPT/DUKPT Compliant

DE 48, subelement 65, subfield 2 indicates whether or not the POS terminal from which the transaction occurred is Unique Key Per Terminal/Derived Unique Key Per Terminal (UKPT/DUKPT)-certified.

##### Attributes

Data Representation:	n-1
Data Field:	Contents of subfield 2
Justification:	N/A

##### Values

---

1	=	Not Certified
2	=	Certified

---

## Subelement 66—Authentication Data

DE 48 (Additional Data—Private Use), subelement 66 is populated by the acquirer and passed to the issuer to indicate the Program Protocol being used, 3-D Secure Version 1.0 (3DS 1.0) or EMV 3-D Secure (3DS 2.0), and Directory Server Transaction ID.

Attribute	Value
Subelement ID	n-2
Subelement Length	n-2
Data Representation	ans...45; LLVAR
Data Field	Contents of subfields
Number of Subfields	2
	Subfield 1—Program Protocol
	Subfield 2—Directory Server Transaction ID

---

### Usage

Following is the usage of subelement 66 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

Message	Org	Sys	Dst
Authorization Request/0100	C	•	C
Authorization Request Response/0110	•	CE	C
Authorization Advice/0120—Acquirer-generated	C	•	C
Authorization Advice/0120—System-generated	•	C	C

---

### Values

See subfields.

---

### Application Notes

---

This is a conditional field and must be provided by the acquirers' part of the authorization messages if they are participating and have previously authenticated using the Mastercard Identity Check or SecureCode program. This field will not be edited to ensure that these elements were provided on the transaction. If it is provided by the acquirer or processor, it must meet the specifications defined.

---

### Subfield 1—Program Protocol

DE 48 (Additional Data—Private Use), subelement 66 (Authentication Data), subfield 1 indicates the Program Protocol.

---

#### Attributes

---

Subfield ID	01
Length Field	2
Data Representation	an-1
Data Field	Contents of subfield 1
Justification	N/A

---

---

#### Values

---

1	=	3-D Secure Version 1.0 (3DS 1.0)
2	=	EMV 3-D Secure (3DS 2.0)

---

### Subfield 2—Directory Server Transaction ID

The Directory Server Transaction ID is generated by the EMV 3DS Mastercard Directory Server during the authentication transaction and passed back to the merchant with the authentication results. DE 48 (Additional Data—Private Use), subelement 66 (Authentication Data), subfield 2 allows the acquirer to pass the Directory Server Transaction ID during authorization in order to link authentication and authorization data.

---

#### Attributes

---

Subfield ID	02
Length Field	2
Data Representation	ans-36

---

---

#### Attributes

---

Data Field	Contents of subfield 2
Justification	N/A

---

---

#### Values

---

The Directory Server Transaction ID is a Universally Unique Transaction ID which can be provided by the processors/acquirers as part of the authentication transaction.

Example of a Directory Server Transaction ID: f38e6948-5388-41a6-bca4-b49723c19437

---

### **Subelement 67—MoneySend Information**

DE 48, subelement 67 (MoneySend Information) contains subfield representing the Sanction Screening Score.

---

#### Attributes

---

Subelement ID:	67
Data Representation:	ans...99; LLVAR
Length Field:	2
Data Field:	Contents of subfield 1
Subfields:	1
Justification:	see subfields

---

#### Usage

---

Following is the usage of subelement 67 (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—System-generated	•	X	C

#### Values

---

See subfields

---

---

### **Subfield 1—Sanction Screening Score**

DE 48, subelement 67, subfield 1 (Sanction Screening Score) contains the Sanction Screening Score populated by Mastercard.

---

#### **Attributes**

Subfield ID:	01
Data Representation:	n-3
Length Field:	2
Data Field:	Contents of subfield 1
Justification:	Right justified with leading zeros

---

#### **Values**

Sanction Screening Score value will be populated by Mastercard on all cross-border MoneySend Payment Transactions globally and domestic MoneySend Payment Transactions in Egypt, Canada, across Europe and the United States. The score is populated based on the Sender name (consumer, business, government, and non-government) matched against key screening lists such as the OFAC Specially Designated Nationals and Blocked Persons List, UN List, and EU List. The score will be 3 bytes and between a value of 000–100 or 999. A higher score indicates a closer match to names on the applicable screening lists, while lower scores indicate a less likely match. When a score cannot be determined, the value will be 999.

---

### **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
Data Representation:	ans...40; LLVAR
	The “LL” length field of LLVAR must be an integral multiple of 4, not to exceed 40.
Length Field:	2
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
Reversal Advice/0420	•	C	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

---

See the following section Subelement 71—Valid Subfield 1 and Subfield 2 Value Combinations.

---

### Subfield 2—On-behalf Result 1

DE 48, subelement 71, subfield 2 (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

---

See the following section Subelement 71—Valid Subfield 1 and Subfield 2 Value Combinations.

---

### **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 Field:	Contents of position 4
Justification:	N/A

#### **Values**

Mastercard use only. May contain a space or a value.

### **Subelement 71—Valid Subfield 1 and Subfield 2 Value Combinations**

Following is the valid DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services [OBS]), subfield 1 (On-behalf [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.

Attributes	Subfield 1 (OB Service)	Subfield 2 (OB Result 1)
Data Representation	an-2	an-1
Data Field	Contents of positions 1–2	Contents of position 3
Justification	Left-justified	N/A

**NOTE: DE 48, subelement 71 will contain all applicable, on-behalf service results that were performed on a given transaction; examples include Mastercard Digital Enablement Service (MDES) service results and Mastercard Identity Check service results.**

DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)	DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)
01 = Chip to Magnetic Stripe Conversion Service	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

<b>DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)</b>	<b>DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)</b>
	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
02 = M/Chip Cryptogram Pre-validation Service	A = Valid Application Cryptogram (AC); ATC outside allowed range
	E = Valid Application Cryptogram; ATC Replay
	F = Format Error
	G = Application Cryptogram is valid but not an ARQC nor a TC, status of TVR/CVR unknown
	I = Invalid Cryptogram
	K = No matching key file for this PAN, PAN expiry date and KDI combination
	T = Valid ARQC/TC and ATC; TVR/CVR invalid
	U = Unable to process
	V = Valid
	X = Security platform time out
	Z = Security platform processing error
03 = M/Chip Cryptogram Validation in Stand-In Processing	A = Valid Application Cryptogram (AC); ATC outside allowed range
	E = Valid Application Cryptogram; ATC Replay
	F = Format Error
	G = Application Cryptogram is valid but not an ARQC nor a TC, status of TVR/CVR unknown
	I = Invalid Cryptogram
	K = No matching key file for this PAN, PAN expiry date and KDI combination
	T = Valid ARQC/TC and ATC; TVR/CVR invalid
	U = Unable to process
	V = Valid
	X = Security platform time out
	Z = Security platform processing error

<b>DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)</b>	<b>DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)</b>
04 = M/Chip Cryptogram Regeneration Service	C = Regeneration of the M/Chip cryptogram was completed
05 = Mastercard® SecureCode™ AAV Verification Service	I = Invalid AAV
	K = No matching key file for this PAN, PAN expiry date and KDI combination
	U = Unable to process
	V = Valid
	X = Security platform time out
	Z = Security platform processing error
06 = Mastercard® SecureCode™ Dynamic AAV Verification in Stand-In Processing	I = Invalid AAV
	K = No matching key file for this PAN, PAN expiry date and KDI combination
	U = Unable to process
	V = Valid
	X = Security platform time out
	Z = Security platform processing error
08 = Online PIN Pre-validation (Europe Only)	I = Invalid PIN
	P = Mandatory PVV not on file
	R = PIN retry exceeded (invalid PIN)
	U = Unable to process
	V = Valid
09 = Online PIN Validation in Stand-In (Europe only)	I = Invalid PIN
	P = Mandatory PVV not on file
	R = PIN retry exceeded (invalid PIN)
	U = Unable to process
	V = Valid
10 = CVC 1 Validation Stand-In Service	I = Invalid CVC 1
	U = Unable to process
	V = Valid
11 = CVC 1 Pre-Validation Service	I = Invalid CVC 1

<b>DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)</b>	<b>DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)</b>
<b>NOTE: This service is not offered to issuers in the Russian Federation processing domestic transactions.</b>	K = No matching key file for this PAN, PAN Expiry date combination
	U = Unable to process
	V = Valid
<b>NOTE: Issuers that enroll account ranges in the OBS 11 (CVC 1 Pre-Validation Service) that are currently enrolled in OBS 10 (CVC 1 Validation Stand-In Service) must request the removal of those account ranges from the OBS 10 service.</b>	
14 = Contactless Mapping Service	C = Conversion of contactless account number to PAN was completed
	I = Invalid
	U = Unable to process
15 = Dynamic CVC 3 Pre-validation (with or without Contactless Mapping Service)	A = ATC outside allowed range (applicable when ATC value is dynamic [varying] value)
	E = CVC 3 ATC Replay
	I = Invalid CVC 3
	K = No matching key file for this PAN, PAN expiry date, and KDI combination
	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
	X = Security platform time out
	Z = Security platform system error

---

<b>DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)</b>	<b>DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)</b>
16 = Dynamic CVC 3 Validation in Stand-In Processing	A = ATC outside allowed range (applicable when ATC value is dynamic [varying] value)  E = CVC 3 ATC Replay  I = Invalid CVC 3  K = No matching key file for this PAN, PAN expiry date, and KDI combination
	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
	X = Security platform time out
	Z = Security platform system error
17 = In Control Virtual Card Service	A = Virtual Card Number (expiration date does not match)  B = Virtual Card Number (expiration date expired)  C = Virtual Card Number Virtual CVC 2 does not match  D = In Control Validity Period Limit  E = In Control Transaction Amount Limit Check  F = In Control Cumulative Amount Limit Check  G = In Control Transaction Number Usage  H = In Control Merchant ID Limit  I = In Control Invalid Virtual Card Number—Real Card Number mapping relationship  J = In Control MCC Limit  K = In Control Database Status Bad  L = In Control Geographic Restriction  M = In Control Transaction Type Restriction  P = In Control Transaction Time/Date Restriction

---

<b>DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)</b>	<b>DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)</b>
	U = Unable to process
	V = Valid
18 = Fraud Scoring Service	C = Fraud Scoring Service was performed successfully
	U = Fraud Scoring Service was not performed successfully
20 = In Control RCN Spend Control Service	D = In Control Validity Period Limit
	E = In Control Transaction Amount Limit Check
	F = In Control Cumulative Amount Limit Check
	G = In Control Transaction Number Usage
	H = In Control Merchant ID Limit
	J = In Control MCC Limit
	K = In Control Database Status Bad
	L = In Control Geographic Restriction
	M = In Control Transaction Type Restriction
	P = In Control Transaction Time/Date Restriction
	U = Unable to process
	V = Valid
25 = Account Data Compromise Information	Y = Compromised Event Data Found
	N = Compromised Event Data Not Found
	U = Unable to process
26 = Point-of-Interaction Service	A = Amount does not qualify for Installment
	E = Merchant ID does not qualify for installment
	F = PAN does not qualify for Installment
	I = Does not qualify for installment as the installment plan count exceeds the allowed limit
	M = MCC does not qualify for Installment
	N = Record not found
	P = Installment Parameters missing
	U = Unable to Process
	V = Qualified for Installment

<b>DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)</b>	<b>DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)</b>
31 = Chip CVC to CVC 1 Conversion Service—CVC 1 Key/Decision Matrix Only	C = Chip CVC Validated Successfully; Conversion of Chip CVC to CVC 1 Performed Successfully  F = Track Data Formatted Incorrectly  I = Chip CVC Invalid; Conversion of Chip CVC to CVC 1 Not Performed  K = Issuer CVC 1 Key Record <b>not</b> Found for Account Range / Expiry Date combination; Service Not Performed  U = Unable to process
32 = Chip CVC to CVC 1 Conversion Service—Separate Keys/Decision Matrices	C = Chip CVC Validated Successfully; Conversion of Chip CVC to CVC 1 Performed Successfully  F = Track Data Formatted Incorrectly  I = Chip CVC Invalid; Conversion of Chip CVC to CVC 1 Not Performed  K = Issuer Chip CVC Key Record <b>not</b> found and Issuer CVC 1 Key Record <b>not</b> found for Account Range / Expiry Date combination; Service Not Performed  L = Issuer CVC 1 Key Record <b>not</b> Found for Account Range / Expiry Date combination; Service Not Performed  M = Issuer Chip CVC Key Record <b>not</b> Found for Account Range / Expiry Date combination; Service Not Performed  U = Unable to process
33 = MoneySend Blocking Service	A = MoneySend Issuer Blocking—Transaction limit not allowed for the MoneySend Payment type  B = MoneySend Issuer Blocking—Merchant not allowed for the MoneySend Payment type  D = MoneySend Issuer Blocking—Country not allowed for the MoneySend Payment type  E = MoneySend Issuer Blocking—Domestic activity only allowed  F = MoneySend Issuer Blocking—Sanction Screening Score limit exceeded

<b>DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)</b>	<b>DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)</b>
G	= MoneySend Mastercard Blocking—Transaction limit not allowed for the MoneySend Payment type and Country
H	= MoneySend Mastercard Blocking—Merchant not allowed for the MoneySend Payment type
I	= MoneySend Mastercard Blocking—Cross-border not allowed for the MoneySend Payment type
J	= MoneySend Mastercard Blocking—MoneySend Transaction Count exceeded
K	= MoneySend Mastercard Blocking—Aggregate transaction amount limit exceeded
L	= MoneySend Issuer Blocking—MoneySend Transaction Count exceeded
M	= MoneySend Issuer Blocking—Aggregate transaction amount limit exceeded
N	= MoneySend Issuer Monitoring—MoneySend Transaction Count exceeded
O	= MoneySend Issuer Monitoring—Aggregate transaction amount limit exceeded
P	= MoneySend Issuer Monitoring—Transaction amount limit exceeded
Q	= MoneySend Issuer Monitoring—Sanction Screening Score exceeded
R	= MoneySend Issuer Blocking—Invalid Card
S	= MoneySend Mastercard Blocking—Product code invalid for the Transaction Type indicator
T	= MoneySend Mastercard Blocking—Transaction Amount limit not allowed for the MoneySend Funding transaction type
U	= Unable to process
V	= Valid
W	= MoneySend Mastercard Blocking—Country not allowed for the MoneySend Transaction

<b>DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)</b>	<b>DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)</b>
	X = MoneySend Mastercard Blocking—MoneySend Transaction—Invalid format
37 = Mastercard Merchant Presented QR Blocking Service	D = Mastercard Merchant Presented QR Blocking—Transaction Amount Limit Exceeded
	E = Mastercard Merchant Presented QR Blocking—Cumulative Transaction Amount Or Count Limit Exceeded
	F = Mastercard Merchant Presented QR Blocking—Domestic Activity Only
	U = Unable to Process
	V = Valid
50 = Mastercard Digital Enablement Service PAN Mapping	C = Conversion of Token to PAN completed successfully
	F = Format Error
	I = Invalid Token
	U = Unable to process
51 = Mastercard Digital Enablement Service Chip Pre-Validation	A = ATC outside allowed range (applicable when ATC value is dynamic [varying] value)
	E = ATC Replay
	F = Format Error
	G = Application Cryptogram is valid but not an ARQC nor a TC, status of TVR/CVR unknown
	I = Invalid Cryptogram
	K = No matching key file for this PAN, PAN expiry date and KDI combination
	T = Valid ARQC/TC and ATC; TVR/CVR invalid
	U = Unable to process
	V = Valid ARQC/TC and ATC and TVR/CVR
	X = Security platform time out
	Z = Security platform system error
52 = Mastercard Digital Enablement Service CVC 3 Pre-Validation	A = ATC outside allowed range (applicable when ATC value is dynamic [varying] value)
	E = CVC 3 ATC Replay

<b>DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)</b>	<b>DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)</b>
	H = Invalid Time Validation
	I = Invalid CVC 3
	K = No matching key file for this PAN, PAN expiry date, and KDI combination
	N = Unpredictable Number Length Indicator Mismatch
	U = Unable to process
	V = Valid
	X = Security platform time out
	Z = Security platform system error
61 = Mastercard Digital Enablement Service Cloud-based Payments Chip Pre-Validation Service	D = ATC Invalid—Not in list of currently active Single-Use Keys
	E = ATC Replay
	F = Format Error
	I = Invalid MD AC and UMD AC
	K = No matching key file for this PAN, PAN expiry date and KDI combination
	L = Invalid MD AC; Valid UMD AC
	M = Valid MD AC; Invalid UMD AC (Mobile PIN Try Counter Max Limit Reached, Token Suspended)
	P = Valid MD AC; Invalid UMD AC (Invalid Mobile PIN)
	T = Invalid TVR/CVR
	U = Unable to process
	V = Valid
	X = Security platform time out
	Z = Security platform system error
62 = Mastercard Digital Enablement Service Cloud-based Payments Magnetic Stripe Pre-Validation Service	D = ATC Invalid—Not in list of currently active Single-Use Keys
	E = ATC Replay
	F = Format Error
	I = Invalid MD AC and UMD AC

<b>DE 48, Subelement 71, Subfield 1 (OB Service) Values (an-2)</b>	<b>DE 48, Subelement 71, Subfield 2 (OB Result 1) Values (an-1)</b>
H	= Invalid Time Validation
K	= No matching key file for this PAN, PAN expiry date and KDI combination
L	= Invalid MD AC; Valid UMD AC
M	= Valid MD AC; Invalid UMD AC (Mobile PIN Try Counter Max Limit Reached, Token Suspended)
N	= Unpredictable Number Length Indicator Mismatch
P	= Valid MD AC; Invalid UMD AC (Invalid Mobile PIN)
U	= Unable to process
V	= Valid
X	= Security platform time out
Z	= Security platform system error

## **Subelement 72—Issuer Chip Authentication**

DE 48, subelement 72 (Issuer Chip Authentication) carries data used during cryptogram processing.

---

### Attributes

---

Subelement ID:	72
Data Representation:	b...16; LLVAR (the “LL” length field of LLVAR must be between 8–16 positions.)
Length Field:	2
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 Advice/0120—System-generated	•	C	C

---

### Values

---

Mastercard generated.

---

---

### Application Notes

---

Issuers no longer need to echo DE 48, subelement 72 in their response messages.

---

## 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

---

Data Representation: an...30; LLVAR

The “LL” length field of LLVAR must be an integral multiple of 3 not to exceed 30.

---

Length Field: 2

---

Data Field: Contents of subfields

---

Subfields: 2

---

Justification: See subfields

---

### Usage

---

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
-------------------------------------	---	---	---

---

### Values

---

See subfields

---

### Application Notes

---

DE 48, subelement 74 is not applicable in the 0120/0130, 0400/0410 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.

---

### Chip Fallback Transaction Downgrade

---

The Dual Message System will include DE 48, subelement 74 in the Authorization Request Response/0110 message when the transaction is eligible for the Chip Fallback Transaction Downgrade. In which case DE 48, subelement 74, subfield 1 value will be “90” and subfield 2 value will be “C”. Refer to the DE 22—Point-of-Service (POS) Entry Mode section for additional details.

---

---

<b>When the issuer sends an Authorization Request Response/0110 message containing DE 48, subelement 74 and...</b>	<b>THEN the Authorization Platform...</b>
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.

---

<b>Attributes</b>	
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 (Processing Information) contains additional information about the issue incurred during chip transaction processing.

---

<b>Attributes</b>	
Data Representation:	an-1

---

---

Data Field:	Additional information being provided about the service
Justification:	N/A
<b>Values</b>	
A =	Valid Application Cryptogram (AC); Application Transaction Counter (ATC) outside allowed range
C =	Completed Successfully
E =	Valid Application Cryptogram; ATC Replay
F =	Format error in DE 55
G =	Application Cryptogram is valid but is not an ARQC
I =	Application Cryptogram invalid
K =	No matching key file for this PAN, PAN expiry date and KDI combination
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
X =	Security platform time out
Z =	Security platform processing error

---

#### **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.

---

IF subfield 1 contains...	THEN subfield 2 may contain...
02	A, E, F, G, I, K, T, U, X, or Z
03	A, E, F, G, I, K, T, U, X, or Z
50	A, E, F, G, I, T, U, or X
90	C

---

#### **Subelement 75—Fraud Scoring Data**

DE 48, subelement 75 (Fraud Scoring Data) indicates the fraud score on a fraud scoring service transaction.

Mastercard provides two scoring solutions: Expert Monitoring for Issuers or Decision Intelligence. A score will be included in Authorization Request/0100 and Authorization Advice/0120—System-generated messages to the issuer when the Expert Monitoring or Decision Intelligence scoring was performed on a transaction.

Attribute	Description
Subelement ID:	75
Data Representation:	an...32; LLVAR
Length Field:	2
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 and applicable subfields 3–5

### Application Notes

The Authorization Platform inserts this subelement when one of the Fraud Scoring Services is performed or when both a Fraud Scoring Service and the Fraud Rule Manager Service are performed on the transaction.

**NOTE: 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.**

**NOTE: Issuers participating in a scoring service will receive subfields 1–2. If those issuers choose to participate in the Fraud Rule Manager Service then those issuers must also prepare to receive subfields 3–5.**

**NOTE: DE 48, subelement 75 will not be included in Authorization Request/0100 messages to the issuer when Mastercard is unable to perform the Fraud Scoring Service.**

Expert Monitoring for Issuers and Decision Intelligence services evaluate fraud detection elements to produce a score that indicates a level of risk in the transaction. Both services utilize the same DE 48, subelement 75 field with dual message authorization transactions.

Expert Monitoring for Issuers provides best-in-class transaction fraud monitoring that enables Mastercard issuers to evaluate and manage the probability of fraud in transactions at the point of interaction. As an integrated, multi-component, transaction fraud monitoring solution, Expert Monitoring provides:

- Network fraud monitoring
- Customized fraud rule management
- Finely tuned fraud detection models
- Predictive, real-time fraud scoring

Decision Intelligence is a real-time authorization decisioning solution that applies thousands of data points and sophisticated modeling techniques to each transaction, simplifying these insights into a single transaction decision score that helps issuers to fine-tune their authorization decisions with the goal of approving genuine transactions and declining fraudulent ones.

For additional details on these services, refer to the Mastercard Fraud Scoring Services section in the Program and Service Format Requirements chapter of this manual.

---

### **Subfield 1—Fraud Score**

DE 48, subelement 75, subfield 1 (Fraud Score) indicates the transaction risk score.

---

#### **Attribute**

Subfield ID:	01
Data Representation:	an-3
Length Field:	2
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
--------------	----

---

---

Data Representation: an-2

Length Field: 2

Data Field: Contents of positions 1–2

Justification: N/A

---

#### Values

The 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 Score

DE 48, subelement 75, subfield 3 (Rules Score) contains the Fraud Rule Manager Service, rules score.

---

#### Attributes

Subfield ID: 03

Data Representation: an-3

Length Field: 2

Data Field: Contents of positions 1–3

Justification: N/A

---

#### Values

The Fraud Rule Manager Service provides a rules 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 (Rules Reason Code 1) indicates the data used to derive the rule adjusted score.

---

#### Attributes

Subfield ID: 04

Data Representation: an-2

Length Field: 2

Data Field: Contents of positions 1–2

Justification: N/A

---

### Values

---

The Fraud Rule Manager 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 (Rules Reason Code 2) indicates the data used to derive the rule adjusted score.

---

### Attributes

---

Subfield ID:	05
Data Representation:	an-2
Length Field:	2
Data Field:	Contents of positions 1–2
Justification:	N/A

---

### Values

---

The Fraud Rule Manager Service provides the rule reason code, an alphanumeric code where the information provided gives the data used to derive the rules adjusted score.

---

### Application Notes

---

Mastercard will require all issuing and acquiring processors to code for, support, and integrate into their systems the data elements, subelements, and values associated with this item.

The following provides the Global Safety and Security Standards effective dates for each region.

- USA: 21 Apr 2017
- EUR: 13 Oct 2017; Ukraine: 1 Apr 2018
- LAC: 13 Oct 2017
- MEA: 13 Oct 2017
- AP: 13 Apr 2018
- CAN: 13 Apr 2018

For additional information about the requirement please refer to the *Global Safety and Security Standards Roadmap*.

**NOTE: Mastercard does not require issuers or acquirers to enroll in these optional products and services, but they must code their systems to support these fields to leverage such products and services in a timely manner in the event of a security issue.**

---

## Subelement 76—Mastercard Electronic Acceptance Indicator

DE 48, subelement 76 (Mastercard Electronic Acceptance Indicator) identifies that the transaction is a Mastercard Electronic card transaction. It indicates that the acquirer participates or does not participate in Mastercard Electronic card processing.

### Attributes

Subelement ID: 76

Data Representation: a-1

Length Field: 2

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).

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 Card 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—Funding/Payment Transaction Type Indicator**

DE 48, subelement 77 (Funding/Payment Transaction Type Indicator) indicates the type of Funding/Payment Transaction taking place. **NOTE: All MoneySend Funding and Payment Transactions require the presence of this indicator.**

---

#### **Attributes**

Subelement ID:	77
Data Representation:	an-3
Length Field:	2
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
<b>Values</b>			
C01 = Person-to-Person			
C02 = Mastercard rebate			
C03 = rePower 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 = MoneySend Person-to-Person			
C09 = Card Activation			
C51 = MoneySend Additional Funding/Payment Indicator (Reserved for Future Use)			
C52 = MoneySend Account-to-Account Transfers			
C53 = MoneySend Agent Cash Out			
C54 = MoneySend Credit Card Bill Payment			
C55 = MoneySend Business Disbursement			
C56 = MoneySend Government/Non-profit Disbursement			
C57 = MoneySend Acquirer Merchant Settlement			
C58 = MoneySend Cash2ATM (Usage limited to specific countries)			
C59 = MoneySend Cash2Card (Usage limited to specific countries)			
C60 = MoneySend Additional Funding/Payment Indicator (Reserved for Future Use)			
C61 = MoneySend Additional Funding/Payment Indicator (Reserved for Future Use)			
C62 = MoneySend Additional Funding/Payment Indicator (Reserved for Future Use)			
C63 = MoneySend Additional Funding/Payment Indicator (Reserved for Future Use)			
C64 = MoneySend Additional Funding/Payment Indicator (Reserved for Future Use)			
C65 = MoneySend Additional Funding/Payment Indicator (Reserved for Future Use)			
C66 = MoneySend Additional Funding/Payment Indicator (Reserved for Future Use)			
C67 = Mastercard Merchant Presented QR			
C68 = Mastercard Merchant Presented QR Refund			
C91 = Utility Payments—Brazil domestic transactions			
C92 = Government Services—Brazil domestic transactions			
C93 = Mobile phone top-ups—Brazil domestic transactions			
C94 = Coupon Booklet Payments (CARNE)—Brazil domestic transactions			

---

P01 = Mastercard ATM Cash Pick-Up Transaction

---

### **Application Notes**

---

If DE 3, subfield 1 contains value 28 (Payment Transaction), then DE 48, subelement 77 must be present.

If DE 3, subfield 1 contains value 00 (Purchase of Goods and Services) and DE 18 contains value 6538 (MoneySend Funding), 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 and new payment type codes C52–C57 and C67 is limited to eligible countries and eligible acquirers. Refer to the *MoneySend Program Guide*.

Usage of value C09 is limited to Private Label Prepaid Cards issued in the Europe region.

Usage of value C67 is limited to Mastercard Merchant Presented QR transactions.

---

Usage of value C68 is limited to Mastercard Merchant Presented QR refund transactions.

**NOTE: Value C68 is effective as of 12 June 2018.**

---

## **Subelement 78—Payment Service Indicators (Visa Only)**

DE 48, subelement 78 (Payment Service Indicators [Visa Only]) contains subfields which represent various Visa payment service indicators.

---

### **Attributes**

---

Subelement ID:	78
Data Representation:	ans-6
Length Field:	2
Data Field:	Contents of positions 1–6
Subfields:	6
Justification:	See subfields

---

### **Usage**

---

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	C	•	C
Reversal Request/0400	C	•	C
Reversal Request Response/0410	C	•	C

---

---

### Values

---

See subfields.

---

### Application Notes

---

Acquirers are not required to populate this subelement in the Authorization Request/0100 if they do not support any of the Visa payment indicators in subfields 2 through 6 as noted below.

---

### Subfield 1—Spend Qualified Indicator

DE 48, subelement 78, subfield 1 (Spend Qualified Indicator) provides the Visa spend qualification assessment.

---

### Attributes

---

Data Representation: ans-1

---

Data Field: Contents of position 1

---

Justification: N/A

---

### Values

---

Space	Space will be sent back in the Authorization Request Response/0110 message to the acquirer when Visa field 62.25 is not present in the Visa 0110 message response
N	Spend assessment threshold defined by Visa has not been met
B	Basic spend assessment threshold level met
Q	Highest spend assessment threshold level met

---

### Application Notes

---

The value for this field is mapped from Visa field 62.25—Spend Qualified Indicator. Refer to the Visa Base I Technical Specifications manual. Acquirers will need to populate subfield 1 with a “Space” if any other Payment Service Indicator is submitted in the Authorization Request/0100 and Reversal Request/0400 message. “Space” will be sent back in subfield 1 to the acquirer if any other Payment Service Indicator is returned back in Authorization Request Response/0110 and Reversal Request Response/0410 messages.

**NOTE: The Spend Qualified Indicator is used by acquirers for Visa's Account Level Processing (ALP) program.**

---

### Subfield 2—Dynamic Currency Conversion Indicator

DE 48, subelement 78, subfield 2 (Dynamic Currency Conversion Indicator) indicates a transaction for which Dynamic Currency Conversion (DCC) is performed by the merchant at the point of sale.

---

#### Attributes

---

Data Representation: ans-1

---

Data Field: Contents of position 2

---

Justification: N/A

---

#### Values

---

Y Dynamic Currency Conversion was performed at the point of sale.

---

Space No Dynamic Currency Conversion or not echoed in the Authorization Request Response/0110 or Reversal Request Response/0410 message.

---

#### Application Notes

If the merchant performs dynamic currency conversion at the point of sale, acquirers must send this value in the Authorization Request/0100 message and in Reversal Request/0400 message in case of Reversal. This value will be mapped to Visa Field 126.19—Dynamic Currency Conversion Indicator. Refer to the Visa Base I Technical Specifications manual. The acquirer will need to populate subfield 2 with a space if DCC was not performed and any other Payment Service Indicator is submitted in the Authorization Request/0100. “Space” will be sent back in subfield 2 to the acquirer if any other Payment Service Indicator is returned back in Authorization Request Response/0110 message.

**NOTE: Dynamic Currency Conversion (DCC) provides the cardholder the option to pay for goods or services in their own billing currency. DCC occurs when a merchant performs currency conversion locally and submits the transaction in the cardholder's billing currency. Acquirers must ensure that they receive an indicator from their merchants when DCC is performed for a Visa transaction.**

---

#### Subfield 3—U.S. Deferred Billing Indicator

DE 48, subelement 78, subfield 3 (U.S. Deferred Billing Indicator) indicates a transaction for which the billing for merchandise occurred after the merchandise was delivered to the cardholder. This applies to U.S. region acquirers only.

---

#### Attributes

---

Data Representation: ans-1

---

Data Field: Contents of position 3

---

Justification: N/A

---

#### Values

---

D U.S. Deferred Billing Indicator

---

Space No Deferred Billing or not echoed in Authorization Request Response/0110 message

---

#### Application Notes

---

This code is provided by the merchant through U.S. region acquirers in the Authorization Request/0100 message to indicate that a Visa card is to be billed on a deferred basis, that is, the cardholder is to be billed for merchandise already received. This value will be mapped to Visa field 126.12—Service Indicators, position 3 (Deferred Billing Indicator). Refer to the Visa Base I Technical Specifications manual. Acquirers will need to populate subfield 3 with a “Space” if Deferred Billing is not applicable and any other Payment Service Indicator is submitted in the Authorization Request/0100 and Reversal Request /0400 message. “Space” will be sent back in subfield 3 to the acquirer if any other Payment Service Indicator is returned back in Authorization Request Response/0110 and Reversal Request Response/0410 messages.

---

#### **Subfield 4—Visa Checkout Indicator**

DE 48, subelement 78, subfield 4 (Visa Checkout Indicator) indicates that the transaction was processed through Visa Checkout.

---

##### **Attributes**

---

Data Representation: ans-1

---

Data Field: Contents of position 4

---

Justification: N/A

---

<b>Values</b>	<b>Description</b>
Y	Transaction is processed through Visa Checkout
Space	No Visa Checkout or not echoed in the Authorization Request Response/0110 message

---

##### **Application Notes**

---

If the transaction is performed through Visa Checkout, acquirers must send this value in the Authorization Request/0100 message. This value will be mapped to Visa Field 126.18—Agent Unique Account Result. Refer to the Visa Base I Technical Specifications manual. The acquirer will need to populate subfield 4 with a space if Visa Checkout was not performed and any other Payment Service Indicator is submitted in the Authorization Request/0100 and Reversal Request/0400 messages. “Space” will be sent back in subfield 4 to the acquirer if any other Payment Service Indicator is returned back in Authorization Request Response/0110 and Reversal Request Response/0410 messages.

---

#### **Subfield 5—Message Reason Code**

DE 48 (Additional Data—Private Use), subelement 78 (Payment Service Indicators [Visa Only]), subfield 5 provides the message reason code of the transaction.

---

##### **Attributes**

---

Data Representation: ans-1

---

Data Field: Contents of position 5

---

Justification: N/A

---

---

#### Values

Space	Default (No message reason code associated with this transaction)
0	Incremental authorization
1	Resubmission
2	Delayed charges
3	Reauthorization
4	No show
5	Account top up

#### Application Notes

Acquirers must send the value based on the transaction in the Authorization Request/0100 and Reversal Request/0400 message. This value will be mapped to Visa Field 63.3 Message Reason Code. Refer to the *Visa Base I Technical Specifications* manual.

---

#### Subfield 6—Reserved for Future Use

DE 48, subelement 78, subfield 6 (Reserved for Future Use) is reserved for future use.

---

#### Attributes

Data Representation:	ans-1
Data Field:	Contents of position 6
Justification:	N/A

---

#### Values

Space	Reserved for future use
-------	-------------------------

#### 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
Data Representation:	an...50; LLVAR  The "LL" length field of LLVAR must be an integral multiple of 5, not to exceed 50.
Length Field:	2

---

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.

Refer to 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.

Refer to 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 (CVR or TVR Identifier) indicates whether bit reported in error is part of CVR or TVR.

---

#### Attributes

---

Data Representation: an-1

---

Data Field: Contents of position 1

---

Justification: N/A

---

#### **Values**

---

C = CVR

---

T = TVR

---

### **Subfield 2—Byte ID**

DE 48, subelement 79, subfield 2 (Byte ID) 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 (Value of Bit in Error) 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

---

##### **Values**

---

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

---

Data Representation: a-2

---

Length Field: 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**

---

PD	=	The Authorization Platform dropped the PIN (Mastercard Use Only for Credit Transactions with PIN)
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.

## **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
Data Representation:	n-2
Length Field:	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
----	---	------------------------------------

### **Application Notes**

---

Mastercard will require all issuing and acquiring processors to code for, support, and integrate into their systems the data elements, subelements, and values associated with this item.

The following provides the Global Safety and Security Standards effective dates for each region.

- USA: 21 Apr 2017
- EUR: 13 Oct 2017; Ukraine: 1 Apr 2018
- LAC: 13 Oct 2017
- MEA: 13 Oct 2017
- AP: 13 Apr 2018
- CAN: 13 Apr 2018

For additional information about the requirement please refer to the *Global Safety and Security Standards Roadmap*.

**NOTE: Mastercard does not require issuers or acquirers to enroll in these optional products and services, but they must code their systems to support these fields to leverage such products and services in a timely manner in the event of a security issue.**

---

### **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
Data Representation:	a-1
Length Field:	2
Data Field:	Contents of position 1
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 address 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.
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.

#### Application Notes

---

Mastercard will require all issuing and acquiring processors to code for, support, and integrate into their systems the data elements, subelements, and values associated with this item.

The following provides the Global Safety and Security Standards effective dates for each region.

- USA: 21 Apr 2017
- EUR: 13 Oct 2017; Ukraine: 1 Apr 2018
- LAC: 13 Oct 2017
- MEA: 13 Oct 2017
- AP: 13 Apr 2018
- CAN: 13 Apr 2018

For additional information about the requirement please refer to the *Global Safety and Security Standards Roadmap*.

**NOTE: Mastercard does not require issuers or acquirers to enroll in these optional products and services, but they must code their systems to support these fields to leverage such products and services in a timely manner in the event of a security issue.**

---

## Subelement 84—Merchant Advice Code

DE 48, subelement 84 (Merchant Advice Code) contains the merchant advice code.

---

### Attributes

---

Subelement ID:	84
Data Representation:	an-2
Length Field:	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
Authorization Advice/0120—System-generated	•	C	C

---

### Values

---

01	=	New account information available
02	=	Cannot approve at this time, try again later
03	=	Do not try again
04	=	Token requirements not fulfilled for this token type
21	=	Payment Cancellation (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 alphanumeric value in Visa Field 39 (Response Code).

Attributes		
Subelement ID:	84	
Data Representation:	an-2	
Length Field:	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—Account Status (Visa Only)**

DE 48, subelement 85 (Account Status [Visa Only]) identifies the account range as regulated or non-regulated interchange.

Attributes
Subelement ID: 85

---

Data Representation:	a-1
Length Field:	2
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

---

#### **Usage**

Following is the usage of subelement 85 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:	Org	Sys	Dst
Authorization Request Response/0110	C	•	C

---

#### **Values**

R = Account is regulated

N = Account is non-regulated

### **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
Data Representation:	a-1
Length Field:	2
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

---

C = Credential on File

---

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

---

Data Representation: a-1

---

Length Field: 2

---

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 87 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—System-generated	•	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.)

Refer to Application Notes section that follows for Stand-In System considerations.

---

#### 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

---

### **Application Notes**

---

If the issuer participates in the CVC 1 validation service and the transaction meets the criteria for the CVC 1 test, the Stand-In System considers the results of the CVC 1 validation in subelement 87 when responding to the Authorization Request/0100 message. The issuer can control the response that the Stand-In System uses when the CVC 1 value is invalid or validation cannot be performed. The default value is 05 (Do Not Honor). To change these values, contact Key Management Services at key\_management@Mastercard.com.

---

## **Subelement 87—CVV2 Response (Visa Only)**

DE 48, subelement 87 (CVV2 Response) indicates the CVV2 response on a Visa account.

---

### Attributes

---

Subelement ID:	87
Data Representation:	a-1
Length Field:	2
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	
Data Representation:	a-1	
Length Field:	2	
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	

---

---

Data Representation:	a-1
Length Field:	2
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
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**

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
Data Representation:	a-1

---

---

Length Field:	2
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 [Visa Only]) contains the Authorization Characteristics Indicator (Visa field 62.1).

---

Attributes	
Subelement ID:	90
Data Representation:	a-1
Length Field:	2
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

I	=	Incremental authorization
P	=	Preferred customer
R	=	Recurring payment
Y	=	Request for Custom Payment Service participation

#### Application Notes

---

Refer to Visa Base I Technical Specifications manual for a list of all CPS request values in Visa field 62.1.

---

### 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
Data Representation:	a-1
Length Field:	2
Data Field:	Contents of position 1
Subfields:	N/A
Justification:	N/A

#### Usage

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 Response/0110	C	•	C
Reversal Request Response/0410	C	•	C

#### Values

---

Acquirer receives Visa CPS response code, see application notes

---

---

### Application Notes

---

If the request qualifies for Visa CPS and is approved, refer to the Visa Base I Technical Specifications manual for a complete list of CPS-qualified codes in Visa field 62.1. If the original request does not qualify for CPS, Visa returns an “N” or “T” in the response.

---

## 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
Data Representation:	ans...15; LLVAR
Length Field:	2
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
Data Representation:	an...19; LLVAR
Length Field:	2
Data Field:	Contents of positions 1–19
Subfields:	N/A

---

### Usage

---

---

Subelement 91 is used to provide transaction ID and/or Validation Code when subelement 90 indicates an incremental authorization or when submitting a reversal 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/or validation code (Visa field 62.3, 4 bytes alphanumeric) when subelement 90 indicates an incremental authorization or when submitting a 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
Data Representation:	ans...19; LLVAR
Length Field:	2
Data Field:	Contents of positions 1–4, 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
Reversal Request Response/0410	C	•	C

---

#### Values

---

##### When length field is 04:

Subelement 91 contains the Visa CPS validation code (Visa field 62.3, four bytes alphanumeric). Refer to the Visa Base I Technical Specifications manual for more information on Visa CPS validation codes.

---

##### When length field is 15:

---

Subelement 91 contains the transaction ID (Visa field 62.2, 15 bytes numeric).

---

**When length field is 19:**

---

Subelement 91 contains the transaction ID (Visa field 62.2, 15 byte numeric) and CPS validation code (Visa field 62.3, four bytes alphanumeric).

---

## **Subelement 92—CVC 2**

DE 48 (Additional Data—Private Use), subelement 92 contains the CVC 2 value from the signature panel of the card.

---

### **Attributes**

Subelement ID:	92
Data Representation:	n-3
Length Field:	2
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
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.

---

### **Application Notes**

The contents of DE 48, subelement 92—when populated—are passed to the Dual Message System (Authorization) issuer in transactions acquired through the Single Message System.

---

---

For Mastercard Digital Enablement Service (MDES) transactions, DE 48, subelement 92 must be populated when provided by the merchant; it might contain a Dynamic Token Verification code.

---

## **Subelement 92—CVV2 Data (Visa Only)**

DE 48 (Additional Data—Private Use), subelement 92 (CVV2 Data) consists of the Visa CVV2 presence ID, response type, and CVV2 value.

---

### **Attributes**

Subelement ID:	92
Data Representation:	ns-6
Length Field:	2
Data Field:	Contents of positions 1, 2, and 3–6
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

---

#### **Positions 3-6 (CVV2 Value)**

---

Data Representation:	ns-4
Justification:	Right, blank-filled
Data Field:	Contents of positions 3–6
Values:	CVV2 value from the signature panel of the card. Blank or space-fill as needed. No other special character is allowed.

---

### **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
Data Representation:	ans...19; LLVAR
Length Field:	2
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

---

### **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
Data Representation:	ans-4
Length Field:	2
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
----------------------------	---	---	---

---

#### **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
Data Representation:	ans-4
Length Field:	2
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 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 product for a specific program or service established between issuers and merchants.

### **Attributes**

Subelement ID:	95
Data Representation:	an-6
Length Field:	2
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
Authorization Advice/0120—Acquirer-generated	C	•	C
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE
Reversal Advice/0420	•	C	C

### **Values**

Program or service specific.

ARGCTA	=	Installment payment transaction within Argentina
AGROF1	=	Mastercard Agro Card
BNDES1	=	Brazil intracountry transactions using the Mastercard BNDES Card
CHLCTA	=	Installment payment transaction within Chile
COLCTA	=	Installment payment transaction within Colombia
GREECE	=	Installment payment transaction within Greece
HGMINS	=	Installment payment transaction for Georgia
MCGARS	=	Identifies Global Automated Service (GARS) Stand-In activity

MCINST	=	Installment payment transaction
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
Data Representation:	n-4
Length Field:	2
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.

#### **Attributes**

Subelement ID:	96
----------------	----

---

Data Representation:	a-1
Length Field:	2
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
E =	Electronic commerce transaction aggregation
H =	Hotel rental
J =	B2B invoice payments
M =	Healthcare—Medical
N =	Failed market-specific data edit
T =	Transit (in healthcare transactions only)

---

## 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
Data Representation:	a-1
Length Field:	2
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 (Additional Data—Private Use), 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
Data Representation:	n...6; LLVAR
Length Field:	2 positions
Data Field:	Variable length, contents of subelement
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
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 (Additional Data—Private Use), 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
Data Representation:	n...6; LLVAR
Length Field:	2 positions
Data Field:	Variable length, contents of subelement
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, Proper Formatting

The Authorization Platform will perform the following system edit to verify proper formatting of DE 48.

WHEN...	THEN the Authorization Platform...
An Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or Reversal Request/0400 message contains DE 48 (Additional Data—Private Use), DE 108 (MoneySend Reference Data), or DE 112 (Additional Data [National Use]) with subelements that have incorrect length and/or incorrect format (Data Representations), or have multiple instances of the same subelement (when not permitted) within the same data element.	Rejects the message and forwards the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 message where DE 44 is 6 positions for subelement format errors: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Message format error)</li><li>• DE 44 (Additional Response Data) = 0480nn, or 1080nn, or 1120nn (where nn is the subelement number)</li></ul> (DE 44 is three positions for Dual Message System (Authorization) if no subelements are present, for example, for DE 22 format error: DE 44 = 022)

Examples:

- When an edit error occurs on DE 48, the DE 44 data will be populated as these examples below:
  - Error on DE 48 subelement 42, subfield 1: 048042 (no subfield information is provided)
  - Error on DE 48 subelement 61: 048061
- DE 48 TCC format error will be responded with DE 44 = 048000.

For non-DE 48/DE 108/DE 112 format errors, DE 44 will only have DE info and no subelement information. For example, the format error in DE 22 will have DE 44 as 022 for non-DE48/108/112 data elements.

### 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 = 048000</li> </ul>

### **DE 48, TCC and DE 3**

The Authorization Platform 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>
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
<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>

---

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 14**

The Authorization Platform will perform the following system edits.

#### **Combo Cards with a Single PAN**

---

WHEN...	THEN the Authorization Platform...
The Authorization Request/0100, the Authorization Advice/0120—Acquirer-generated, or the Reversal Request/0400 message contains DE 48 (Additional Data—Private Use), subelement 14 (Account Type Indicator) with values other than C (Credit Transaction) or D (Debit Transaction)	Will reject the transaction and forward the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or a Reversal Request Response/0410 with <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 048014 (indicating the data element in error)</li> </ul>

---

#### **DE 48, Subelement 26**

The Authorization Platform performs the following edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The Authorization Request/0100 or Authorization Advice/0120 message includes DE 48 (Additional Data—Private Use), subelement 26 (Wallet Program Data), subfield 1 (Wallet Identifier) with any combination other than a valid numeric value</p> <p><b>NOTE: Special characters, spaces, or all zeros not allowed.</b></p>	<p>Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130—System-generated where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 048026 (indicating the data element in error)</li> </ul>

### **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>
<p>The acquirer sends an Authorization Request/0100 message containing DE 48 (Additional Data—Private Use), subelement 35 (Contactless Non-Card Form Factor Request/Response)</p>	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30 (Format error)</li> <li>• DE 44 = 048035</li> </ul>

The issuer-branded website will perform the following processing based on the Authorization Request Response/0110 messages.

<b>WHEN...</b>	<b>THEN the issuer-branded website...</b>
<p>The Authorization Request Response/0110 message contains DE 48, subelement 35, value A</p>	<p>Arranges for the request contactless card or device to be sent to the cardholder</p>
<p>The Authorization Request Response/0110 message contains DE 48, subelement 35, value D</p>	<p>Declines the cardholder's request for the contactless card or device and instructs the cardholder to contact the issuer for more information</p>

<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 contactless card or device to be sent to the cardholder when:</p> <p>Subelement 83 (Address Verification Service Response) is X or Y</p> <p>and</p> <p>Subelement 87 (Card Validation Code Result) is M</p>
---	---

### **DE 48, Subelement 37**

The Authorization Platform performs the following edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>DE 48 (Additional Data—Private Use), subelement 37 (Additional Merchant Data), subfields 1 (Payment Facilitator ID) or 2 (Independent Sales Organization ID) has values other than 0–9 or contains all zeros in the Authorization Request/0100 or Authorization Advice/0120—Acquirer-generated message</p>	<p>Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = value 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = value 048037 (indicating the data element in error)</li> </ul>
<p>DE 48, subelement 37, subfield 3 (Sub-Merchant ID) contains all spaces or all zeros in the Authorization Request/0100 or Authorization Advice/0120—Acquirer-generated message</p>	<p>Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = value 30</li> <li>• DE 44 = value 048037</li> </ul>

### **DE 48, Subelement 38**

The Authorization Platform performs the following edits.

<b>WHEN...</b>	<b>THEN...</b>
<p>The Authorization Platform finds that the entire account range no longer participates in Enhanced Value, Product Graduation, or High Value 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 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> <li>• 10 (Partial Approval)</li> <li>• 87 (Purchase Amount Only, No Cash Back Allowed)</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>
<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>

<b>WHEN...</b>	<b>THEN...</b>
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	The Authorization Platform rejects the Authorization Request Response/0110 message and sends the Authorization Request/0100 message to the Stand-In System for processing.  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 original Authorization Request/0100 message.
DE 48, subelement 38 is included in the Authorization Request Response/0110 message from the issuer	The Authorization Platform removes DE 48, subelement 38 from the Authorization Request Response/0110 message before providing the 0110 message to the acquirer.

### **DE 48, Subelement 42 and Subelement 43**

The Authorization Platform performs the following system edits.

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	Must contain UCAF data.
2 or 3 and PAN is not Mastercard Electronic	Must contain UCAF data.
5	Must contain UCAF data.
<b>IF this edit...</b>	<b>THEN the Authorization Platform...</b>
Fails	Rejects the transaction with a format error, indicated by:  DE 39 = 30  DE 44 = 048043
Passes	The Authorization Platform goes to the next edit.

<b>WHEN DE 48, subelement 43...</b>	<b>THEN DE 48, subelement 42, subfield 01, position 3 must equal...</b>
Contains UCAF data	1, 2, 3, or 5
Does not contain UCAF data	0, 1, or 6, or not be present
<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) = 048043 (indicating the data element in error)
Passes	The Authorization Platform goes to the next edit.

The Authorization Platform performs the following edits on Authorization Request/0100 messages.

#### **DSRP partial shipments or recurring payments, where SLI value is not 247**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DSRP transaction initiated with a Secure Element or Cloud token, DE 22, subfield 1 = 81 (POS entry mode) and the Authorization Request/0100 contains DE 48, subelement 42, not equal to 247 and DE 48, subelement 43 is not present	Rejects the transaction with <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 0480nn (where nn is the subelement number)</li> </ul>

**Non-DSRP transactions initiated with an MDES token and submitted with a merchant attempt SecureCode AAV**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
A transaction initiated with a Secure Element or Cloud token, DE 22, subfield 1 = 81 (POS entry mode) and the Authorization Request/0100 request contains DE 48, subelement 43, pos1 = h (Merchant Attempt SecureCode AAV)	<p>If dynamic expiration date and dynamic token verification code was successfully validated by the MDES service, then the Authorization Platform goes to the next edit, otherwise rejects the transaction with</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 0480nn (where nn is the subelement number)</li> </ul>

**DE 48, Subelement 43 (Static AAV)**

The following edits on Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages are performed on transactions submitted under the Maestro Recurring Payments Program, the Mastercard Utility Payment Program, and the Maestro Low Risk Merchant Program.

<b>WHEN the Mastercard assigned static AAV in DE 48, subelement 43, position 1 begins with...</b>	<b>THEN the Authorization Platform...</b>
3 and the acceptance brand is not Maestro	<p>Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where:</p> <p>DE 39 (Response Code) = 30 (Format error)</p> <p>DE 44 = 048043 (identifying the data element in error)</p>
5 and the acceptance brand is not Maestro	<p>Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where:</p> <p>DE 39 = 30</p> <p>DE 44 = 048043</p>

---

<b>WHEN the Mastercard assigned static AAV in DE 48, subelement 43, position 1 begins with...</b>	<b>THEN the Authorization Platform...</b>
Any value other than 3 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 = 048043

---

#### **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>
Fails	Generates a format error indicated by:  DE 39 = 30  DE 44 = 061

---

<b>WHEN...</b>	<b>THEN...</b>
Passes	The Authorization Platform goes to the next edit.

### **DE 48, Subelement 61**

The Authorization Platform performs the following edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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.

---

#### **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.
<b>IF the...</b>	<b>THEN the Authorization Platform...</b>
Mastercard Assigned ID is valid	<p>Updates the value in DE 48, subelement 61, subfield 3 as follows:</p> <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	<p>Updates the value in DE 48, subelement 61, subfield 3 as follows:</p> <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 IIAS).</li> </ul>

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 048061</li> </ul>

### **DE 48, Subelement 66**

The Authorization Platform will perform the following system edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>An Authorization Request/0100 or Authorization Advice/0120 message contains DE 48 (Additional Data—Private Use), subelement 66 (Authentication Data) subfield 1 (Program Protocol) that is the incorrect length or incorrect data representation (alphanumeric)</p>	<p>Reject the message and forward to the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message with:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format Error)</li> <li>• DE 44 (Additional Response Data) = 048066</li> </ul>

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
An Authorization Request/0100 or Authorization Advice/0120 message contains DE 48, subelement 66 (Authentication Data) subfield 2 (Directory Server Transaction ID) that is not 36 bytes in length or filled with spaces	<p>Reject the message and forward to the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message with:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format Error)</li> <li>• DE 44 (Additional Response Data) = 048066</li> </ul>

### **DE 48, Subelement 77**

The Authorization Platform will perform the following system edits.

#### **Bill Pay**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The Authorization Request/0100 message or the Reversal Request/0400 message contains DE 48 (Additional Data—Private Use), subelement 77 (Funding/Payment Transaction Type Indicator) with value C91, C92, C93, or C94 and DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) is not value 00 (Purchase)	<p>Will reject the transaction with</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 12 (Invalid Transaction)</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 (U.S. Deferred Billing Indicator)	DE 2 (Primary Account Number [PAN]) must be a Visa PAN

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The Authorization Platform receives an Authorization Request/0100 and Reversal Request/0400 for a Visa-branded, Dual Message System (Authorization) transaction with DE 48 (Additional Data—Private Use), subelement 78 (Payment Service Indicators [Visa Only]) where:</p> <ul style="list-style-type: none"> <li>• Subfield 1 (Spend Qualified Indicator) contains a value other than Space</li> <li>• Subfield 2 (Dynamic Currency Conversion Indicator) contains a value other than Y or Space</li> <li>• Subfield 3 (U.S. Deferred Billing Indicator) contains a value other than D or Space</li> <li>• Subfield 4 (Visa Checkout Indicator) contains a value other than Y or Space</li> <li>• Subfield 5 (Message Reason Code) contains a value other than Space, 0, 1, 2, 3, 4, 5</li> <li>• Subfield 6 (Reserved for Future Use) contains a value other than Space</li> </ul>	<p>Sends an Authorization Request Response/0110 and Reversal Request/0400 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 048078 (indicating the data element in error)</li> </ul>

### **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)	<p>Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 12 (Invalid Transaction)</p>
52 (AVS Request) and DE 39 is 00 (Approved) or 08 (Honor with ID) or 85 (Not declined) and DE 48 SE 83 (AVS Response) is present with a value not equal to X, Y, A, W, Z, N, U, R, S.	<p>Sends the issuer an Authorization Response Negative Acknowledgement/0190 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30 (Format Error)</li> <li>• DE 44 = 048083</li> </ul>

### **DE 48, Subelement 84**

The Authorization Platform performs the following edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 48, subelement 42 and/or DE 48, subelement 43 are invalid due to token requirements that are not met	<p>Returns to the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 0480nn (where nn is the subelement number)</li> <li>• DE 48 (Additional Data—Private Use), subelement 84 = 04</li> </ul> <p><b>NOTE: Issuers do not receive decline advice messages for transactions that are rejected back to acquirers for format errors (DE 39 = 30).</b></p>

#### **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, Subelement 95**

The Authorization Platform performs the following system edit on Authorization Request/0100 and Reversal Request/0400 messages for Brazil installment payment transactions.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 48 (Additional Data—Private Use), subelement 95 (Mastercard Promotion Code) contains the value PARCEL, And DE 112 (Additional Data [National Use]), subelement 001 (Installment Payment Data) is not present	<p>Rejects the transaction sending the acquirer an Authorization Request Response/0110 or Reversal Request Response/0410 where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) contains value 30 (Format error)</li> <li>• DE 44 (Additional Response Data) contains value 112001 (indicating the data element in error)</li> </ul>

#### **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

---

Data Representation:	n-3
Length Field:	N/A
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).

---

### Attributes

Data Representation:	n-3
Length Field:	N/A
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

Data Representation:	n-3
Length Field:	N/A
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
Reversal Request Response/0410	CE	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

Data Representation:	b-8
Length Field:	N/A
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.

<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

---

Data Representation: n-16

---

Length Field: N/A

---

Data Field: Contents of subfields

---

Subfields: 6

---

Justification: See subfields

---

**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.

---

**Application Notes**

Use of DE 53 in online PIN transactions is specific to the PIN translation process performed on the dual message authorization network (Banknet) for Europe Region Acquirers and Issuers. It is not required to be provided in online PIN transactions for messages from non-Europe Region Acquirers.

---

## **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

---

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**

---

Data Representation: an...240; LLLVAR

---

The “LLL” length field of LLLVAR must be an integral multiple of 20, not to exceed 240.

---

Length Field: 3

---

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

#### General

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 (Amount Type) 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. The exception is that if an occurrence of DE 54, subfield 2 value 58 (POI Amount) is sent, then the Authorization Platform will not provide an additional occurrence 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. Issuers may include one additional occurrence of DE 54 subfields in the issuer's currency with an amount type value of 02 to indicate the available balance of the account. If the issuer approves the entire transaction amount, DE 54, subfield 2, with a value 57 will not be present in the authorization request response and the issuer may provide more than one occurrence of DE 54 subfields.

### **Account Balance Response**

---

The account balance response enables the issuers to include balance information as part of the response to a financial authorization request. Issuers can add account balance response information when responding to authorization requests for prepaid accounts and in ATM transactions. The account balance response is an "unsolicited" transmission of account balance data to the point-of-sale (POS) terminal or ATM. Account balance information returned in the Authorization Request Response/0110 must be provided in the same currency as the Cardholder Billing Currency (DE 51).

### **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). When reversing a Purchase with Cash Back Authorization where only the purchase amount of the transaction was approved by the issuer (Response Code 87 (Purchase Only Approval)), acquirers are not required to include the cash portion of the original authorization request in DE 54 of the Reversal Request/0400 message. Also, DE 4 (Amount, Transaction) of the reversal request should also contain only the actual Purchase Amount of the original authorization request.

### **Cash Back without Purchase in Participating Countries**

---

Cash Back without Purchase is supported for intracountry transactions in participating countries 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, values 10, 11, or 12 to indicate the healthcare, prescription, or vision Rx amounts. DE 54, subfield 2, values 10, 11, and 12 are sent only to the issuers that participate in Real-time Substantiation.

Effective with Release 19.Q1, Mastercard expanded DE 54 as follows to support value 12 (Vision Rx Eligibility Amount) for U.S. region acquirers and issuers:

- Overall size allowed by Mastercard = 240 bytes or 12 occurrences
- Number of occurrences an acquiring customer can send = 4
- Number of occurrences stored in USD currency = 4
- Number of occurrences converted to issuers currency = 4
- Number of occurrences sent to issuer = 8 (4 in acquirer currency, 4 in issuer currency)

### **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.](#)

---

### **POI Currency Conversion**

---

When POI currency conversion (also known as Dynamic Currency Conversion [DCC]) is performed, Mastercard suggests that acquirers provide the pre-conversion currency and amount in DE 54 with an amount type value of 58 (POI Amount) in subfield 2 for Authorization Request/ 0100, Authorization Advice/0120, and Reversal Request/0400 messages.

The processing criteria for DCC transactions are as follows:

- The transaction currency code in DE 49 (Currency Code, Transaction) must not be equal to the pre-conversion currency code in DE 54, subfield 3 (Currency Code).
- DE 54 must contain subfield 2 (Amount Type), value 58 (POI Amount), along with all other DE 54 subfields.
- The transaction amount provided in DE 54, subfield 4 (Amount) cannot contain all zeros.
- DE 54, subfield 3 must contain a valid, pre-conversion currency code.
- Issuers are not required to return an occurrence of DE 54 with subfield 2, value 58 in Authorization Request Response/0110 message. If it is returned by the issuer, it will be dropped before the response is forwarded to an acquirer.
- For a Purchase with Cash Back transaction to be subjected to DCC, it must contain two occurrences of DE 54 in Authorization Request/0100 or Authorization Advice/0120 messages: one occurrence with a subfield 2 value of 58 and another occurrence with a subfield 2 value of 40 (Amount Cash Back).
- Mastercard will allow acquirers to send one occurrence of DE 54 with a subfield 2 value of 58 in Reversal Request/0400 messages.
- Mastercard will forward an occurrence of DE 54 with subfield 2, value of 58 in Reversal Advice/0420 messages to the issuers if the acquirer has provided an occurrence of DE 54 with subfield 2, value 58 in Authorization Request/0100 or Reversal Request/0400 message, except when a Reversal Advice/0420 message is sent to the issuer when an Authorization Request Response/0110 message from the issuer is not delivered to the acquirer.

For partial Reversal Request/0400 messages subjected to DCC, acquirers may optionally supply the remainder of the transaction amount to be authorized in pre-conversion currency in DE 54, subfield 4 (Amount).

---

### **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

---

Required As: Conditional

---

### Example Values

---

01 = Ledger Balance

---

02 = Available Balance

---

03 = Amount Owing

---

04 = Amount Due

---

10 = Healthcare Eligibility Amount

---

11 = Prescription Eligibility Amount

---

12 = Vision Rx Eligibility Amount

---

13 = Reserved for future use

---

14 = Reserved for future use

---

17 = Mastercard Prepaid Online Bill Pay Transaction Fee Amount

---

40 = Amount Cash Back

---

44 = Amount Gratuity

---

57 = Original Amount

---

58 = POI Amount

---

59 = Limit/Balance available amount from Mastercard In Control

---

## 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**

---

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

---

### **DE 54—Authorization Platform Edits**

The Authorization Platform will perform the following system edits.

WHEN...	THEN the Authorization Platform...
<p>The acquirer sends an Authorization Request/0100 or an Authorization Advice/0120 message in which:</p> <ul style="list-style-type: none"><li>• An occurrence of DE 54 (Additional Amounts) contains a subfield 2 (Amount Type) value of 58 (Additional Amount, POI Amount), and</li><li>• An occurrence of DE 54 contains a subfield 3 (Currency Code) value that is equal to the DE 49 (Currency Code, Transaction) value.</li></ul>	<p>Will reject the transaction where:</p> <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format Error)</li><li>• DE 44 (Additional Response Data) = 054 (indicating the data element in error)</li></ul>
<p>OR</p> <ul style="list-style-type: none"><li>• An occurrence of DE 54 contains an invalid currency code in subfield 3.</li></ul>	

## 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, the issuer agent, or MDES 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 and can be present in DSRP transactions.

### Attributes

Data Representation:	b...255; LLLVAR The “LLL” length field of LLLVAR
Length Field:	3
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*.

Refer to DE 55—Authorization Platform Edits for a description of the edits performed on this data element.

For DSRP information, refer to Mastercard Cloud-Based Payments Product description.

---

## **DE 55—Subelement Encoding Scheme**

DE 55 contains chip data formatted in accordance with EMV specifications. Reference Book 3 of the EMV specification for details regarding coding of tag-length-value (TLV) data objects. The chip data in DE 55 consists of a series of subelements in a "tag-length-value" 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>22</sup></b>	<b>Each Component Length<sup>23</sup></b>	<b>Total Subelement Length<sup>24</sup></b>
<b>Required Subelements in Authorization Request/0100</b>				
				For Authorization requests related to Chip full-grade transactions and requests related to e-commerce transactions with EMV compliant ICC data, acquirers must provide DE 55 including the following subelements:
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)  (Mandatory if the corresponding data object [EMV tag 9F10] is provided by the card to the terminal)	9F10	ID	2	4–35
		length	1	
		data	1–32	
Unpredictable Number	9F37	ID	2	7
		length	1	
		data	4	
Application Transaction Counter	9F36	ID	2	5
		length	1	
		data	2	
Terminal Verification Result (TVR)	95	ID	1	7
		length	1	
		data	5	

<sup>22</sup> The hexadecimal representation is given here. Every two positions of hexadecimal data is one byte of binary data.

<sup>23</sup> Lengths are in binary format.

<sup>24</sup> The Total Subelement Length is the sum of the subelement's ID, length, and data subfields.

<b>Subelement Description</b>	<b>Tag Value</b>	<b>Component<sup>22</sup></b>	<b>Each Component Length<sup>23</sup></b>	<b>Total Subelement Length<sup>24</sup></b>
Transaction Date	9A	ID	1	5
		length	1	
		data	3	
Transaction Type	9C	ID	1	3
		length	1	
		data	1	
Amount Authorized	9F02	ID	2	9
		length	1	
		data	6	
Transaction Currency Code	5F2A	ID	2	5
		length	1	
		data	2	
Application Interchange Profile	82	ID	1	4
		length	1	
		data	2	
Terminal Country Code	9F1A	ID	2	5
		length	1	
		data	2	
Cardholder Verification Method (CVM) Results	9F34	ID	2	6
		length	1	
		data	3	

**NOTE: The presence of 9F34 is mandatory for all authorization messages containing DE 55.**

Terminal Capabilities	9F33	ID	2	6
(U.S. region only)		length	1	
		data	3	

<sup>22</sup> The hexadecimal representation is given here. Every two positions of hexadecimal data is one byte of binary data.

<sup>23</sup> Lengths are in binary format.

<sup>24</sup> The Total Subelement Length is the sum of the subelement's ID, length, and data subfields.

<b>Subelement Description</b>	<b>Tag Value</b>	<b>Component<sup>22</sup></b>	<b>Each Component Length<sup>23</sup></b>	<b>Total Subelement Length<sup>24</sup></b>
Dedicated File Name	84	ID	1	7–18
		length	1	
		data	5–16	
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/0100**

When DE 55 is present in the Authorization Request/0100 message, the following subelements are optional in DE 55:

Application Primary Account Number (PAN) Sequence Number	5F34	ID	2	4
		length	1	
		data	1	
Application Selection Registered Proprietary Data	9F0A	ID	2	3–Var
		length	1	
		data <sup>25</sup>	Var	
Terminal Type	9F35	ID	2	4
		length	1	
		data	1	
Interface Device (IFD) Serial Number	9F1E	ID	2	11
		length	1	
		data	8	

<sup>22</sup> The hexadecimal representation is given here. Every two positions of hexadecimal data is one byte of binary data.

<sup>23</sup> Lengths are in binary format.

<sup>24</sup> The Total Subelement Length is the sum of the subelement's ID, length, and data subfields.

<sup>25</sup> For technical information such as the formatting and allowed values of the Application Selection Registered Proprietary Data subelement, refer to the *M/Chip Requirements for Contact and Contactless* manual.

<b>Subelement Description</b>	<b>Tag Value</b>	<b>Component<sup>22</sup></b>	<b>Each Component Length<sup>23</sup></b>	<b>Total Subelement Length<sup>24</sup></b>
Transaction Category Code	9F53	ID	2	4
		length	1	
		data	1	
Application Version Number	9F09	ID	2	5
		length	1	
		data	2	
Transaction Sequence Counter	9F41	ID	2	5–7
		length	1	
		data	2–4	
Terminal Capabilities	9F33	ID	2	6
		(non-U.S. regions only)	length	1
			data	3
Third Party Data	9F6E	ID	2	8–35
		length	1	
		data	5–32	

#### **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	

<sup>22</sup> The hexadecimal representation is given here. Every two positions of hexadecimal data is one byte of binary data.

<sup>23</sup> Lengths are in binary format.

<sup>24</sup> The Total Subelement Length is the sum of the subelement's ID, length, and data subfields.

<b>Subelement Description</b>	<b>Tag Value</b>	<b>Component<sup>22</sup></b>	<b>Each Component Length<sup>23</sup></b>	<b>Total Subelement Length<sup>24</sup></b>
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.)	71	ID	1	3–129
		length	1	
Issuers may send more than one instance (maximum of 10 instances or maximum length of DE 55) of subelement 71 in the Authorization Request Response/0110.		data	1–127	

## 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>

<sup>22</sup> The hexadecimal representation is given here. Every two positions of hexadecimal data is one byte of binary data.

<sup>23</sup> Lengths are in binary format.

<sup>24</sup> The Total Subelement Length is the sum of the subelement's ID, length, and data subfields.

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:

- DE 39 = 30
- DE 44 = 055

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:

- DE 39 = 30
- DE 44 = 055

<b>WHEN...</b>	<b>THEN...</b>
DE 55 is present in the Authorization Request/ 0100 message or the Authorization Advice/0120 message	<p>DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 must be 03, 05, 07, or 81 or the Authorization Platform rejects the Authorization Request/0100 message or Authorization Advice/ 0120 message where:</p> <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	<p>The Authorization Platform sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 055</li> </ul>
DE 55 is greater than 255 characters in length in the Authorization Request/0100 message	<p>The Authorization Platform sends the acquirer an Authorization Request Response/0110 where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 055</li> </ul>

The Authorization Platform will perform the following edits on an Authorization Request Response/  
0110 message.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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 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>

### **Authorization Platform Edits—Cardholder Authentication Service**

The Authorization Platform will perform the following system edits related to the Cardholder Authentication Service.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>An Account Status Inquiry Transaction for account ranges participating in the Cardholder Authentication Service - the Authorization Request/0100 message contains:</p> <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) setup for Type 1 Authentication Service, and</li> <li>• DE 4 (Amount, Transaction) has a value of zero, and</li> <li>• DE 23 (Card Sequence Number) contains a value of 01X, and</li> <li>• DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI]), and</li> <li>• DE 55 (Integrated Circuit Card [ICC] System-Related Data) is present and tag 9F10: <ul style="list-style-type: none"> <li>– CVR byte1, bit1 is present with a value other than 1 (successful), or</li> <li>– CVR byte2, bit2 is present with a value other than 1 (biometric).</li> </ul> </li> </ul>	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 05 (Do not honor), and</li> </ul> <p>Sends the issuer an Authorization Advice/0120 message with DE 60 (Advice Reason Code):</p> <ul style="list-style-type: none"> <li>• Subfield 1 (Advice Reason Code) value 160 (Authentication Advice to Issuer), and</li> <li>• Subfield 2 (Advice Detail Code) value 0078 (M/ Chip Biometric Data not present)</li> </ul>
<p>An Account Status Inquiry Transaction for account ranges participating in the Cardholder Authentication Service - the Authorization Advice/0120—Acquirer-generated message contains:</p> <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) setup for Type 1 Authentication Service, and</li> <li>• DE 4 (Amount, Transaction) has a value of zero, and</li> <li>• DE 23 (Card Sequence Number) contains a value of 01X (X can be any number from 0 to 9 inclusive), and</li> <li>• DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI]), and</li> <li>• DE 55 (Integrated Circuit Card [ICC] System-Related Data) is present and tag 9F10: <ul style="list-style-type: none"> <li>– CVR byte1, bit1 is present with a value other than 1 (successful), or</li> <li>– CVR byte2, bit2 is present with a value other than 1 (biometric).</li> </ul> </li> </ul>	<p>Sends the acquirer an Authorization Advice Response/0130 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format Error), and</li> <li>• DE 44 (Additional Response Data) = 055 (indicating the data element in error)</li> </ul>

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>An Account Status Inquiry Transaction for account ranges participating in the Cardholder Authentication Service - the Authorization Request/0100 message contains:</p> <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) setup for Type 2 Authentication Service, and</li> <li>• DE 4 (Amount, Transaction) has a value of zero, and</li> <li>• DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI]), and</li> <li>• DE 55 (Integrated Circuit Card [ICC] System-Related Data) is present and tag 9F10: <ul style="list-style-type: none"> <li>– CVR byte1, bit1 is present with a value other than 1 (successful), or</li> <li>– CVR byte2, bit2 is present with a value other than 1 (biometric).</li> </ul> </li> </ul>	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 05 (Do not honor), and</li> </ul> <p>Sends the issuer an Authorization Advice/0120 message with DE 60 (Advice Reason Code):</p> <ul style="list-style-type: none"> <li>• Subfield 1 (Advice Reason Code) value 160 (Authentication Advice to Issuer), and</li> <li>• Subfield 2 (Advice Detail Code) value 0078 (M/ Chip Biometric Data not present)</li> </ul>
<p>An Account Status Inquiry Transaction for account ranges participating in the Cardholder Authentication Service - the Authorization Advice/0120—Acquirer-generated message contains:</p> <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) setup for Type 2 Authentication Service, and</li> <li>• DE 4 (Amount, Transaction) has a value of zero, and</li> <li>• DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI]), and</li> <li>• DE 55 (Integrated Circuit Card [ICC] System-Related Data) is present and tag 9F10: <ul style="list-style-type: none"> <li>– CVR byte1, bit1 is present with a value other than 1 (successful), or</li> <li>– CVR byte2, bit2 is present with a value other than 1 (biometric).</li> </ul> </li> </ul>	<p>Sends the acquirer an Authorization Advice Response/0130 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format Error), and</li> <li>• DE 44 (Additional Response Data) = 055 (indicating the data element in error)</li> </ul>

---

## DE 56—Payment Account Data

DE 56 (Payment Account Data) contains unique, non-financial reference information associated with the PAN or token used to initiate the transaction.

Attribute	Value			
Data Representation:	an...37; LLLVAR			
Length Field:	3			
Data Field:	Contents of subelements			
Subelements:	1			
Justification:	See subelement			
<b>Usage</b>				
Following is the usage of DE 56 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:			Org	Sys
			Dst	
Authorization Request/0100	•	X	C	
Authorization Request/0100—Account Status inquiry (merchant initiated message and MDSE pre-digitization message)	•	X	C	
Authorization Request/0100—Tokenization Complete Notification*	•	X	C	
Authorization Request Response/0110	C	X	C	
Authorization Request Response/0110—Tokenization Authorization Request Response*	C	X	C	
Authorization Request Response/0110—Account Status Inquiry*	C	X	C	
Authorization Advice/0120—Acquirer-generated	•	X	C	
Authorization Advice/0120—System-generated	•	X	C	
Authorization Advice Response/0130—Issuer-generated	C	X	C	
Reversal Request/0400	•	X	C	
Reversal Request Response/0410	C	X	C	
Reversal Advice/0420	•	X	C	
Reversal Advice Response/0430	O	•	•	
Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Complete Notification*	•	X	C	

\* MDSE pre-digitization message

## **Subelement 01—Payment Account Data**

DE 56, subelement 01 (Payment Account Data) contains the applicable subfields to carry the unique Payment Account Data specifically associated with the PAN or token used to initiate the transaction.

<b>Attribute</b>	<b>Value</b>
Subelement ID	n-2
Subelement Length	01
Data Representation	an...33; LLVAR
Data Field	Contents of positions 1–2
Number of Subfields	1
	Payment Account Reference

### **Subfield 01—Payment Account Reference (PAR)**

DE 56, subelement 01, subfield 01 (Payment Account Reference [PAR]) contains the assigned PAR value. A PAR is a unique value associated with a single PAN and attributed to all tokens associated with that PAN. A PAR can be used to link transactions containing PANs or tokens associated with the same underlying payment account.

<b>Attribute</b>	<b>Value</b>
Subfield ID	n-2
Subfield Length	01
Data Representation	an...29; LLVAR
Justification	...29
<b>Position</b>	<b>Description</b>
1–4	BIN Controller Identifier—A four-character value assigned by EMVCo
5–29	A unique 25-character alphanumeric uppercase value generated by the BIN Controller and linked to a PAN

## **DE 57–DE 59—Reserved for National Use**

DE 57–DE 59 are reserved for future use.

Attributes
Data Representation:

---

Length Field:	3
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

---

Data Representation:	ISO: ans...999; LLLVAR
	Mastercard: ans...060; LLLVAR

---

Length Field:	3
Data Field:	Contents of subfields
Subfields:	3
Justification:	See subfields

---

<b>Usage</b>
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
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

---

**Values**

---

See subfields

---

**Application Notes**

---

Not all Advice Reason Codes may be used within all programs and services.

---

**Subfield 1—Advice Reason Code**

DE 60, subfield 1 contains the advice reason code.

---

Attributes

---

Data Representation: n-3

---

Data Field: Contents of positions 1–3

---

Justification: N/A

---

**Values**

---

This subfield is mandatory for all advice messages and indicates the general purpose of the advice message.

---

The following tables displays the general values for subfields 1 and 2 based on message type for all products, though each code does not pertain to all products. To determine whether the processor or the Single Message System includes DE 60, refer to the Message Flow chapter for descriptions and diagrams for advice messages.

The Single Message System will perform system edits for DE 60 (Advice Reason Code) on transaction messages that do not contain the appropriate codes in DE 60, subfield 1 (Advice Reason Code) and subfield 2 (Advice Reason Detail Code) for the following message types:

---

Message Type Brand Impacted

---

Financial Transaction Advice/0220 Cirrus, Maestro

---

Acquirer Reversal Advice/0420 Cirrus, Maestro

---

Issuer Reversal Advice/0422 Cirrus, Maestro, Debit Mastercard

---

**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>26</sup>	✓	✓	✓		✓	✓

---

<sup>26</sup> This secondary route is to either the Stand-In System or the optional alternate route.

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
101	Alternate Issuer Route: IPS signed out <sup>26</sup>	✓	✓	✓		✓	✓
102	Alternate Issuer Route: IPS timed out <sup>26</sup>	✓	✓	✓		✓	✓
103	Alternate Issuer Route: IPS unavailable <sup>26</sup>	✓	✓	✓		✓	✓
105	Transaction processed via X-Code	✓	✓	✓			
107	PIN processing error	✓				✓	✓
108	Alternate Issuer Route: MIP Error <sup>26</sup>	✓	✓	✓		✓	✓
109	Alternate Issuer Route: Issuer Edit Response Error <sup>26</sup>	✓	✓	✓		✓	✓
111	Alternate Issuer Route: Issuer Host System Error <sup>26</sup>	✓	✓	✓		✓	✓
112	Alternate Route: Network Not Dispatched Error <sup>26</sup>	✓	✓	✓		✓	✓
113	Alternate Route: Issuer Undelivered <sup>26</sup>	✓	✓	✓		✓	✓
114	Alternate Route: Direct Down Option <sup>26</sup>	✓	✓	✓		✓	✓
115	Transaction Processed via On-behalf Service Decision	✓				✓	✓
116	Invalid Merchant	✓					
120	Transaction Blocking	✓				✓	✓
121	Account Lookup Service	✓	✓			✓	
126	Pay with Rewards Processing Advice to Issuer	✓					
140	Unable to convert contactless or virtual account number	✓				✓	
141	Mastercard Digital Enablement Service Advice to Issuer	✓				✓	
151	In Control Processing Advice to Issuer (Mastercard Merchant Presented QR)	✓					
160	Authentication Advice to Issuer	✓				✓	
180	CAT Risk Level 3	✓	✓				
190	Acquirer Processing System (APS) Approved	✓	✓	✓		✓	✓
191	Acquirer Processing System (APS) Completed Authorization Transaction	✓	✓		✓	✓	
192	M/Chip Offline Advice to Issuer	✓				✓	
200	In Control 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 system edits on Authorization Advice/0120—Acquirer-generated messages.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 60 in the Authorization Advice/0120— Acquirer-generated messages is not the value 190 (Acquirer Processing System (APS) Approved) or 191 (Acquirer Processing System (APS) Completed Authorization Transaction) or 192 (M/Chip Offline Advice to Issuer)	Sends the acquirer an 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) = 060 (Invalid DE 60 value)</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 Sign-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
0009	Reject: Invalid Time Validation
0041	Reject: Payment Cancellation
0078	Reject: M/Chip Biometric Data not Present

#### **DE 60, Subfield 2 Values, in Authorization Advice/0120—Issuer-Generated**

The following values are valid in Authorization Advice/0120—Issuer-generated messages.

<b>Code</b>	<b>Description</b>
0030	Accept: Member-generated Authorization Advice/0120 sent to the risk 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.

<b>Values</b>	
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	Reject: Invalid Time Validation
0010	Reject: Stand-In Monitoring Rule
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

Values	
0028	Reject: invalid CVC 1
0029	Reject: expired card
0031	Reject: unable to decrypt/encrypt PIN data. (Used with Advice Reason Code 107)
0036	Reject: CVC 1 Unable to process
0047	Reject: CVC 1 No matching key file for this PAN, PAN expiry date combination; status unknown

#### DE 60, Subfield 2 Values, in Administrative Advice/0620

Following are the valid values in Administrative Advice/0620 messages.

Code	Description
0029	MIP-generated risk Advice transactions
0030	Member-generated risk Advice transactions
0250	Activation Code Notification
0251	Tokenization Complete Notification
0252	Tokenization Event Notification

#### 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

<b>Code</b>	<b>Description</b>
0094	Business account maintenance request
0095	Business counteroffer reply
0096	Business pre-approved offer inquiry

### **DE 60, Subfield 2 Values, in Dynamic CVC 3 Validation**

Following are valid values in Dynamic CVC 3 Validation transactions.

<b>Code</b>	<b>Description</b>
0037	Reject: No matching key file for this PAN, PAN expiry date, and KDI combination
0038	Reject: Security Platform Time Out
0040	Reject: Security Platform System Error
0042	Reject: CVC 3 Unable to process
0043	Reject: ATC outside allowed range
0044	Reject: CVC 3 Invalid
0045	Reject: CVC 3 Unpredictable number mismatch
0046	Reject: ATC Replay

### **DE 60, Subfield 2 Values, in Mastercard In Control Service**

The following values are valid in Mastercard In Control™ Service transactions.

<b>Code</b>	<b>Description</b>
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: In Control
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

---

<b>Code</b>	<b>Description</b>
0071	Reject: Decline Other
0072	Reject: Geographic Restriction
0073	Reject: Transaction Type Restriction
0075	Reject: Transaction Time/Date Restriction
0076	Reject: Sanction Screening Score Restriction
0077	Reject: MoneySend Transaction Count Check

---

### **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 Data Processing Error
0033	Reject: PIN or CHIP Validation Failed
0034	Reject: Chip validation failed
0035	Reject: TVR/CVR validation failed
0037	Reject: No matching key File for this PAN, PAN expiry date and KDI combination—Validation of ARQC and CVR/TR not performed, status unknown
0038	Reject: Security platform time out
0039	Reject: Cryptogram not ARQC
0040	Reject: Security platform processing error
0043	Reject: ATC outside allowed range
0046	Reject: ATC Replay
0054	Reject: Track Data Format Error
0055	Reject: Chip CVC Invalid
0056	Reject: Chip CVC/CVC 1 Unable to process

---

### **DE 60, Subfield 2 Values, in Mastercard Digital Enablement Service**

Following are valid values in Mastercard Digital Enablement Service.

---

<b>Code</b>	<b>Description</b>
0201	Reject: Invalid Token—Primary Account Number mapping relationship
0202	Reject: Token in suspended status

---

<b>Code</b>	<b>Description</b>
0203	Reject: Token deactivated
0204	Reject: ATC Invalid—Not in List of Currently Active Single Use Keys
0205	Reject: ATC Replay
0206	Reject: Invalid MD AC and UMD AC (Invalid Mobile PIN)
0207	Reject: Valid MD AC; Invalid UMD AC (Mobile PIN Try Counter Max Limit not Reached, Token not Suspended)
0208	Reject: Invalid MD AC; Valid UMD AC
0209	Reject: Valid MD AC; Invalid UMD AC (Mobile PIN Try Counter Max Limit Reached, Token Suspended)
0210	Reject: Unpredictable Number Length Indicator Mismatch
0211	Reject: TVR/CVR validation failed
0212	Reject: Unable to Process
0213	Reject: Invalid Token
0215	Reject: Declined by Transaction Analysis
0032	Reject: Chip Data Processing Error
0034	Reject: Chip validation failed
0035	Reject: TVR/CVR validation failed
0039	Reject: Cryptogram not ARQC
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 Merchant Presented QR Service**

Following are valid values in Mastercard Merchant Presented QR Service transactions.

<b>Code</b>	<b>Description</b>
0064	Reject: Transaction Limit Check
0065	Reject: Cumulative Limit Check
0072	Reject: Geographic Restriction

### **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

### **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

---

<b>Code</b>	<b>Description</b>
0301	Reject: transaction limit test  Mastercard default limits caused transaction to fail; card not present at point of interaction
0310	Reject: transaction limit test  Customer-defined limits caused transaction to fail; card present at point of interaction
0311	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
0411	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
0111	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
0511	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
0611	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
0711	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
0811	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
0911	Reject: transaction limit test  Customer-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 (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  Customer-defined limits caused transaction to fail; card present at point of interaction
1011	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
1111	Reject: transaction limit test  Customer-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.

Code	Description
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  Customer-defined limits caused transaction to fail; card present at point of interaction
1211	Reject: transaction limit test  Customer-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.

Code	Description
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  Customer-defined limits caused transaction to fail; card present at point of interaction
1311	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
1411	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
1511	Reject: transaction limit test  Customer-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  Customer-defined limits caused transaction to fail; card present at point of interaction
1611	Reject: transaction limit test  Customer-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
1903	Reject: via MIP Transaction Blocking
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:

---

Data Field:	Contents of positions 8–60
Justification:	Left
<b>Values</b>	
Advice message text	

---

## DE 61—Point-of-Service (POS) Data

DE 61 (Point-of-Service [POS] Data) indicates the conditions that exist at the point of service at the time of the transaction. Note that DE 61 supersedes and replaces the ISO-specified DE 25 (Point-of-Service [POS] Condition Code) which is not used in the *Customer Interface Specification*.

---

Attributes																											
Data Representation:		ISO: ans...999; LLLVAR																									
Mastercard: ans...026; LLLVAR																											
<hr/>																											
Length Field:	3																										
Data Field:	Contents of subfields																										
Subfields:	14																										
Justification:	See subfields																										
<hr/>																											
<b>Usage</b>																											
Following is the usage of DE 61 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:																											
<table><thead><tr><th></th><th>Org</th><th>Sys</th><th>Dst</th></tr></thead><tbody><tr><td>Authorization Request/0100</td><td>M</td><td>•</td><td>M</td></tr><tr><td>Authorization Advice/0120—Acquirer-generated</td><td>M</td><td>•</td><td>M</td></tr><tr><td>Authorization Advice/0120—Issuer-generated</td><td>M</td><td>M</td><td>•</td></tr><tr><td>Authorization Advice/0120—System-generated</td><td>•</td><td>M</td><td>M</td></tr><tr><td>Reversal Request/0400</td><td>M</td><td>•</td><td>M</td></tr></tbody></table>					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
	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																								
<hr/>																											
<b>Values</b>																											
<hr/>																											

---

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); server

### **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

---

#### **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); server
4	=	On premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA)
8	=	Additional POS Terminal Locations

### 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	=	Cardholder not present (mail/facsimile order)
3	=	Cardholder not present (phone or Automated Response Unit [ARU])
4	=	Standing order/recurring transactions
5	=	Cardholder not present (Electronic order [home PC, Internet, mobile phone, PDA])

#### Application Notes

---

Refer to the Canada Region Debit Mastercard Merchant Acceptance section in the Program and Service Format Requirements chapter of this manual for details on the use of subfield 4 for Canada-acquired transactions.

---

### **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 does not have 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 Field: Contents of position 7

---

---

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

**Values**

0	=	Normal request (original presentment)
2	=	SecureCode Phone Order
3	=	ATM Installment Inquiry
4	=	Prauthorized request
5	=	Time Based Payment Authorization Request—Brazil domestic transactions
6	=	ATC Update
8	=	Account Status Inquiry Service (ASI)
9	=	Tokenization Request/Notification

**Application Notes**

For DE 61, subfield 7, value 8, see separate description of Account Status Inquiry Service (both Purchase ASI and Payment ASI) and Product Inquiry Service.

---

## **Subfield 8—POS Transaction Security**

DE 61, subfield 8 (POS Transaction Security) indicates the card acceptor's confidence in the transaction security level.

Attributes

Data Representation:	n-1
Data Field:	Contents of position 8
Justification:	N/A

**Values**

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.

Attributes

Data Representation:	n-1
Data Field:	Contents of position 9

---

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

**Values**

Zero-filled.
--------------

### Subfield 10—Cardholder-Activated Terminal Level

DE 61, subfield 10 (Cardholder-Activated Terminal Level) indicates the type of cardholder activated terminal used by the cardholder to initiate the transaction.

---

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
---	---	-------------------------

---

9	=	MPOS Acceptance Device
---	---	------------------------

**NOTE: Mobile POS are always attended devices and not cardholder activated.**

---

**Application Notes**

When the recipient of the money transfer (Payment Transaction; DE 3 subfield 1=09) is not present, the transaction is not considered a CAT level transaction. In that case the CAT level = 0.

---

### Subfield 11—POS Card Data Terminal Input Capability Indicator

DE 61, subfield 11 indicates the set of methods supported by the terminal for the input of account number, card, or mobile device data.

---

### Attributes

---

Data Representation:	n-1
Data Field:	Contents of position 11
Justification:	N/A

---

### Values

---

0	=	Input capability unknown or unspecified.
1	=	No terminal used (voice/ARU authorization); server.
2	=	Terminal supports magnetic stripe input only.
3	=	Contactless EMV/Chip (Proximity Chip)  Terminal supports contactless EMV input and contactless magstripe input. The terminal also may support one or more other card input types, including EMV contact chip input, magnetic stripe input and key entry input.
4	=	Contactless Mag Stripe (Proximity Chip)  Terminal supports contactless magstripe input but not contactless EMV input. The terminal also may support one or more other card input types, including EMV contact chip input, magnetic stripe input, and key entry input.
5	=	Terminal supports EMV contact chip input and magnetic stripe input.
6	=	Terminal supports key entry input only.
7	=	Terminal supports magnetic stripe input and key entry input.
8	=	Terminal supports EMV contact chip input, magnetic stripe input and key entry input.
9	=	Terminal supports EMV contact chip input only.

---

### Application Notes

---

DE 61, subfield 11 values 3, 4 (contactless related), 5, 8, and 9 (chip contact) related can ONLY be used if the terminal is chip certified by Mastercard .

DE 61, subfield 11 is used in conjunction with DE 22 (Point of Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode). DE 22, subfield 1 values indicate the method by which the PAN was entered.

DE 61, subfield 11 indicates the terminal data input capabilities and not the specific manner in which the terminal captured the card data for a given transaction.

For example, values 5 and 8 could be used for a magnetic stripe transaction originating from an EMV contact chip capable terminal when the contact magnetic stripe reader was used instead. Similarly, value 3 would be used for a contact chip transaction originating from a contactless EMV capable terminal when the EMV contact chip reader was used.

### Subfield 12—POS Authorization Life Cycle

DE 61, subfield 12 (POS Authorization Life Cycle) indicates the number of days a preauthorization will stay in effect for Visa Custom Payment Service automobile rentals and hotel reservations—otherwise it must contain zeros.

---

#### Attributes

---

Data Representation: n-2

---

Data Field: Contents of positions 12 and 13

---

Justification: N/A

---

#### Values

---

Indicates the number of days the preauthorization stays in effect; ATM and Maestro POS transactions should use 01, Visa CPS transactions use applicable value. Must be zero filled when not applicable.

---

### Subfield 13—POS Country Code (or Sub-Merchant Information, if applicable)

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

---

Refer to the *Quick Reference Booklet* for valid country codes.

---

#### Application Notes

---

Refer to the Canada Region Debit Mastercard Merchant Acceptance section in the Program and Service Format Requirements chapter of this manual for details on the use of subfield 13 for Canada-acquired transactions.

---

### Subfield 14—POS Postal Code (or Sub-Merchant Information, if applicable)

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.

---

### Application Notes

---

Subfield 14 must be present if postal codes are available in the acquiring country. However, subfield 14 may be omitted rather than a space or blank filled if the postal code does not exist in the acquiring country. If the data is missing or blank filled for an acquiring country identified as using postal codes, the Authorization Platform will not reject the message; however a data integrity error may be reported.

Postal code data, when present, must be valid and accurate. 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

WHEN the Acquirer...	THEN the Authorization Platform...
Sends an Authorization Request/0100 message containing less than nine characters	Sends an Authorization Request Response/0110 message to the acquirer where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 061</li></ul>
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: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 061</li></ul>

## Non-ATM CAT Level 1 Transactions

WHEN the Authorization Request/0100 message contains...	THEN the Authorization Platform...
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.
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	Sends an Authorization Request Response/0110 message to the acquirer where: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 052</li> </ul>
<b>MoneySend transactions with a CAT 1 are excluded from this edit.</b>	

## Electronic Commerce Transactions

IF...	THEN...	Otherwise, the Authorization Platform...
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 ( <i>SecureCode</i> Phone Order) and Subfield 10 must contain value 6 (Electronic commerce)	Rejects the authorization transaction with a format error indicated by: <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 061</li> </ul>

### Phone Order Transactions

IF...	THEN...	Otherwise, the Authorization Platform...
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 ( <i>SecureCode Phone Order</i> ) and Subfield 10 must not contain value 6	Rejects the authorization transaction with a format error indicated by: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 061</li></ul>

### 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 [ASI]) 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 [ASI]) 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>

## Contactless Chip Transaction Edits

<b>WHEN the Authorization Request/0100, Authorization Advice/0120, Reversal Request/0400, message contains...</b>	<b>THEN the Authorization Platform...</b>
The PAN entry mode (DE 22 [Point-of-Service Entry Mode], subfield 1 [POS Terminal PAN Entry Mode]) of 07 (PAN auto-entry via contactless M/Chip) and DE 61 (Point-of-Service [POS] Data), subfield 11 (POS Card Data Terminal Input Capability Indicator) is not 3 (Contactless M/Chip [Proximity Chip])	<p>Sends 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</li> <li>• DE 44 = 061</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

Data Representation:	ISO:	ans...999; LLLVAR
	Mastercard:	ans...100; LLLVAR
Length Field:	3	
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
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 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.

## 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

Data Representation:	ISO:	ans...999; LLLVAR
----------------------	------	-------------------

Mastercard:	an...050; LLLVAR		
Length Field:	3		
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.

#### Attributes

Data Representation: an-3

Data Field: Contents of positions 1–3

Justification: Left

#### Values

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
ACS	Digital Debit		✓				
AMX	American Express <sup>28</sup>				✓		
BPD	Business Premium Debit		✓				
CBL	Carte Blanche <sup>28</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>28</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	✓					
DSV	Discover <sup>28</sup>				✓		
DWF	Debit Mastercard Humanitarian Prepaid		✓				
EXC	ADP/Exchange <sup>28</sup>			✓			
HNR	Honor <sup>28</sup>			✓			
ITT	Instant Teller <sup>28</sup>			✓			
JCB	Japanese Credit Bureau <sup>28</sup>		✓				
LNC	LINC New York <sup>28</sup>		✓				

<sup>27</sup> This product code is effective in all regions other than the Canada region as of 13 April 2018, and is effective in the Canada region as of 13 July 2018.

<sup>28</sup> This product code is not a valid value in DE 120, MCC103 or MCC104, field 3, Card Program.

<sup>29</sup> This product code is not currently available for issuance in the Canada region.

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
MAB	World Elite™ Mastercard® Business	✓					
MAC	Mastercard® Corporate World Elite®	✓					
MAP	Mastercard Commercial Payments Account	✓					
MAQ	Mastercard® Prepaid Commercial Payments Account	✓					
MBB	Mastercard Prepaid Consumer	✓					
MBC	Mastercard Prepaid Voucher	✓					
MBD	Mastercard Professional Debit Business Card	✓					
MBE	Mastercard® Electronic Business Card	✓					
MBF	Mastercard® Alimentação (Food) (MBF—Prepaid Mastercard Food)	✓					
MBK	Mastercard Black	✓					
MBM	Mastercard® Refeição (Meal) (MBM—Prepaid Mastercard Meal)	✓					
MBP	Mastercard Corporate Prepaid	✓					
MBS	Mastercard® B2B Product	✓					
MBT	Mastercard Corporate Prepaid Travel	✓					
MBW	World Mastercard® Black Edition—Debit	✓					
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>28</sup>	✓					
MCO	Mastercard Corporate	✓					
MCP	Mastercard Corporate Purchasing Card®	✓					
MCS	Mastercard® Standard 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>
MCT	Titanium Mastercard	✓					
MCU	Mastercard Unembossed	✓					
MCV	Merchant-Branded Program	✓					
MCW	World Mastercard™ Card	✓					
MDB	Debit Mastercard BusinessCard Card	✓					
MDG	Debit Gold Mastercard®	✓					
MDH	World Debit Embossed	✓					
MDI	Debit Other Unembossed	✓					
MDJ	Debit Mastercard® (Enhanced)	✓					
MDK	Debit Mastercard 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	✓					
MDW	World Elite™ Debit Mastercard® (Mastercard Black™ Debit LAC region excluding Mexico)	✓					
MEB	Mastercard Executive BusinessCard Card	✓					
MEC	Mastercard® Electronic Commercial	✓					
MED	Debit Mastercard Electronic	✓					
MEF	Mastercard Electronic Payment Account	✓					
MEO	Mastercard Corporate Executive Card® <sup>28</sup>	✓					
MEP	Premium Debit Mastercard	✓					
MES	Mastercard Enterprise Solution	✓					

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
MET	Titanium 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	✓					
MGP	Mastercard® Prepaid Gold Payroll	✓					
MGS	Platinum Mastercard® Prepaid General Spend	✓					
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	✓					

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
MLA	Mastercard Central Travel Solutions Air	✓					
MLC	Mastercard Micro-Business Card	✓					
MLD	Mastercard Distribution Card	✓					
MLE	Mastercard® Pedágio Prepaid Card (MLE—Mastercard Brazil General Benefits)	✓					
MLF	Mastercard Agro	✓					
MLL	Mastercard Central Travel Solutions Land	✓					
MNF	Mastercard® Public Sector Commercial Card	✓					
MNW	World Mastercard Card (Europe)	✓					
MOC	Standard Maestro® Social					✓	
MOG	Maestro® Gold <sup>28</sup>					✓	
MOP	Maestro® Platinum <sup>28</sup>					✓	
MOW	World Maestro					✓	
MPA	Prepaid Mastercard Payroll Card	✓					
MPB	Mastercard Preferred BusinessCard	✓					
MPC	Mastercard Professional Card	✓					
MPD	Mastercard Flex Prepaid	✓					
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	✓					

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
MPX	Prepaid Mastercard Flex Benefit Card	✓					
MPY	Prepaid Mastercard Employee Incentive Card	✓					
MPZ	Prepaid Mastercard Emergency Assistance Card	✓					
MRB	Prepaid Mastercard Electronic BusinessCard	✓					
MRC	Prepaid Mastercard Electronic Card	✓					
MRD	Platinum Debit Mastercard® Prepaid General Spend	✓					
MRF	European Regulated Individual Pay	✓					
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)					✓	

<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					✓	
MTP	Mastercard Platinum Prepaid Travel Card			✓			
MUP	Platinum Debit Mastercard Unembossed			✓			
MUS	Prepaid Mastercard Unembossed US			✓			
MUW	Mastercard World Domestic Affluent			✓			
MVA	Mastercard® B2B VIP 1			✓			
MVB	Mastercard® B2B VIP 2			✓			
MVC	Mastercard® B2B VIP 3			✓			
MVD	Mastercard® B2B VIP 4			✓			
MVE	Mastercard® B2B VIP 5			✓			
MVF	Mastercard® B2B VIP 6			✓			
MVG	Mastercard® B2B VIP 7			✓			
MVH	Mastercard® B2B VIP 8			✓			
MVI	Mastercard® B2B VIP 9			✓			
MVJ	Mastercard® B2B VIP 10			✓			
MVK	Mastercard® B2B VIP 11			✓			
MWB	World Mastercard® for Business			✓			
MWD	World Deferred			✓			
MWE	Mastercard World Elite			✓			
MWF	Mastercard Humanitarian Prepaid			✓			
MWO	Mastercard Corporate World			✓			

<sup>30</sup> This product code is not currently available for issuance in the Canada region.

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
MWP	Mastercard® World Prepaid	✓					
MWR	World Retailer Centric Payment	✓					
NYC	NYCE Network <sup>28</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>28</sup>		✓				
PRO	Proprietary Card <sup>28</sup>		✓				
PUL	Pulse <sup>28</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>28</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		✓				

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
STR	Star Network <sup>28</sup>		✓				
SUR	Prepaid Mastercard Unembossed Outside US		✓				
TBE	Business—Immediate Debit		✓				
TCB	Mastercard Business Card—Immediate Debit		✓				
TCC	Mastercard (Mixed BIN)—Immediate Debit		✓				
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		✓				

---

<b>Code</b>	<b>Description</b>	<b>MC</b>	<b>NP</b>	<b>VI</b>	<b>TE</b>	<b>MS</b>	<b>CI</b>
TPC	Mastercard Professional Card—Immediate Debit	✓					
TPL	Platinum Mastercard—Immediate Debit	✓					
TWB	World Mastercard® Black Edition—Immediate Debit	✓					
VIS	VisaNet <sup>28</sup>			✓			
WBE	World Mastercard® Black Edition	✓					
WDR	World Debit Mastercard Rewards	✓					
WMR	World Mastercard Rewards	✓					
WPD	World Prepaid Debit	✓			✓	✓	

---

## **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.

---

<b>Attributes</b>	
Data Representation:	an...9
Data Field:	Contents of positions 4–12
Justification:	Left
<b>Values</b>	
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.

---

<b>Attributes</b>	
Data Representation:	b-8
Length Field:	N/A
Data Field:	N/A

---

---

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

---

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

---

### Usage

---

May contain message authentication code as defined by ISO standards.

---

### 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

---

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

---

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

---

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

---

Data Representation:	n-1
----------------------	-----

---

Length Field:	N/A
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

---

Data Representation:	n-2
Length Field:	N/A
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

---

Data Representation:	n-3
Length Field:	N/A
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.

---

**Attributes**

---

Data Representation: n-3

---

Length Field: N/A

---

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**

---

Data Representation: n-3

---

Length Field: N/A

---

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—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
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—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.

Code	Financial Network	MC	NP	VI	TE	MS	CI
001 =	Sign-on (by prefix)	✓	✓	✓	✓	✓	✓
002 =	Sign-off (by prefix)	✓	✓	✓	✓	✓	✓

<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>
061 =	Group sign-on (by Mastercard group sign-on)	✓	✓	✓	✓	✓	✓
062 =	Group sign-off (by Mastercard group sign-on)	✓	✓	✓	✓	✓	✓
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>	✓	✓			✓	✓

### **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	✓	✓	✓	✓	✓	✓

---

<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>
082 =	Host session deactivation	✓	✓	✓	✓	✓	✓

### **Network Management Request/0800—PEK Exchange**

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>
161 =	Encryption key exchange	✓	✓			✓	✓

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

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>
162 =	Solicitation for Encryption Key Exchange	✓	✓			✓	✓
163 =	Solicitation for Encryption Key Exchange - TR-31 Keyblock	✓	✓	✓	✓	✓	✓

### **Network Management Request Response/0810—PEK Exchange**

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>
163 =	Solicitation for Encryption Key Exchange - TR-31 Keyblock	✓	✓	✓	✓	✓	✓

### **Network Management Advice/0820—PEK Exchange**

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>
164 =	Encryption TR-31 Block Key Exchange Confirmation of Success	✓	✓	✓	✓	✓	✓
165 =	Encryption TR-31 Block Key Exchange Advice of Failure	✓	✓	✓	✓	✓	✓

## 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

---

Data Representation:	n-4
Length Field:	N/A
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

---

Data Representation:	n-4
Length Field:	N/A
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

---

Data Representation: n-6

---

Length Field: N/A

---

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

---

Data Representation: n-10

---

Length Field: N/A

---

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

---

Data Representation: n-10

---

Length Field: N/A

---

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

---

Data Representation: n-10

---

Length Field: N/A

---

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

---

Data Representation: n-10

---

Length Field: N/A

---

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

---

Data Representation: n-10

---

Length Field: N/A

---

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

---

Data Representation: n-10

---

Length Field: N/A

---

Data Field: N/A

---

Subfields: N/A

---

Justification: Right

---

### Usage

---

The Authorization Platform currently does not use this data element.

---

## DE 80—Inquiries, Number

DE 80 (Inquiries, Number) is the sum number of inquiry transaction requests processed.

---

### Attributes

---

Data Representation: n-10

---

---

Length Field:	N/A
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

---

Data Representation:	n-10
Length Field:	N/A
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

---

Data Representation:	n-12
Length Field:	N/A
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**

---

Data Representation: n-12

---

Length Field: N/A

---

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**

---

Data Representation: n-12

---

Length Field: N/A

---

Data Field: N/A

---

Subfields: N/A

---

Justification: Right

---

**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

---

Data Representation: n-12

---

Length Field: N/A

---

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

---

Data Representation: n-16

---

Length Field: N/A

---

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

---

Data Representation: n-16

---

Length Field: N/A

---

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

---

Data Representation: n-16

---

Length Field: N/A

---

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

---

Data Representation: n-16

---

Length Field: N/A

---

Data Field: N/A

---

---

Subfields: N/A

Justification: Right

**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

---

Data Representation: n-42

---

Length Field: N/A

---

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.

DE 90, subfield 1 must contain the Message Type Identifier (MTI) of the original authorization message. The remaining subfields may contain valid matching values from the original authorization or may be zero-filled if they are not available.

For reversal messages, if DE 7 (Transmission Date and Time) and DE 11 (System Trace Audit Number [STAN]) from the original Authorization 0100/0110 cannot be saved, DE 90, subelements 2 and 3 may be zero-filled within the Reversal Request/0400 message.

---

### **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. If the Forwarding Institution ID code was not present in the original message, then subfield 5 must contain all zeros.

---

## DE 91—Issuer File Update Code

DE 91 (Issuer File Update Code) indicates to the system maintaining a file which procedure to follow.

### Attributes

Data Representation: an-1

Length Field: N/A

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
--	---	----	----

### Values

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

Data Representation: an-2

Length Field: N/A

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

Data Representation: n-5

Length Field: N/A

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

Data Representation: ans-7

Length Field: N/A

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

---

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

---

Data Representation: n-42

---

Length Field: N/A

---

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.

---

## 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

---

Data Representation:	ISO: b-8 Mastercard: n-8
Length Field:	N/A
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 messages.

---

## DE 97—Amount, Net Settlement

DE 97 (Amount, Net Settlement) is the net value of all gross amounts.

---

### Attributes

---

Data Representation:	an-17
----------------------	-------

---

---

Length Field:	N/A
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
<b>Values</b>	
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
<b>Values</b>	
N/A	

---

## **DE 98—Payee**

DE 98 (Payee), is the third-party beneficiary in a payment transaction.

---

Attributes	
Data Representation:	ans-25

---

---

Length Field:	N/A
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	
Data Representation:	n...11; LLVAR
Length Field:	2
Data Field:	N/A
Subfields:	N/A
Justification:	N/A
<b>Usage</b>	
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	
Data Representation:	n...11; LLVAR
Length Field:	2
Data Field:	Contents of positions 1–11
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

---

Data Representation:	ans...17; LLVAR
----------------------	-----------------

Length Field:	2
---------------	---

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

### Values

MCC102	=	Stand-In Account File
MCC103	=	Electronic Warning Bulletin File
MCC104	=	Local Stoplist File
MCC105	=	Payment Cancellation File
MCC106	=	PAN Mapping File
MCC107	=	Enhanced Value File
MCC108	=	Product Graduation File
MCC109	=	Contactless Application Transaction Counter (ATC) File
MCC111	=	PAN-PAR (Payment Account Reference) Mapping File

## DE 102—Account ID 1

DE 102 (Account ID-1) is a series of digits that identify a customer account or relationship. Customers 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

Data Representation:	ans...28; LLVAR
Length Field:	2
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
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. Customers primarily use it for the “to” account in a transfer transaction.

---

### Attributes

---

Data Representation: ans...28; LLVAR

---

Length Field: 2

---

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

---

---

Data Representation: ans...100; LLLVAR

Length Field: 3

Data Field: N/A

Subfields: N/A

Justification: N/A

---

**Usage**

The Authorization Platform currently does not use this data element.

---

## DE 105–DE 107—Reserved for Mastercard Use

---

DE 105–DE 107 (Reserved for Mastercard Use) are reserved for Mastercard use.

---

**Attributes**

---

Data Representation: ans...999; LLLVAR

Length Field: 3

Data Field: N/A

Subfields: N/A

Justification: N/A

---

**Usage**

The Authorization Platform currently does not use this data element.

---

## DE 108—MoneySend Reference Data

---

DE 108 (MoneySend Reference Data) provides the capability for the acquirers to send in sender, receiver, and transaction level data to the issuer in MoneySend Payment Transactions and MoneySend Funding Transactions. DE 108 provides the capability to acquirers to send to the issuer data for Mastercard™ Merchant Presented QR Payment Transactions, and Mastercard Merchant Presented QR Funding Transactions.

---

**Attributes**

---

Data Representation: ans...999; LLLVAR

Length Field: 3

Data Field: Contents of subelements

---

---

Subelements:	6
Justification:	See "Subelements"

---

### **Usage—MoneySend Transactions**

---

Following is the usage of DE 108 (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
Reversal Request/0400	O	•	C
Reversal Request Response/0410	C	•	C

---

### **Application Notes For MoneySend Transactions**

---

For MoneySend Payment Transactions, acquirers that process transactions must send and receive DE 108 (MoneySend Reference Data). Issuers must receive and return DE 108 (MoneySend Reference Data) for all MoneySend Payment Transactions.

For MoneySend Funding Transactions, acquirers that process transactions may optionally send and be prepared to receive if sending DE 108 (MoneySend Reference Data) for MoneySend Funding Transactions. Issuers must receive and return DE 108 (MoneySend Reference Data) when submitted by the acquirer on MoneySend Funding Transactions.

MoneySend Transactions will not contain the following (Mastercard Merchant Presented QR only) DE 108 subelements and subfields.

- Subelement 05 (Digital Account Information), subfield 01 (Digital Account Reference Number)
  - Subelement 05, subfield 02 (Mastercard Merchant Presented QR Receiving Account Number)
  - Subelement 06 (QR Dynamic Code Data)
- 

### **Application Notes For Mastercard Merchant Presented QR Transactions**

---

For Mastercard Merchant Presented QR Funding Transactions, acquirers that process transactions must send DE 108 (MoneySend Reference Data). Issuers must receive DE 108 (MoneySend Reference Data) for all Mastercard Merchant Presented QR Funding Transactions.

Mastercard Merchant Presented QR Payment Transactions may contain the following DE 108 subelements and subfields.

- Subelement 02 (Sender Data), subfield 11 (Sender Account Number)
- Subelement 03 (MoneySend Transaction Data), subfield 01 (Unique Transaction Reference Number)
- Subelement 03, subfield 02 (Additional Message) (Payment Transactions only)
- Subelement 03, subfield 03 (Funding Source)
- Subelement 05 (Digital Account Information), subfield 01 (Digital Account Reference Number)
- Subelement 05, subfield 02 (Mastercard Merchant Presented QR Receiving Account Number)
- Subelement 06 (QR Dynamic Code Data)

Mastercard Merchant Presented QR Payment Transactions will not return DE 108 to the acquirer in any response message.

Customers should be aware that QR data for Mastercard Merchant Presented QR Payment Transactions, may be received in either DE 108 subelement 03, subfield 02 or DE 108, subelement 06. Subelement 06 is considered the primary location and should be considered first as the location for QR Data.

---

## **DE 108—Authorization Platform Edits**

The Authorization Platform will perform the following system edit to verify proper formatting of DE 108.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
An Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or Reversal Request/0400 message contains DE 48 (Additional Data—Private Use), DE 108 (MoneySend Reference Data), or DE 112 (Additional Data [National Use]) with subelements that have incorrect length and/or incorrect format (Data Representations), or have multiple instances of the same subelement (when not permitted) within the same data element.	<p>Rejects the message and forwards the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 message where DE 44 is 6 positions for subelement format errors:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Message format error)</li> <li>• DE 44 (Additional Response Data) = 0480nn, or 1080nn, or 1120nn (where nn is the subelement number)</li> </ul> <p>(DE 44 is three positions for Dual Message System (Authorization) if no subelements are present, for example, for DE 22 format error: DE 44 = 022)</p>

Examples:

- When an edit error occurs on DE 48, the DE 44 data will be populated as these examples below:
  - Error on DE 48 subelement 42, subfield 1: 048042 (no subfield information is provided)
  - Error on DE 48 subelement 61: 048061
- DE 48 TCC format error will be responded with DE 44 = 048000.

For non-DE 48/DE 108/DE 112 format errors, DE 44 will only have DE info and no subelement information. For example, the format error in DE 22 will have DE 44 as 022 for non-DE48/108/112 data elements.

## **Subelement 01—Receiver/Recipient Data**

This subelement contains the receiver name, address, phone number, date of birth, and account details.

<b>Attribute</b>	<b>Value</b>
Subelement ID	01
Subelement Length	3
Data Representation	ans...322; LLLVAR

Attribute	Value
Number of Subfields	17
	Subfield 01—Receiver/Recipient First Name
	Subfield 02—Receiver/Recipient Middle Name
	Subfield 03—Receiver/Recipient Last Name
	Subfield 04—Receiver/Recipient Street Address
	Subfield 05—Receiver/Recipient City
	Subfield 06—Receiver/Recipient State/Province Code
	Subfield 07—Receiver/Recipient Country
	Subfield 08—Receiver/Recipient Postal Code
	Subfield 09—Receiver/Recipient Phone Number
	Subfield 10—Receiver/Recipient Date of Birth
	Subfield 11—Receiver/Recipient Account Number
	Subfield 12—Receiver/Recipient Identification Type
	Subfield 13—Receiver/Recipient Identification Number
	Subfield 14—Receiver/Recipient Identification Country Code
	Subfield 15—Receiver/Recipient Identification Expiration Date
	Subfield 16—Receiver/Recipient Nationality
	Subfield 17—Receiver/Recipient Country of Birth

---

### **Subfield 01—Receiver/Recipient First Name**

DE 108, subelement 01, subfield 01 (Receiver/Recipient First Name) contains the Recipient/Receiver first name.

<b>Attribute</b>	
Subfield ID	01
Subfield Length	2
Data Representation	ans...35; LLVAR
Justification	N/A

<b>Values</b>	<b>Description</b>
If present, cannot contain all spaces or all numeric values.	

---

#### **Application Notes**

Subfield 01 must be present for cross-border MoneySend Payment Transactions and must be properly formatted. Subfield 01 is optional for MoneySend Funding Transactions and domestic MoneySend Payment Transactions.

The first name (Consumer/Business) of the recipient/receiver is included in this subelement.

The table that follows describes the correct submission of business names.

---

#### **Application Notes—Mastercard Merchant Presented QR Transactions**

Subfield 01 is optional for Mastercard Merchant Presented QR Payment Transactions. It is not edited and will be forward to destination.

Subfield 01 is not applicable for Mastercard Merchant Presented QR Refund Payment or Funding Transactions.

<b>Business Name</b>	<b>First Name</b>	<b>Last Name</b>
XYZ	XYZ	XYZ
XYZ International	XYZ	International
XYZ DBA MA	XYZ	DBA MA

### **Subfield 02—Receiver/Recipient Middle Name**

DE 108, subelement 01, subfield 02 (Receiver/Recipient Middle Name) contains the middle name of the Recipient/Receiver.

<b>Attribute</b>	<b>Value</b>
Subfield ID	02
Subfield Length	2
Data Representation	ans-1
Justification	N/A

<b>Values</b>	<b>Description</b>
	Valid value will consist of the middle name initial of the Receiver.
<b>Application Notes</b>	
Subfield 02 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subfield 03—Receiver/Recipient Last Name**

DE 108, subelement 01, subfield 03 (Receiver/Recipient Last Name) contains the last name of the Recipient/Receiver.

<b>Attribute</b>
Subfield ID
03
Subfield Length
2
Data Representation
ans...35; LLVAR
Justification
N/A

<b>Values</b>	<b>Description</b>
	If present cannot contain all spaces or all numeric values.
<b>Application Notes</b>	

---

Values	Description
--------	-------------

Subfield 03 must be present for cross-border MoneySend Payment Transaction and must be properly formatted. Subfield 03 is optional for MoneySend Funding and Domestic MoneySend Payment Transactions.

The last name (Consumer/Business) of the recipient/receiver is included in this subelement.

The table that follows describes the correct submission of business names.

---

#### **Application Notes—Mastercard Merchant Presented QR Transactions**

Subfield 03 is optional for Mastercard Merchant Presented QR Payment Transactions. It is not edited and will be forward to destination.

Subfield 03 is not applicable for Mastercard Merchant Presented QR Refund Payment or Funding Transactions.

---

Business Name	First Name	Last Name
XYZ	XYZ	XYZ
XYZ International	XYZ	International
XYZ DBA MA	XYZ	DBA MA

#### **Subfield 04—Receiver/Recipient Street Address**

DE 108, subelement 01, subfield 04 (Receiver/Recipient Street Address) contains the Street Address of the Recipient/Receiver.

---

Attribute	
Subfield ID	04
Subfield Length	2
Data Representation	ans...50; LLVAR
Justification	N/A

---

Values	Description
--------	-------------

Valid value will consist of the street address of the Receiver.

---

#### **Application Notes**

Values	Description
	Subfield 04 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

### **Subfield 05—Receiver/Recipient City**

DE 108, subelement 01, subfield 05 (Receiver/Recipient City) contains the city of the Receiver/Recipient.

Attributes	
Subfield ID	05
Subfield Length	2
Data Representation	ans...25; LLVAR
Justification	N/A

### **Values**

Valid location city name of the Receiver/Recipient.

### **Application Notes**

Subfield 05 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

### **Application Notes—Mastercard Merchant Presented QR Transactions**

Subfield 05 is optional for Mastercard Merchant Presented QR Payment Transactions. It is not edited and will be forward to destination.

Subfield 05 is not applicable for Mastercard Merchant Presented QR Refund Payment or Funding Transactions.

### **Subfield 06—Receiver/Recipient State/Province Code**

DE 108, subelement 01, subfield 06 (Receiver/Recipient State/Province Code) contains the state/province code of the Recipient/Receiver.

Attributes	
Subfield ID	06
Subfield Length	2
Data Representation	ans...3; LLVAR
Justification	N/A

### **Values**

Valid location state code of the Receiver/Recipient.

### **Application Notes**

---

Subfield 06 for MoneySend Payment Transactions cannot contain spaces or invalid code when country is U.S. or Canada. Subfield 06 is optional for MoneySend Funding Transactions.

---

### **Subfield 07—Receiver/Recipient Country**

DE 108, subelement 01, subfield 07 (Receiver/Recipient Country) contains the country of the Recipient/Receiver.

Attribute	Value
Subfield ID	07
Subfield Length	2
Data Representation	ans-3
Justification	N/A

Values	Description
	If present must be a valid ISO country code and must not be part of blocked country list.

#### **Application Notes**

Subfield 07 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

Transaction will be declined if the sender country is subject to comprehensive geographic sanctions published by the Office of Foreign Assets Control (OFAC), <http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx>. The current list of countries subject to such sanctions is Cuba, Iran, North Korea, Sudan, and Syria; however, this list is subject to change.

---

### **Subfield 08—Receiver/Recipient Postal Code**

DE 108, subelement 01, subfield 08 (Receiver/Recipient Postal Code) contains the postal code of the Recipient/Receiver.

Attribute
Subfield ID
Subfield Length
Data Representation
Justification

Values	Description
Valid location Postal Code of the Recipient's/Receiver.	
<b>Application Notes</b>	
Subfield 08 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subfield 09—Receiver/Recipient Phone Number**

DE 108, subelement 01, subfield 09 (Receiver/Recipient Phone Number) contains the phone number of the Recipient/Receiver.

Attribute	
Subfield ID	09
Subfield Length	2
Data Representation	ans...20; LLVAR
Justification	N/A

Values	Description
Valid phone number of the Recipient/Receiver.	
<b>Application Notes</b>	
Subfield 09 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Application Notes—Mastercard Merchant Presented QR Transactions**

Subfield 09 is optional for Mastercard Merchant Presented QR Payment Transactions. It is not edited and will be forward to destination.

Subfield 09 is not applicable for Mastercard Merchant Presented QR Refund Payment or Funding Transactions.

### **Subfield 10—Receiver/Recipient Date of Birth**

DE 108, subelement 01, subfield 10 (Receiver/Recipient Date of Birth) contains the date of birth of the Receiver/Recipient.

Attributes	
Subfield ID	10

---

Subfield Length	2
Data Representation	n-8
Justification	N/A

**Values**

---

Valid date of birth of the Receiver/Recipient in the format MMDDYYYY.

**Application Notes**

---

Subfield 10 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

**Application Notes—Mastercard Merchant Presented QR Transactions**

---

Subfield 10 is optional for Mastercard Merchant Presented QR Payment Transactions. It is not edited and will be forward to destination.

Subfield 10 is not applicable for Mastercard Merchant Presented QR Refund Payment or Funding Transactions.

---

**Subfield 11—Receiver/Recipient Account Number**

DE 108, subelement 01, subfield 11 (Receiver/Recipient Account Number) contains the account number of the Recipient/Receiver.

---

Attribute	
Subfield ID	11
Subfield Length	2
Data Representation	n...20; LLVAR
Justification	N/A

---

Values	Description
--------	-------------

Valid Account Number of the Receiver/Recipient.

**Application Notes**

---

Subfield 11 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

**Application Notes—Mastercard Merchant Presented QR Transactions**

---

Values	Description
	Subfield 11 is optional for Mastercard Merchant Presented QR Payment Transactions. It is not edited and will be forward to destination.
	Subfield 11 is not applicable for Mastercard Merchant Presented QR Refund Payment or Funding Transactions.

### **Subfield 12—Receiver/Recipient Identification Type**

DE 108, subelement 01, subfield 12 (Receiver/Recipient Identification Type) contains the identification type of the Recipient/Receiver.

Attribute	
Subfield ID	12
Subfield Length	2
Data Representation	n-2
Justification	N/A

Values	Description
If present on all MoneySend Payment transactions, it must contain one of the following valid values:	
00	= Passport
01	= National Identification Card
02	= Driver's License
03	= Government Issued
04	= Other
05–10	= Reserved

#### **Application Notes**

Subfield 12 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

### **Subfield 13—Receiver/Recipient Identification Number**

DE 108, subelement 01, subfield 13 (Receiver/Recipient Identification Number) contains the identification number of the Recipient/Receiver.

<b>Attribute</b>	
Subfield ID	13
Subfield Length	2
Data Representation	ans...25; LLVAR
Justification	N/A

<b>Values</b>	<b>Description</b>
Valid identification number of the Receiver/Recipient.	
<b>Application Notes</b>	
Subfield 13 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

#### **Subfield 14—Receiver/Recipient Identification Country Code**

DE 108, subelement 01, subfield 14 (Receiver/Recipient Identification Country Code) contains the identification country code of the Recipient/Receiver.

<b>Attribute</b>	
Subfield ID	14
Subfield Length	2
Data Representation	ans-3
Justification	N/A

<b>Values</b>	<b>Description</b>
Valid identification country code of the Receiver/Recipient.	
<b>Application Notes</b>	
Subfield 14 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

#### **Subfield 15—Receiver/Recipient Identification Expiration Date**

DE 108, subelement 01, subfield 15 (Receiver/Recipient Identification Expiration Date) contains the identification expiration date of the Recipient/Receiver.

<b>Attribute</b>	
Subfield ID	15
Subfield Length	2
Data Representation	n-8
Justification	N/A

<b>Values</b>	<b>Description</b>
	Valid identification expiration date of the Receiver/Recipient in the format MMDDYYYY.
<b>Application Notes</b>	
Subfield 15 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subfield 16—Receiver/Recipient Nationality**

DE 108, subelement 01, subfield 16 (Receiver/Recipient Nationality) contains the nationality of the Recipient/Receiver.

<b>Attribute</b>	
Subfield ID	16
Subfield Length	2
Data Representation	ans-3
Justification	N/A

<b>Values</b>	<b>Description</b>
	Nationality of the Receiver/Recipient as defined by a valid country code for the country of citizenship.
<b>Application Notes</b>	
Subfield 16 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subfield 17—Receiver/Recipient Country of Birth**

DE 108, subelement 01, subfield 17 (Receiver/Recipient Country of Birth) contains the country of birth of the Recipient/Receiver.

<b>Attribute</b>	
Subfield ID	17
Subfield Length	2
Data Representation	ans-3
Justification	N/A

<b>Values</b>	<b>Description</b>
Valid Country of birth of the Receiver/Recipient.	
<b>Application Notes</b>	
Subfield 17 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

## **Subelement 02—Sender Data**

This subelement contains the sender name, address, phone number, date of birth, and account details.

<b>Attribute</b>	<b>Value</b>
Subelement ID	02
Subelement Length	3
Data Representation	ans...322; LLLVAR

<b>Attribute</b>	<b>Value</b>
Number of Subfields	17
	Subfield 01—Sender First Name
	Subfield 02—Sender Middle Name
	Subfield 03—Sender Last Name
	Subfield 04—Sender Street Address
	Subfield 05—Sender City
	Subfield 06—Sender State/Province Code
	Subfield 07—Sender Country
	Subfield 08—Sender Postal Code
	Subfield 09—Sender Phone Number
	Subfield 10—Sender Date of Birth
	Subfield 11—Sender Account Number
	Subfield 12—Sender Identification Type
	Subfield 13—Sender Identification Number
	Subfield 14—Sender Identification Country Code
	Subfield 15—Sender Identification Expiration Date
	Subfield 16—Sender Nationality
	Subfield 17—Sender Country of Birth

### **Subfield 01—Sender First Name**

DE 108, subelement 02, subfield 01 (Sender First Name) contains the first name of the Sender.

<b>Attribute</b>
Subfield ID

<b>Attribute</b>	
Subfield Length	2
Data Representation	ans...35; LLVAR
Justification	N/A

<b>Values</b>	<b>Description</b>
If present, cannot contain all spaces or all numeric values.	

#### **Application Notes**

Subfield 01 must be present for MoneySend Payment Transactions and must be properly formatted.  
Subfield 01 is optional for MoneySend Funding Transactions.

The first name (Consumer/Business/Government/Non-Government Organization) of the sender is included in this subelement.

The table that follows describes the correct submission of business names.

#### **Application Notes—Mastercard Merchant Presented QR Transactions**

Subfield 01 is optional for Mastercard Merchant Presented QR Payment Transactions. It is not edited and will be forward to destination.

Subfield 01 is not applicable for Mastercard Merchant Presented QR Refund Payment or Funding Transactions.

<b>Business Name</b>	<b>First Name</b>	<b>Last Name</b>
XYZ	XYZ	XYZ
XYZ International	XYZ	International
XYZ DBA MA	XYZ	DBA MA

#### **Subfield 02—Sender Middle Name**

DE 108, subelement 02, subfield 02 (Sender Middle Name) contains the middle name initial of the Sender.

<b>Attribute</b>	<b>Value</b>
Subfield ID	02

<b>Attribute</b>	<b>Value</b>
Subfield Length	2
Data Representation	ans-1
Justification	N/A

<b>Values</b>	<b>Description</b>
	Valid value will consist of the middle name initial of the Sender.
<b>Application Notes</b>	
Subfield 02 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subfield 03—Sender Last Name**

DE 108, subelement 02, subfield 03 (Sender Last Name) contains the last name of the Sender.

<b>Attribute</b>
Subfield ID
03
Subfield Length
2
Data Representation
ans...35; LLVAR
Justification
N/A

<b>Values</b>	<b>Description</b>
	If present, cannot contain all spaces or numeric values.
<b>Application Notes</b>	
Subfield 03 must be present for MoneySend Payment Transactions and must be properly formatted. Subfield 03 is optional for MoneySend Funding Transactions.	

The last name (Consumer/Business/Government/Non-Government Organization) of the sender is included in this subelement.

The table that follows describes the correct submission of business names.

---

#### **Application Notes—Mastercard Merchant Presented QR Transactions**

---

Values	Description
	Subfield 03 is optional for Mastercard Merchant Presented QR Payment Transactions. It is not edited and will be forward to destination.
	Subfield 03 is not applicable for Mastercard Merchant Presented QR Refund Payment or Funding Transactions.

Business Name	First Name	Last Name
XYZ	XYZ	XYZ
XYZ International	XYZ	International
XYZ DBA MA	XYZ	DBA MA

#### **Subfield 04—Sender Street Address**

DE 108, subelement 02, subfield 04 (Sender Street Address) contains the street address of the Sender.

Attribute	
Subfield ID	04
Subfield Length	2
Data Representation	ans...50; LLVAR
Justification	N/A

Values	Description
	Valid values will consist of street address of the Sender.
<b>Application Notes</b>	
	Subfield 04 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

#### **Subfield 05—Sender City**

DE 108, subelement 02, subfield 05 (Sender City) contains the city of the Sender.

<b>Attribute</b>	
Subfield ID	05
Subfield Length	2
Data Representation	ans...25; LLVAR
Justification	N/A

<b>Values</b>	<b>Description</b>
	Valid location city name of the Sender.

**Application Notes**

Subfield 05 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

**Subfield 06—Sender State/Province Code**

DE 108, subelement 02, subfield 06 (Sender State/Province Code) contains the state/province code of the Sender.

**Attributes**

Subfield ID	06
Subfield Length	2
Data Representation	ans...3; LLVAR
Justification	N/A

**Values**

Valid location State code of the Sender. Cannot contain spaces or invalid code when country is U.S. or Canada.

**Application Notes**

Subfield 06 is optional for MoneySend Payment Transactions and MoneySend Funding Transactions. If submitted on MoneySend Payment Transactions, subfield 06 cannot contain spaces or invalid code when country is U.S. or Canada.

**Subfield 07—Sender Country**

DE 108, subelement 02, subfield 07 (Sender Country) contains the country code of the Sender.

<b>Attribute</b>	<b>Value</b>
Subfield ID	07
Subfield Length	2
Data Representation	ans-3
Justification	N/A

<b>Values</b>	<b>Description</b>
	If present must be a valid ISO country code and must not be part of blocked country list.

#### **Application Notes**

Subfield 07 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions. Transaction will be declined if the sender country is subject to comprehensive geographic sanctions published by the Office of Foreign Assets Control (OFAC), <http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx>. The current list of countries subject to such sanctions is Cuba, Iran, North Korea, Sudan, and Syria; however, this list is subject to change.

### **Subfield 08—Postal Code**

DE 108, subelement 02, subfield 08 (Postal Code) contains the postal code of the Sender.

<b>Attributes</b>	
Subfield ID	08
Subfield Length	2
Data Representation	ans...10; LLVAR
Justification	N/A

#### **Values**

Valid location Postal Code of the Sender.

#### **Application Notes**

Subfield 08 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

### **Subfield 09—Sender Phone Number**

DE 108, subelement 02, subfield 09 (Sender Phone Number) contains the phone number of the Sender.

<b>Attribute</b>	
Subfield ID	09
Subfield Length	2
Data Representation	ans...20; LLVAR
Justification	N/A

<b>Values</b>	<b>Description</b>
	Valid phone number of the Sender.
<b>Application Notes</b>	
Subfield 09 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subfield 10—Sender Date of Birth**

DE 108, subelement 02, subfield 10 (Sender Date of Birth) contains the date of birth of the Sender.

<b>Attributes</b>	
Subfield ID	10
Subfield Length	2
Data Representation	n-8
Justification	N/A

<b>Values</b>	
Valid values will consist of the date of birth of the Sender in the format MMDDYYYY.	
<b>Application Notes</b>	
Subfield 10 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subfield 11—Sender Account Number**

DE 108, subelement 02, subfield 11 (Sender Account Number) contains the account number of the Sender.

<b>Attribute</b>	
Subfield ID	11

<b>Attribute</b>	
Subfield Length	2
Data Representation	n...20; LLVAR
Justification	N/A

<b>Values</b>	<b>Description</b>
	<p>Valid account number of the Sender.</p> <p>The account number that was used to fund the money transfer (for example, the sender used a credit, debit, or other account to fund the money transfer). When cash is used to fund the money transfer, this field should be populated with a unique transaction reference number or an account number from the OI. This information will assist in identifying the sender if the receiving institution requires additional information from the originating institution for the money transfer.</p>

#### **Application Notes—MoneySend Transactions**

Subfield 11 must be present for MoneySend Payment Transactions and must be properly formatted. Subfield 11 is optional for MoneySend Funding Transactions.

#### **Application Notes—Mastercard Merchant Presented QR Transactions**

##### **Payment Transaction Usage:**

- Authorization Request/0100—Mandatory. Edit must validate. Forward to destination
- Reversal Advice/0420—Value from Authorization Request/0100 forwarded to destination

##### **Refund Payment Transaction Usage:**

- Reversal Advice/0420—Value from Authorization Request/0100 forwarded to destination

##### **Funding Transaction Usage:**

- Subfield 11 is not applicable

#### **Subfield 12—Sender Identification Type**

DE 108, subelement 02, subfield 12 (Sender Identification Type) contains the identification type of the Sender.

<b>Attribute</b>	
Subfield ID	12
Subfield Length	2
Data Representation	n-2

<b>Attribute</b>	
Justification	N/A

<b>Values</b>	<b>Description</b>
If present on all MoneySend Payment transactions, it must contain one of the following valid values:	
00	= Passport
01	= National Identification Card
02	= Driver's License
03	= Government Issued
04	= Other
05–10	= Reserved

#### **Application Notes**

Subfield 12 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

### **Subfield 13—Sender Identification Number**

DE 108, subelement 02, subfield 13 (Sender Identification Number) contains the identification number of the Sender.

<b>Attribute</b>	
Subfield ID	13
Subfield Length	2
Data Representation	ans...25; LLVAR
Justification	N/A

<b>Values</b>	<b>Description</b>
	Valid identification number of the Sender.

#### **Application Notes**

Subfield 13 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.

### **Subfield 14—Sender Identification Country Code**

DE 108, subelement 02, subfield 14 (Sender Identification Country Code) contains the identification country code of the Sender.

<b>Attribute</b>	
Subfield ID	14
Subfield Length	2
Data Representation	ans-3
Justification	N/A

<b>Values</b>	<b>Description</b>
	Valid identification country code of the Sender.
<b>Application Notes</b>	
Subfield 14 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subfield 15—Sender Identification Expiration Date**

DE 108, subelement 02, subfield 15 (Sender Identification Expiration Date) contains the identification expiration date of the Sender.

<b>Attribute</b>	
Subfield ID	15
Subfield Length	2
Data Representation	n-8
Justification	N/A

<b>Values</b>	<b>Description</b>
	Valid identification expiration date of the Sender in the format MMDDYYYY.
<b>Application Notes</b>	
Subfield 15 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subfield 16—Sender Nationality**

DE 108, subelement 02, subfield 16 (Sender Nationality) contains the nationality of the Sender.

<b>Attribute</b>	
Subfield ID	16
Subfield Length	2
Data Representation	ans-3
Justification	N/A

<b>Values</b>	<b>Description</b>
	Nationality of the sender as defined by a valid country code for the country of citizenship.
<b>Application Notes</b>	
Subfield 16 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subfield 17—Sender Country of Birth**

DE 108, subelement 02, subfield 17 (Sender Country of Birth) contains the country of birth of the Sender.

<b>Attribute</b>	
Subfield ID	17
Subfield Length	2
Data Representation	ans-3
Justification	N/A

<b>Values</b>	<b>Description</b>
	Valid country of birth of the Sender.
<b>Application Notes</b>	
Subfield 17 is optional for MoneySend Funding Transactions and MoneySend Payment Transactions.	

### **Subelement 03—MoneySend Transaction Data**

This subelement contains the transaction reference number, funding source, participation ID, and additional data related to MoneySend transactions and Mastercard Merchant Presented QR transactions.

<b>Attribute</b>	<b>Value</b>	
Subelement ID	03	
Subelement Length	3	
Data Representation	ans...138; LLLVAR	
Number of Subfields	5	Subfield 01—Unique Transaction Reference
		Subfield 02—Additional Message
		Subfield 03—Funding Source
		Subfield 04—Participant ID
		Subfield 05—Transaction Purpose

#### **Subfield 01—Unique Transaction Reference**

DE 108, subelement 03, subfield 01 (Unique Transaction Reference) contains the Unique Transaction Reference number for Mastercard Merchant Presented QR Funding Transactions.

<b>Attribute</b>	<b>Value</b>
Subfield ID	01
Subfield Length	2
Data Representation	ans-19
Justification	N/A

Values	Description
	<p>Unique Transaction Reference Number (ans-19). Valid value string will contain a leading zero (0), followed by:</p> <ul style="list-style-type: none"><li>• ICA (n-6)</li><li>• Year (n-1)</li><li>• Julian Date (n-3)</li><li>• Time hhmmss (n-6)</li><li>• Transaction Sequence Number (01–99) (n-2)</li></ul> <p>Example: 0555555801215305401</p>

---

#### **Application Notes**

---

Subfield 01 is optional for MoneySend Funding and MoneySend Payment Transactions.

---

#### **Application Notes—Mastercard Merchant Presented QR Transactions**

---

##### **Payment Transaction Usage:**

- Authorization Request/0100—Optional. If present, edit must validate. Forward to destination if edit validates
- Reversal Advice/0420—Optional. If present, value from Authorization Request/0100 forwarded to destination

##### **Refund Payment Transaction Usage:**

- Authorization Request/0100—Optional. If present, edit must validate. Forward to destination if edit validates
- Reversal Advice/0420—Value from Authorization Request/0100 forwarded to destination

##### **Funding Transaction Usage:**

- Authorization Request/0100—Mandatory. If present, edit must validate. Forward to destination if edit validates
  - Authorization Advice/0120—Optional. If present, edit must validate. Forward to destination if edit validates
  - Reversal Request/0400—Optional. If present, edit must validate. Forward to destination if edit validates
  - Reversal Advice/0420—Value from Authorization Request/0100 forwarded to destination
- 

#### **Subfield 02—Additional Message**

DE 108, subelement 03, subfield 02 (Additional Message) contains the additional message.

<b>Attribute</b>	
Subfield ID	02
Subfield Length	2
Data Representation	ans...65; LLVAR
Justification	N/A

<b>Values</b>	<b>Application Notes</b>
Subfield 02 is optional for MoneySend Funding and MoneySend Payment Transactions.	

#### **Application Notes—Mastercard Merchant Presented QR Transactions**

##### **Payment Transaction Usage:**

- Authorization Request/0100—Optional. If present, edit must validate. Forward to destination if edit validates
- Reversal Advice/0420—Optional. If present, value from Authorization Request/0100 forwarded to destination

##### **Refund Payment Transaction Usage:**

- Subfield 02 is not applicable

##### **Funding Transaction Usage:**

- Authorization Advice/0120—Optional. If present, edit must validate. Forward to destination if edit validates
- Reversal Request/0400—Optional. If present, edit must validate. Forward to destination if edit validates
- Reversal Advice/0420—Value from Authorization Request/0100 forwarded to destination

#### **Subfield 03—Funding Source**

DE 108, subelement 03, subfield 03 (Funding Source) contains the information representing the MoneySend transaction funding source.

<b>Attribute</b>	
Subfield ID	03

Attribute	
Subfield Length	2
Data Representation	n-2;
Justification	N/A

Values	Description
Must be present, and must contain one of the following valid values for MoneySend Payment Transactions:	
<ul style="list-style-type: none"><li>• 01=Credit</li><li>• 02=Debit</li><li>• 03=Prepaid</li><li>• 04=Deposit Account</li><li>• 05=Mobile Money Account</li><li>• 06=Cash</li><li>• 07=Reserved for future use</li></ul>	

#### **Application Notes**

Subfield 03 is optional for MoneySend Funding transactions.

#### **Application Notes—Mastercard Merchant Presented QR Transactions**

##### **Payment Transaction Usage:**

- Authorization Request/0100—Mandatory. Edit must validate. Forward to destination
- Reversal Advice/0420—Value from Authorization Request/0100 forwarded to destination

##### **Refund Payment Transaction Usage:**

- Reversal Advice/0420—Value from Authorization Request/0100 forwarded to destination

##### **Funding Transaction Usage:**

- Subfield 03 is not applicable

#### **Subfield 04—Participation ID**

DE 108, subelement 03, subfield 04 (Participation ID) contains participation ID details of the Sender.

Attribute	
Subfield ID	04

<b>Attribute</b>	
Subfield Length	2
Data Representation	ans...30; LLVAR
Justification	N/A

<b>Values</b>	<b>Description</b>
	Contains the participation ID of the Sender.
<b>Application Notes</b>	
Subfield 04 is optional for MoneySend Payment and MoneySend Funding Transactions.	

### **Subfield 05—Transaction Purpose**

DE 108, subelement 03, subfield 05 (Transaction Purpose) contains MoneySend transaction purpose details.

<b>Attribute</b>	
Subfield ID	05
Subfield Length	2
Data Representation	n-2
Justification	N/A

Values	Description
If present on a MoneySend Payment transaction, it must contain one of the following valid values:	
00	= Family Support
01	= Regular Labor Transfers (expatriates)
02	= Travel & Tourism
03	= Education
04	= Hospitalization & Medical Treatment
05	= Emergency Need
06	= Savings
07	= Gifts
08	= Other
09–15	= Reserved

---

#### Application Notes

---

Subfield 05 is optional for MoneySend Payment and MoneySend Funding Transactions.

---

### Subelement 04—MoneySend Language Description

This subelement contains additional language details supported by the customer.

Attribute	Value
Subelement ID	04
Subelement Length	3
Data Representation	ans...061; LLLVAR
Number of Subfields	2
	Subfield 1—Language Identification
	Subfield 2—Language Data

#### Subfield 01—Language Identification

DE 108, subelement 04, subfield 01 (Language Identification) contains information about the language selected by the customer.

<b>Attribute</b>	<b>Value</b>
Subfield ID	01
Subfield Length	2
Data Representation	ans-3
Justification	N/A

---

#### **Application Notes**

Subfield 01 is optional for MoneySend Funding and MoneySend Payment Transactions.

---

<b>Attribute</b>
Subfield ID
02
Subfield Length
2
Data Representation
b...50; LLVAR
Justification
N/A

---

#### **Application Notes**

Subfield 02 is optional for MoneySend Funding and MoneySend Payment Transactions.

---

### **Subelement 05—Digital Account Information**

DE 108 (MoneySend Reference Data), subelement 05 (Digital Account Information) contains data specific to Mastercard Merchant Presented QR transactions.

<b>Attribute</b>	<b>Value</b>
Subelement ID	n-2
Subelement Length	3

Attribute	Value	
Data Representation	ans...99; LLLVAR	
Number of Subfields	2	Subfield 01—Digital Account Reference Number Subfield 02—Mastercard Merchant Presented QR Receiving Account Number

---

#### Application Notes

---

Subelement 05 is used only for Mastercard Merchant Presented QR transactions.

**NOTE: Subelement 05 becomes effective as of 12 June 2018.**

---

#### Subfield 01—Digital Account Reference Number

DE 108 (MoneySend Reference Data), subelement 05 (Digital Account Information), subfield 01 (Digital Account Reference Number) is provided in a Mastercard Merchant Presented QR Payment Transaction to allow Receiving Institutions the ability to initiate a refund to the consumer via the Originating Institution. **NOTE: Subfield 01 is effective as of 12 June 2018.**

Attribute
Subfield ID
01
Subfield Length
2
Data Representation
n...19; LLVAR
Justification
N/A

---

### Application Notes—Mastercard Merchant Presented QR Transactions

---

#### Payment Transaction Usage:

- Authorization Request/0100—Optional. If present, edit must validate. If not present, Mastercard will populate with value from DE 108, subelement 02, subfield 11 (Sender Account Number); Forward to destination.
- Reversal Advice/0420—Optional. If present, value from Authorization Request/0100 forwarded to destination

#### Refund Payment Transaction Usage:

- Reversal Advice/0420—Value from Authorization Request/0100 forwarded to destination

#### Funding Transaction Usage:

- Subfield 01 is not applicable
- 

### Subfield 02—Mastercard Merchant Presented QR Receiving Account Number

DE 108 (MoneySend Reference Data), subelement 05 (Digital Account Information), subfield 02 (Mastercard Merchant Presented QR Receiving Account Number) provided in a Mastercard Merchant Presented QR Funding Transaction contains the receiving account number.

Attribute	
Subfield ID	02
Subfield Length	2
Data Representation	ans...34; LLVAR
Justification	NA

Values	Description
Valid Account Number of the Receiver.	

---

### Application Notes—Mastercard Merchant Presented QR Transactions

---

#### Payment Transaction Usage:

- Subfield 02 is not applicable

#### Refund Payment Transaction Usage:

- Subfield 02 is not applicable

#### Funding Transaction Usage:

- Authorization Request/0100—Optional. If present, edit must validate. Forward to destination if edit validates
  - Authorization Advice/0120—Optional. If present, edit must validate. Forward to destination if edit validates
  - Reversal Request/0400—Optional. If present, edit must validate. Forward to destination if edit validates
  - Reversal Advice/0420—Optional. If present, value from Authorization Request/0100 forwarded to destination
- 

### Subelement 06—QR Dynamic Code Data

DE 108 (MoneySend Reference Data), subelement 06 (QR Dynamic Code Data) is available for regional data with limited Mastercard editing or data validation.

Attribute	Value
Subelement ID	06
Subelement Length	3
Data Representation	ans...237; LLLVAR
Justification	Left
Number of Subfields	N/A

---

#### Values

---

If present, must be alphanumeric or special characters and a valid length.

---

---

## Application Notes—Mastercard Merchant Presented QR Transactions

---

### Payment Transaction Usage:

- Authorization Request/0100—Optional. If present, edit must validate. Forward to destination if edit validates
- Reversal Advice/0420—Optional. If present, value from Authorization Request/0100 forwarded to destination

### Refund Payment Transaction Usage:

- Subelement 06 is not applicable

### Funding Transaction Usage:

- Authorization Request/0100—Optional. If present, edit must validate. Forward to destination if edit validates
  - Authorization Advice/0120—Optional. If present, edit must validate. Forward to destination if edit validates
  - Reversal Request/0400—Optional. If present, edit must validate. Forward to destination if edit validates
  - Reversal Advice/0420—Optional. If present, value from Authorization Request/0100 forwarded to destination
- 

## DE 109—Reserved for ISO Use

---

DE 109 (Reserved for ISO Use) is reserved for ISO use.

---

### Attributes

---

Data Representation: ans...999; LLLVAR

---

Length Field: 3

---

Data Field: N/A

---

Subfields: N/A

---

Justification: N/A

---

### Usage

---

The Authorization Platform currently does not use this data element.

---

## DE 110—Additional Data–2

DE 110 (Additional Data-2) is reserved for use based on product type.

### Attributes

Data Representation:	ISO Standard: ans...999; LLLVAR Mastercard Standard: ans...999; LLLVAR
Length Field:	3 positions, value =...999
Data Field:	Contents of subelements 9-10
Subelements:	2
Justification:	See "Subelements"

### Usage

Following is the usage of DE 110 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages.

Message	Org	Sys	Dst
Network Management Request/0800—PEK Exchange	•	O	C
Network Management Request Response/0810—PEK Exchange	O	M	•
Network Management Advice/0820—PEK Exchange	•	M	M

### Application Notes

DE 110 provides 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 that may be used for multiple purposes. This data element's content may vary by program and service.

The following tables provide formats and descriptions for the subelements in DE 110. Currently, there are two subelements but as subelements are added, the subelement sequence will not have to be in the order of ID value.

---

## **Subelement 9—ANSI X9 TR-31 Key Block Key (128-bit Key Block Protection Key)**

DE 110, subelement 9 (ANSI X9 TR-31 Key Block Key [128-bit Key Block Protection Key]) contains the attributes provided in a Network Management Request/0800 message.

<b>Attribute</b>	<b>Value</b>
Subelement ID	n-2
Subelement Length	n-3
Data Representation	an-80

---

### **Usage**

Following is the usage of subelement 09 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Network Management Request/0800 —PEK Exchange	•	M	M
Network Management Request Response/0810— PEK Exchange	O	C	•
Network Management Request Advice/0820— PEK Exchange	•	•	•

---

## **Subelement 9—ANSI X9 TR-31 Key Block Key (192-bit Key Block Protection Key)**

DE 110, subelement 9 (ANSI X9 TR-31 Key Block Key [192-bit Key Block Protection Key]) contains the attributes provided in a Network Management Request/0800 message.

<b>Attribute</b>	<b>Value</b>
Subelement ID	n-2
Subelement Length	n-3
Data Representation	an-96

---

### **Usage**

Following is the usage of subelement 09 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

---

#### **Usage**

<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Network Management Request/0800 —PEK Exchange	•	M	M
Network Management Request Response/0810— PEK Exchange	O	C	•
Network Management Request Advice/0820— PEK Exchange	•	•	•

---

#### **Subelement 10—Key Check Value**

DE 110, subelement 10 (Key Check Value) contains the attributes in a Network Management Request/0800 message.

<b>Attribute</b>	<b>Value</b>
Subelement ID	n-2
Subelement Length	n-3
Data Representation	an-6

---

#### **Usage**

Following is the usage of subelement 10 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Network Management Request/0800 —PEK Exchange	•	M	M
Network Management Request Response/0810— PEK Exchange	O	C	•
Network Management Request Advice/0820— PEK Exchange	•	M	M

---

#### **DE 111—Reserved for ISO Use**

---

DE 111 (Reserved for ISO Use) is reserved for ISO use.

<b>Attributes</b>	
Data Representation:	ans...999; LLLVAR
Length Field:	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 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.

<b>Attributes</b>	
Data Representation:	ans...100; LLLVAR (The operational length is limited to 100 bytes for global usage)  ans-176 (for Brazil domestic usage only for Brazil Commercial and Financing Data)  ans-233 (for Brazil domestic usage only for BNDES card alternative financing options)  ans...195; LLLVAR (for Japan domestic usage only for Japan National Data payment transactions)  ans...779 (Global for all regions for the Mastercard Installment Payment Service)  For customers in the Europe region participating in installment payments, the overall length of DE 112 is restricted to 591 bytes to accommodate operational limitations.
Length Field:	3
Data Field:	Contents of subelements
Subelements:	Determined by program
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—Acquirer-generated	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Authorization Advice/0120—System-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.**

---

## **DE 112—Encoding Scheme**

Mastercard organizes DE 112 into a group of encoded subelements. The following table illustrates the structure of DE 112.

<b>LLL      “VAR”—maximum length varies by program; refer to Data Representation previously for maximum length by program</b>						
3 bytes	3 bytes	3 bytes	variable by program	3 bytes	3 bytes	variable by program
Total Length	<b>First Subelement (SE) Data</b>			<b>Second Subelement (SE) Data</b>		
	SE ID	SE Length	SE Variable Length Data	SE ID	SE Length	SE Variable Length Data

<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 maximum allowed by program.
3	Subelement ID	In the range 000–099 000–069                  Defined universally for all programs and services.

---

<b>Number of Bytes</b>	<b>Attribute</b>	<b>Description</b>
		070–099      Defined for individual programs and services.
3	Subelement Length	Varies by program.
1...nnn	Subelement Variable Length Data	Contains valid values.

---

## DE 112—Authorization Platform Edits

The Authorization Platform will perform the following system edit to verify proper formatting of DE 112.

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
An Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or Reversal Request/0400 message contains DE 48 (Additional Data—Private Use), DE 108 (MoneySend Reference Data), or DE 112 (Additional Data [National Use]) with subelements that have incorrect length and/or incorrect format (Data Representations), or have multiple instances of the same subelement (when not permitted) within the same data element.	<p>Rejects the message and forwards the acquirer an Authorization Request Response/0110, Authorization Advice Response/0130, or Reversal Request Response/0410 message where DE 44 is 6 positions for subelement format errors:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Message format error)</li> <li>• DE 44 (Additional Response Data) = 0480nn, or 1080nn, or 1120nn (where nn is the subelement number)</li> </ul> <p>(DE 44 is three positions for Dual Message System (Authorization) if no subelements are present, for example, for DE 22 format error: DE 44 = 022)</p>

---

Examples:

- When an edit error occurs on DE 48, the DE 44 data will be populated as these examples below:
  - Error on DE 48 subelement 42, subfield 1: 048042 (no subfield information is provided)
  - Error on DE 48 subelement 61: 048061
- DE 48 TCC format error will be responded with DE 44 = 048000.

For non-DE 48/DE 108/DE 112 format errors, DE 44 will only have DE info and no subelement information. For example, the format error in DE 22 will have DE 44 as 022 for non-DE48/108/112 data elements.

## All Regions—Installment Payment Transactions

Following are the technical specifications for Authorization/01xx messages for the global Mastercard Installment Payment Service. Refer to the *Mastercard Installment Payment Service User Guide* for additional details.

### **Subelement 21—Installment Payment Data 1**

Subelement 21 (Installment Payment Data 1) is used in the Authorization System for installment payment transactions.

#### **Attributes**

Subelement ID:	021
Data Representation:	an-3
Length Field:	3
Data Field:	Contents of positions 1–3
Subfields:	N/A
Justification:	Right with leading zeros

#### **Usage**

Following is the usage of subelement 021 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	O	•	C
Reversal Request/0400	O	•	O
Reversal Request Response/0410	O	•	O

#### **Values**

Position	Attribute	Description
1–2	n-2	<p>Installment Type</p> <p>Contains the type of installment. Valid values include:</p> <ul style="list-style-type: none"> <li>• 20 = Issuer-Financed</li> <li>• 21 = Merchant-Financed</li> <li>• 22 = Acquirer-Financed</li> <li>• 23 = Co-branded Merchant Financed</li> <li>• 24 = Issuer Merchant Co-Financed</li> </ul>

---

3	a-1	Payment Options  Payment options provided by issuer. Valid values include: <ul style="list-style-type: none"><li>• I (Pay in Installments Only)</li><li>• F (Pay in Full Only)</li><li>• B (Pay in Full or Pay in Installments)</li></ul>
---	-----	---

---

### **Subelement 22—Installment Payment Data 2**

Subelement 22 (Installment Payment Data 2) is used in the Authorization System for installment payment transactions.

---

#### **Attributes**

---

Subelement ID: 022

Data Representation: ns...720; LLLVAR

The “LLL” length field of LLLVAR must be an integral multiple of 12, not to exceed 720.

Length Field: 3

Data Field: Contents of subfields 1–7

Subfields: 7

Justification: See subfields

---

#### **Usage**

---

Following is the usage of subelement 022 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	O	•	C
Reversal Request/0400	O	•	O
Reversal Request Response/0410	O	•	O

---

#### **Values**

---

See subfields

---

#### **Application Notes**

---

An “occurrence” is defined as one set of the seven subfields in subelement 022. Depending on the conditions of the message, subelement 022 can be sent by the acquirer, by the issuer, or by Mastercard.

---

### **Subfield 1—Number of Installments**

DE 112, subelement 022, subfield 1 (Number of Installments) contains the number of installment payments provided by the issuer and selected by the cardholder.

---

#### **Attributes**

Data Representation	n-2
Data Field	Contents of positions 1–2
Justification	Right with leading zeros

---

#### **Values**

Valid values are 02–99

---

### **Subfield 2—Interest Rate**

DE 112, subelement 022, subfield 2 (Interest Rate) contains the rate (two decimal places) that the issuer assesses the cardholder for the installment payment.

---

#### **Attributes**

Data Representation	ns-5
Data Field	Contents of positions 3–7
Justification	Right with leading zeros

---

#### **Values**

Will be populated as spaces if interest rate is not required to be displayed in the terminal.

---

### **Subfield 3—Installment Fee**

DE 112, subelement 022, subfield 3 (Installment Fee) contains the fee amount in cardholder billing currency that the issuer assesses the cardholder for the installment payments.

---

#### **Attributes**

Data Representation	ns-12
Data Field	Contents of positions 8–19
Justification	Right with leading zeros

---

#### **Values**

Will be populated as spaces if installment fee is not required to be displayed in the terminal.

---

### **Subfield 4—Annual Percentage Rate**

DE 112, subelement 022, subfield 4 (Annual Percentage Rate [APR]) contains the rate (two decimal places) that the issuer charges the cardholder for the installment payment.

---

**Attributes**

Data Representation	ns-5
Data Field	Contents of positions 20–24
Justification	Right with leading zeros

**Values**

Will be populated as spaces if Annual Percentage Rate is not required to be displayed in the terminal.

---

**Subfield 5—First Installment Amount**

DE 112, subelement 022, subfield 5 (First Installment Amount) contains the amount of the first installment in cardholder billing currency that the issuer will charge the cardholder for the installment payments.

---

**Attributes**

Data Representation	ns-12
Data Field	Contents of positions 25–36
Justification	Right with leading zeros

**Values**

Default is all spaces

---

**Subfield 6—Subsequent Installment Amount**

DE 112, subelement 022, subfield 6 (Subsequent Installment Amount) contains the amount of the subsequent installments in cardholder billing currency that the issuer will charge the cardholder for the installment payments.

---

**Attributes**

Data Representation	ns-12
Data Field	Contents of positions 37–48
Justification	Right with leading zeros

**Values**

Default is all spaces

---

**Subfield 7—Total Amount Due**

DE 112, subelement 022, subfield 7 (Total Amount Due) contains the total amount due in cardholder billing currency that the issuer charges the cardholder for the installment payments.

**Attributes**

Data Representation	ns-12
Data Field	Contents of positions 49–60
Justification	Right with leading zeros

**Values**

Default is all spaces

**Subelement 23—Installment Payment Data 3**

Subelement 23 (Installment Payment Data 3) is used in the Authorization System for installment payment transactions.

**Attributes**

Subelement ID:	023
Data Representation:	ns-38
Length Field:	3
Data Field:	Contents of positions 1–38
Subfields:	N/A
Justification:	Right with leading zeros

**Usage**

Following is the usage of subelement 023 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	•	X	C
Authorization Request Response/0110	C	•	C
Reversal Request/0400	O	•	O
Reversal Request Response/0410	O	•	O

**Values**

Position	Description
1–2	Minimum Number of Installments—Contains the number of installment payments provided by the issuer and selected by the cardholder. Valid values are 02–99.
3–4	Maximum number of installments—Contains the number of installment payments provided by the issuer and selected by the cardholder. Valid values are 02–99.

---

5–9	Interest Rate—Contains the interest rate (2 decimal) that the issuer charges the cardholder for the installment payments. Will be populated as spaces if Interest Rate is not required to be displayed in the terminal.
10–21	Installment Fee—Contains the fee amount that the issuer charges the cardholder for the installment payments in cardholder billing currency. Will be populated as spaces if Installment Fee is not required to be displayed in the terminal. Default is all zeros.
22–26	Annual Percentage Rate (APR)—Contains the annual percentage rate (2 decimal) that the issuer charges the cardholder for the installment payment. Will be populated as spaces if Annual Percentage Rate is not required to be displayed in the terminal.
27–38	Total Amount Due—Contains the total amount due in cardholder billing currency that the issuer charges the cardholder for the installment payment.

---

### **Alternate Processing**

Installment payments are not eligible for alternate processing (Stand-In System or X-Code System). When an issuer is not available, or offline, the Installment Payment transactions will be declined using the Authorization Request Response/0110 message containing DE 39 (Response Code), value 91 (Authorization System or issuer system inoperative).

### **Brazil—Payment Transactions**

Following are the technical specifications for Authorization/01xx messages for Brazil payment transactions within Brazil.

#### **Subelement 012—Brazil Commercial and Financing Data**

DE 112, subelement 012 (Brazil Commercial and Financing Data) contains additional data to support financing data provided by the acquirer, merchant, or issuer.

**NOTE: For data requirements for Brazil intracountry transactions using the Mastercard BNDES card, refer to the section that follows. The following table applies to non-BNDES transactions only.**

---

#### **Attributes**

---

Subelement ID:	012
Data Representation:	ans-170
Length Field:	3
Data Field:	Contents of positions 1–170
Subfields:	N/A

---

---

Justification:	N/A		
<b>Values</b>			
Field Name/ Positions	Type	Size	Comment
Financing Type (Positions 1–20)	Alpha	20	Type of loan operation, agreed between Merchant and issuer. Examples: AGRO-CUSTEIO, AGRO-INVEST, FINAME, CBN.
Buyer ID Type (Position 21)	Alpha	1	Possible values F or J:  F = pessoa Física (person/consumer)  J = pessoa Jurídica (company/commercial)
Buyer ID (Positions 22–35)	Numeric	14	Merchant to fill in with cardholder's CPF (Cadastro de Pessoa Física, a registration number provided by the Brazil government to all persons living in Brazil) or company's CNPJ (Cadastro Nacional da Pessoa Jurídica, registration number provided by the Brazil government to all merchants) number or issuers to supply with company's CNPJ number.
Buyer Phone Number (Positions 36–46)	Numeric	11	Merchant to fill in with buyer phone number.
Purchase Identification (Positions 47–66)	Alphanumeric	20	Invoice data or purchase request data, depending on agreement between merchant and issuer.
Installments Cycle (Positions 67–68)	Numeric	2	Different amortization types than monthly. For future use, it does not affect transaction clearing and settlement.
Interest Rate (Positions 69–86)	Numeric	18 (12.6)	Interest rate on loan. For future use.
Grace Period (Positions 87–89)	Numeric	3	Number of amortization cycles to wait before charging the installments. For future use, it does not affect transaction clearing and settlement.
Grace Period Cycle (Positions 90–92)	Numeric	3	Allow different grace period types than monthly. For future use, it does not affect transaction clearing and settlement.
Grace Period Interest Rate (Positions 93–110)	Numeric	18 (12.6)	Interest rate on grace period. For future use, it does not affect transaction clearing and settlement.
Reference Field 1 (Positions 111–130)	Numeric	20	Acquirer to populate with merchant's CNPJ number.

---

Reference Field 2 (Positions 131–150)	Alpha	20	Data exchange between merchant and issuer, to identify the transaction.
Reference Field 3 (Positions 151–170)	Alpha	20	Data exchange between merchant and issuer, to identify the transaction.
Filler Data (Positions 171–227)	Alphanumeric	57	Reserved for future Brazil domestic enhancements.

---

### **Mastercard Brazil BNDES Card Data Requirements**

Mastercard has enhanced the Mastercard Brazilian Development Bank (BNDES) Card to increase card issuance and usage in Brazil and support alternative financing options for small and medium-sized businesses.

Mastercard supports the presence of additional data fields for Brazil intracountry transactions submitted with product code MLD (Mastercard Distribution Card). This addition meets BNDES requirements, in terms of addendum data processed and sent by the BNDES generic module, through the acquirers.

The Mastercard BNDES Card is a solution to access a credit line with subsidized rates by BNDES to finance investments for micro-, small-, and medium-sized businesses established in Brazil.

This product is developed for Brazil domestic use only and transactions are sent to the Mastercard Network using the MLD (Mastercard Distribution Card) product code with a specific promotion code (BNDES1) in all transactions. These are issuer-financed installment (up to 48 installments) transactions, made exclusively through the BNDES Operations Portal.

BNDES has enhanced its Operations Portal's Generic Module, which requires acquirers to send additional data through the Mastercard Network.

**NOTE: All Brazil domestic transactions using the Mastercard BNDES card must contain DE 63 (Network Data), subfield 1 (Financial Network Code), value MLD (Mastercard Distribution Card) in the authorization message. The specific promotion code value BNDES1 must be included in DE 48 (Additional Data—Private Use), subelement 95 (Mastercard Promotion Code).**

In issuer-financed installment billing, the acquirer submits a single clearing record for the full transaction amount. The issuer then bills the cardholder for the installments in accordance with the terms agreed by the cardholder at the point of sale.

**NOTE: A customer's CNPJ number is the registration number provided by the Brazil government to all merchants.**

DE 112, subelement 012 (Brazil Commercial and Financing Data) contains additional data to support Brazil intracountry, consumer credit transactions submitted with value MLD (Mastercard Distribution Card) in DE 63 (Network Data), subfield 1 (Financial Network Code).

---

For Brazil intracountry transactions using the Mastercard BNDES card, the following data must be included.

---

#### **Attributes**

---

Subelement ID:	012
Data Representation:	ans-227
Length Field:	3
Data Field:	Contents of positions 1–227
Subfields:	N/A
Justification:	N/A

---

#### **Values**

---

<b>Data Element</b>	<b>Subelement</b>	<b>Positions</b>	<b>Value</b>
DE 112 (Additional Data [National Use])	Subelement 012 (Brazil Commercial and Financing Data)	Positions 1–20 (Financing Type)	CBN
		Position 21 (Buyer ID Type)	J
		Positions 22–35 (Buyer ID)	CNPJ number (Buyer Company Tax ID)
		Positions 36–110	Spaces
		Positions 111–130 (Reference Field 1)	CNPJ number (Merchant Brazilian Tax ID)
		Positions 131–227	Spaces

---

#### **Subelement 013—Crediário First Simulation**

DE 112 (Additional Data [National Use]), subelement 013 contains the issuer's payment conditions for the first Crediário simulation.

---

#### **Attributes**

---

Subelement ID:	013
Data Representation:	n-131
Length Field:	3
Data Field:	Contents of positions 1–131
Subfields:	N/A

---

---

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

---

### Usage

Following is the usage of subelement 013 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

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

---

### Values

Field Name/ Positions	Type	Size	Comment
Installment Plan Type (Positions 1–2)	Numeric	2	Identifies whether this is an issuer, a merchant, or a Crediaro financed installment plan.  Value 25 = Crediaro
Total Number of Installments (Positions 3–4)	Numeric	2	Number of installments the cardholder chose to pay.  From 02–99
Installment Amount (Positions 5–16)	Numeric	12	Value that the cardholder is going to pay per month. Parcelas (or installment) amount issuer calculates, including calculated interest; two decimal places.
Total Amount (Positions 17–28)	Numeric	12	Total Installment Amount (Monthly installment amount multiplied by the Number of Installments).  Transaction total amount issuer calculates, including calculated interest; two decimal places.
Monthly Interest Rate (Positions 29– 32)	Numeric	4	Interest Rates the Issuer calculates and charges per month; two decimal places.
Annual Interest Rate (Positions 33–37)	Numeric	5	Interest Rates the issuer calculates and charges per year; two decimal places.

---

<b>Values</b>			
Monthly Total Effective Cost (CET) (Positions 38–49)	Numeric	12	Total amount charged monthly to cardholder including the payments, interest, fees, insurance, and other amounts; two decimal places.
% Total Effective Cost (Positions 50– 61)	Numeric	12	Total Effective Cost, expressed as a percentage; two decimal places.
Date of first installment (Positions 62–67)	Numeric	6	Date of the first installment payment in yymmdd (year, month, day) format.
Taxes (Positions 68– 74)	Numeric	7	All taxes, if applicable, that the cardholder is paying, including IOF; two decimal places.
% Taxes of Total Amount (Positions 75–78)	Numeric	4	Percentage of the whole purchase price that the taxes represent.
Fee (Positions 79–85)	Numeric	7	All fees, if applicable, that the cardholder is paying; two decimal places.
% Fee of Total Amount (Positions 86–89)	Numeric	4	Percentage of the whole purchase price that the fees represent.
Insurance (Positions 90–96)	Numeric	7	Any insurance, if applicable, that the cardholder is paying; two decimal places.
% Insurance of Total Amount (Positions 97–100)	Numeric	4	Percentage of the whole purchase price that the insurance represents.
Other (Positions 101–107)	Numeric	7	Any other added values, if applicable, that the cardholder is paying; two decimal places.
% Other of Total Amount (Positions 108–111)	Numeric	4	Percentage of the whole purchase price that any other added values represent.
Total Amount to Merchant (Positions 112–123)	Numeric	12	Total amount that will be paid to the merchant (purchase amount); two decimal places.
% Amount to Merchant of Total Amount (Positions 124–127)	Numeric	4	Percentage of the total amount that will be paid to the merchant.

---

---

### Values

---

Reserved for Future Use (Positions 128–131)	Numeric	4
---	---------	---

---

---

### Application Notes

---

This subelement should be provided to indicate the merchant terminal's capabilities in supporting the first option for the Crediário installment program and services.

Information not populated or optional to a specific field should be zero-filled.

---

### Subelement 014—Crediário Second Simulation

DE 112 (Additional Data [National Use]), subelement 014 contains the issuer's payment conditions for the second Crediário simulation.

---

### Attributes

---

Subelement ID:	014
Data Representation:	n-131
Length Field:	3
Data Field:	Contents of positions 1–131
Subfields:	N/A
Justification:	N/A

---

---

### Usage

---

Following is the usage of subelement 014 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

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

---

<b>Values</b>			
<b>Field Name/ Positions</b>	<b>Type</b>	<b>Size</b>	<b>Comment</b>
Installment Plan Type (Positions 1–2)	Numeric	2	Identifies whether this is an issuer, a merchant, or a Crediaro financed installment plan.  Value 25 = Crediaro
Total Number of Installments (Positions 3–4)	Numeric	2	Number of installments the cardholder chose to pay.  From 02–99
Installment Amount (Positions 5–16)	Numeric	12	Value that the cardholder is going to pay per month. Parcelas (or installment) amount issuer calculates, including calculated interest; two decimal places.
Total Amount (Positions 17–28)	Numeric	12	Total Installment Amount (Monthly installment amount multiplied by the Number of Installments).  Transaction total amount issuer calculates, including calculated interest; two decimal places.
Monthly Interest Rate (Positions 29– 32)	Numeric	4	Interest Rates the Issuer calculates and charges per month; two decimal places.
Annual Interest Rate (Positions 33–37)	Numeric	5	Interest Rates the issuer calculates and charges per year; two decimal places.
Monthly Total Effective Cost (CET) (Positions 38–49)	Numeric	12	Total amount charged monthly to cardholder including the payments, interest, fees, insurance, and other amounts; two decimal places.
% Total Effective Cost (Positions 50– 61)	Numeric	12	Total Effective Cost, expressed as a percentage; two decimal places.
Date of first installment (Positions 62–67)	Numeric	6	Date of the first installment payment in yymmdd (year, month, day) format.
Taxes (Positions 68– 74)	Numeric	7	All taxes, if applicable, that the cardholder is paying, including IOF; two decimal places.

---

<b>Values</b>			
% Taxes of Total Amount (Positions 75–78)	Numeric	4	Percentage of the whole purchase price that the taxes represent.
Fee (Positions 79–85)	Numeric	7	All fees, if applicable, that the cardholder is paying; two decimal places.
% Fee of Total Amount (Positions 86–89)	Numeric	4	Percentage of the whole purchase price that the fees represent.
Insurance (Positions 90–96)	Numeric	7	Any insurance, if applicable, that the cardholder is paying; two decimal places.
% Insurance of Total Amount (Positions 97–100)	Numeric	4	Percentage of the whole purchase price that the insurance represents.
Other (Positions 101–107)	Numeric	7	Any other added values, if applicable, that the cardholder is paying; two decimal places.
% Other of Total Amount (Positions 108–111)	Numeric	4	Percentage of the whole purchase price that any other added values represent.
Total Amount to Merchant (Positions 112–123)	Numeric	12	Total amount that will be paid to the merchant (purchase amount); two decimal places.
% Amount to Merchant of Total Amount (Positions 124–127)	Numeric	4	Percentage of the total amount that will be paid to the merchant.
Reserved for Future Use (Positions 128–131)	Numeric	4	

---

### **Application Notes**

This subelement should be provided to indicate the merchant terminal's capabilities in supporting the second option for the Crediário installment program and services.

Information not populated or optional to a specific field should be zero-filled.

### **Subelement 015—Crediário Third Simulation**

DE 112 (Additional Data [National Use]), subelement 015 contains the issuer's payment conditions for the third Crediário simulation.

---

#### **Attributes**

---

Subelement ID:	015
Data Representation:	n-131
Length Field:	3
Data Field:	Contents of positions 1–131
Subfields:	N/A
Justification:	N/A

---

---

#### **Usage**

---

Following is the usage of subelement 015 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Authorization Request Response/0110	C	•	C
Authorization Advice/0120—Acquirer-generated	C	•	C

---

---

#### **Values**

---

<b>Field Name/ Positions</b>	<b>Type</b>	<b>Size</b>	<b>Comment</b>
Installment Plan Type (Positions 1–2)	Numeric	2	Identifies whether this is an issuer, a merchant, or a Crediario financed installment plan.  Value 25 = Crediario
Total Number of Installments (Positions 3–4)	Numeric	2	Number of installments the cardholder chose to pay.  From 02–99
Installment Amount (Positions 5–16)	Numeric	12	Value that the cardholder is going to pay per month. Parcelas (or installment) amount issuer calculates, including calculated interest; two decimal places.

---

---

<b>Values</b>			
Total Amount (Positions 17–28)	Numeric	12	Total Installment Amount (Monthly installment amount multiplied by the Number of Installments).  Transaction total amount issuer calculates, including calculated interest; two decimal places.
Monthly Interest Rate (Positions 29–32)	Numeric	4	Interest Rates the Issuer calculates and charges per month; two decimal places.
Annual Interest Rate (Positions 33–37)	Numeric	5	Interest Rates the issuer calculates and charges per year; two decimal places.
Monthly Total Effective Cost (CET) (Positions 38–49)	Numeric	12	Total amount charged monthly to cardholder including the payments, interest, fees, insurance, and other amounts; two decimal places.
% Total Effective Cost (Positions 50–61)	Numeric	12	Total Effective Cost, expressed as a percentage; two decimal places.
Date of first installment (Positions 62–67)	Numeric	6	Date of the first installment payment in yymmdd (year, month, day) format.
Taxes (Positions 68–74)	Numeric	7	All taxes, if applicable, that the cardholder is paying, including IOF; two decimal places.
% Taxes of Total Amount (Positions 75–78)	Numeric	4	Percentage of the whole purchase price that the taxes represent.
Fee (Positions 79–85)	Numeric	7	All fees, if applicable, that the cardholder is paying; two decimal places.
% Fee of Total Amount (Positions 86–89)	Numeric	4	Percentage of the whole purchase price that the fees represent.
Insurance (Positions 90–96)	Numeric	7	Any insurance, if applicable, that the cardholder is paying; two decimal places.
% Insurance of Total Amount (Positions 97–100)	Numeric	4	Percentage of the whole purchase price that the insurance represents.
Other (Positions 101–107)	Numeric	7	Any other added values, if applicable, that the cardholder is paying; two decimal places.

---

---

### Values

% Other of Total Amount (Positions 108–111)	Numeric	4	Percentage of the whole purchase price that any other added values represent.
Total Amount to Merchant (Positions 112–123)	Numeric	12	Total amount that will be paid to the merchant (purchase amount); two decimal places.
% Amount to Merchant of Total Amount (Positions 124–127)	Numeric	4	Percentage of the total amount that will be paid to the merchant.
Reserved for Future Use (Positions 128–131)	Numeric	4	

---

### Application Notes

This subelement should be provided to indicate the merchant terminal's capabilities in supporting the third option for the Crediário installment program and services.

Information not populated or optional to a specific field should be zero-filled.

---

### Subelement 018—Brazil Post-Dated Transaction Data

DE 112, subelement 018 (Brazil Post-Dated Transaction Data) contains additional data to support post-dated transaction data provided by the acquirer.

---

### Attributes

Subelement ID	018
Data Representation	ans-39
Length of Field	3
Data Field	Contents of positions 1–39
Subfields	N/A
Justification	N/A

---

### Usage

---

Following is the usage of subelement 018 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:			
Authorization Request/0100		C	• C
Authorization Request Response/0110		CE	• C
Authorization Advice/0120		C	• C
Reversal Request/0400		C	• C
<b>Values</b>			
Field Name	Positions	Attribute	Field Description
Service Code	1–2	n-2	<p>Type of post-dated transaction.</p> <p>Valid Values:</p> <ul style="list-style-type: none"> <li>• 30 = Post-Dated with Guarantee</li> <li>• 31 = Post-Dated without Guarantee</li> </ul> <p>Must be present and equal to 30 or 31 when DE 61, subfield 7 = 5.</p>
Number of Installments	3	n-1	<p>Valid Values:</p> <p>If present, value will always be 1.</p>
Guarantee	4	a-1	<p>Valid Values:</p> <ul style="list-style-type: none"> <li>• Y = Yes</li> <li>• N = No</li> </ul>
Guarantee Amount	5–12	n-8	<p>Amount of guarantee to be settled; assumed to be a credit to the issuer.</p> <p>Valid Values:</p> <p>Must be 00000000 if Position 1–2 = 31 (Post-Dated without Guarantee).</p>
Post Settlement Date	13–18	n-6	<p>Proposed settlement date (expected date for completion message arrival).</p> <p>Format: MMDDYY</p>
Original Mastercard Settlement Date	19–24	n-6	<p>Contains zeros on authorization message.</p> <p>Format: MMDDYY</p>

---

---

Original Banknet Reference Number	25–33	n-9	Original Banknet reference number assigned by Banknet to original authorization request; contains zeros on authorization request/0100 message.
Authorization Code	34–39	n-6	Contains the online authorization code provided by the issuer on the original authorization response.

---

### Authorization Platform Edits

The Authorization Platform performs the following system edits on DE 112, subelement 018 (Brazil Post-Dated Transaction Data), on authorization messages submitted for Post-Dated transactions in Brazil.

#### Post-Dated Transactions

---

WHEN...	THEN the Authorization Platform...
The Authorization Request/0100 message contains DE 112 (Additional Data—National Use), subelement 018 (Brazil Post-Dated Transaction Data) and the issuer account range is not set up for the Post-Dated Payment service or the issuer and acquirer country codes are not the same	Will reject the transaction with <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 57 (Transaction not permitted to issuer/cardholder)</li> </ul>
The Authorization Request/0100 message contains DE 112 (Additional Data—National Use), subelement 018 (Brazil Post-Dated Transaction Data), subfield 1 (Service Code) contains value 30 or 31 and DE 61 (Point of Service Data), subfield 7 (POS Transaction Status) does not contain value 5 (Time Based Payment Authorization Request)	Will reject the transaction with <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 061 (indicating the data element in error)</li> </ul>
The Authorization Request/0100 message contains DE 61 (Point of Service Data), subfield 7 (POS Transaction Status) does not contain value 5 (Time Based Payment Authorization Request) and DE 112 (Additional Data—National Use), subelement 018 (Brazil Post-Dated Transaction Data), subfield 1 (Service Code) does not contain value 30 or 31	Will reject the transaction with <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 112018 (indicating the data element in error)</li> </ul>

---

## Alternate Processing

Post-Dated transactions are not eligible for Stand-In or X-Code processing. If an issuer is not available, or offline, the transactions will be declined using the Authorization Request Response/0110 message containing DE 39 (Response Code), value 91 (Authorization Platform or issuer system inoperative).

### Subelement 019—Original Purchase Amount

DE 112 (Additional Data [National Use]), subelement 019 contains the amount (two decimal places) that the cardholder wants to finance. Subelement 019 is to be used only for Crediário Account Status Inquiry (ASI) transactions.

#### Attributes

Subelement ID:	019
Data Representation:	n-12
Length Field:	3
Data Field:	Contents of positions 1–12
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of subelement 019 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

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

#### Values

This subelement must contain valid numeric data.

---

### Application Notes

---

This subelement should be provided to indicate the merchant terminal's capabilities for displaying the original purchase amount for the Crediário installment program.

Information not populated or optional to a specific field should be zero-filled.

---

## Brazil—Merchant Fraud Scoring Data

Following are the technical specifications for Authorization Request/0100 and Authorization Request Response/0110 messages that contain merchant fraud scoring data for card-not-present (CNP) transactions from acquirers in Brazil.

### Subelement 028—Merchant Fraud Score Data

DE 112, subelement 028 (Merchant Fraud Score Data) should be used by acquirers in Brazil to send merchant fraud score data.

---

#### Attributes

---

Subelement ID 028

---

Data Representation: ns-4

---

Length Field: 3

---

Data Field: Contents of positions 1–4

---

Subfields: N/A

---

Justification: see values

---

#### Usage

---

Following is the usage of subelement 028 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	O	•	C
Authorization Request Response/0110	•	X	C

#### Values

---

Acquirers may perform merchant fraud scoring either by themselves or through payment gateways. Acquirers in Brazil can forward the merchant fraud scoring information to issuers using this subelement. Issuers can use this data to know that merchant fraud scoring is done by the acquirer and use the data to make approval decision for CNP transaction.

Merchant Fraud Score data provided by acquirers in Brazil should be in the range -999 to +999. Merchant fraud score should be right justified with leading zeros if the value is less than three digits.

---

---

### Application Notes

---

Issuers are not expected to echo DE 112, subelement 028 (Merchant Fraud Score Data) in the Authorization Request Response/0110 message. Mastercard will echo DE 112, subelement 028 (Merchant Fraud Score Data) from Authorization Request/0100 to the acquirers in the Authorization Request Response/0110 message.

---

## Chile—Payment Transactions

Following are the technical specifications for Authorization/01xx messages for Chile payment transactions within Chile.

### Subelement 010—Installment Payment Data

DE 112, Chile, subelement 010 is used in the Authorization Platform for installment payment transactions within Chile.

Subelement 010 must be present if DE 48 (Additional Data—Private Use), subelement 95 (Mastercard Promotion Code) contains the value CHLCTA.

Subelement 010 contains the following subfields used in Chile Domestic Switch (ChIDS) processing. For details on data requirements for these subfields refer to the *Chile Domestic Switch Implementation Guide*.

- Subfield 1—Total Purchase Amount
- Subfield 2—Number of Installments
- Subfield 3—Installment Type
- Subfield 4—Installment Amount
- Subfield 5—Transaction Interest Rate
- Subfield 6—Deferred Period
- Subfield 7—Deferred Period 1: Installment Amount
- Subfield 8—Deferred Period 1: Interest Rate
- Subfield 9—Deferred Period 1: Period Identifier
- Subfield 10—Deferred Period 2 Installment Amount
- Subfield 11—Deferred Period 2 Interest Rate
- Subfield 12—Deferred Period 2 Period Identifier
- Subfield 13—Deferred Period 3 Installment Amount
- Subfield 14—Deferred Period 3 Interest Rate
- Subfield 15—Deferred Period 3 Period Identifier
- Subfield 16—Simulation Flag
- Subfield 17—Grace Period Flag
- Subfield 18—Grace Period
- Subfield 19—Deferred Period Simulation Flag
- Subfield 20—Reserved for Annual Equivalent Charge Rate (CAE)

## Colombia—Domestic Transactions

Following are the technical specifications for Authorization/01xx messages for Colombia domestic transactions.

### Subelement 035—Issuer Fee Inquiry Indicator

DE 112, Colombia, subelement 035 (Issuer Fee Inquiry Indicator) is populated by the acquirer and passed to the issuer to indicate that a transaction qualifies as an Issuer Fee Inquiry.

#### Attributes

Subelement ID:	035
Data Representation:	n-2
Length Field:	n-3
Data Field:	Contents of positions 1–2
Subfields:	N/A
Justification:	N/A

#### Usage

Following is the usage of subelement 035 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

Message	Org	Sys	Dst
Authorization Request/0100	C	•	C

Values	Description
01	Indicates Issuer Fee Inquiry Request

### Subelement 036—Issuer Fee Amount

DE 112, Colombia, subelement 036 (Issuer Fee Amount) is populated by the issuer with the fee amount that would be associated with the intended ATM cash withdrawal.

#### Attributes

Subelement ID:	036
Data Representation:	n-12
Length Field:	n-3

---

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

---

### Usage

Following is the usage of subelement 036 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

Message	Org	Sys	Dst
Authorization Request Response/0110	C	•	C

---

Values	Description
Valid numeric data	Ex: 000000000123

---

**NOTE: Amounts are expressed without a decimal separator. For currencies that support exponents, users and systems are responsible for placing the decimal separator appropriately. Currently only for use in Colombia, where currency exponent = 2.**

## Colombia—Payment Transactions

Following are the technical specifications for Authorization/01xx messages for Colombia payment transactions within Colombia.

### Subelement 010—Installment Payment Data

DE 112, Colombia, subelement 010 (Installment Payment Data) is used in the authorization platform for Colombia payment transactions.

Subelement 010 must be present if DE 48, subelement 95 (Mastercard Promotion Code) contains the value COLCTA.

---

Attributes	
Subelement ID:	010
Data Representation:	ans-2
Length Field:	3
Data Field:	Contents of positions 1–2
Subfields:	N/A

---

---

Justification: Left-justified with trailing spaces

---

Usage: Conditional

---

**Example Values**

---

XX = The number of installments (01–XX) Maximum number of installments accepted in Colombia varies from time to time (99 as maximum value allowed)

---

**Subelement 011—Customer ID**

DE 112, Colombia, subelement 011 (Customer ID) is the customer associated with a voice, card not present, or manual transaction.

---

Attributes

---

Subelement ID: 011

---

Data Representation: ans-11

---

Length Field: 3

---

Data Field: Contents of positions 1–11

---

Subfields: N/A

---

Justification: Left-justified with trailing spaces

---

Usage: Conditional

---

**Example Values**

---

Contains customer ID information.

---

**Cuotas—Payment Transactions**

Following are the technical specifications for Authorization/01xx messages 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

---

Data Representation: ans...4

---

Length Field: 3

---

Data Field: Contents of positions 1–4 where:

XX	=	positions 1–2
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
Data Representation:	ans...55
Length Field:	3
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.

---

### **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

---

Data Representation: an-4 (Authorization Request/0100)  
an-137 (Authorization Request Response/0110)

---

Length Field: 3

---

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
<b>Values</b>	
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
<b>Values</b>	
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 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

## **Europe Region and Philippines—Payment Transactions**

Following are the technical specifications for Authorization/01xx messages for the Europe Region and Philippines payment transactions.

### **Subelement 009—Installment Payment Data**

DE 112, subelement 009 (Installment Payment Data) is used in the Authorization System for installment payment transactions in Georgia and Philippines.

DE 112, subelement 009 only applies when DE 48 (Additional Data—Private Use), subelement 95 (Mastercard Promotion Code) contains the value HGMINS or PHINST.

**NOTE: Customers in the Europe region should refer to global release articles and the *Mastercard Installment Payment Service User Guide* for information about installment payment processing. Mastercard will no longer publish this information in articles specific to the Europe region as this service is now available globally. Refer to the previous section All Regions—Installment Payment Transactions.**

Attributes	
Subelement ID:	009
Data Representation:	n-33
Length Field:	3

---

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	C	•	C
Authorization Advice/0120—Issuer-generated	C	C	•
Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE

### **Values**

Installment type (positions 1– 2) Installment type contains a type of installment. Valid values include 20 (Issuer-financed), 21 (Merchant-financed), and 22 (Acquirer-financed).

Number of installments (positions 3–4)	Number of installments contains the number of installment payments selected by the cardholder. Valid values are 01–99.
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 in transaction currency.
Subsequent installment amount (positions 22–33)	Subsequent installment amount contains the amount of the subsequent installment in transaction currency.

**NOTE: DE 112 (Additional Data [National Use]), subelement 009 (Installment Payment Data) is a conditional echo in the Authorization Request Response/0110 message for Philippines installment payment transactions for finance type 21 (merchant-financed).**

### **Authorization Platform Edits**

The Authorization Platform performs the following edits on data element 112, subelement 009 (Installment Payment Data), on authorization messages submitted for installment payment transactions in Georgia.

---

WHEN...	THEN the Authorization Platform...
---------	------------------------------------

---

<p>DE 48 (Additional Data—Private Use), subelement 95 (Mastercard Promotion Code) contains the value HGMINs and DE 112 (Additional Data [National Use]), subelement 009 (Installment Payment Data) is not present in an Authorization Request/0100 message</p>	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 112009</li> </ul>
<p>DE 48, subelement 95 contains the value HGMINs and DE 112, subelement 009 is present in the Authorization Request/0100 message and DE 112, subelement 009 is not present back in the Authorization Request Response/0110 message</p>	<p>Sends the issuer an Authorization Negative Acknowledgement/0190 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 (Additional Response Data) = 112009 (indicating the data element in error)</li> </ul> <p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 91 (Authorization System or issuer system inoperative) or 05 (Do not honor)</li> </ul>

---

### **Subelement 020—Domestic Card Acceptor Tax ID**

Subelement 020 (Domestic Card Acceptor Tax ID) is used in the Croatia Authorization System for payment transactions.

---

Attributes		
Subelement ID:	020	
Data Representation:	ans-20; LLVAR	
Length Field:	3	
Data Field:	Contents of Positions 1–20	
Subfields:	N/A	
Justification:	Left with trailing spaces	

---

### **Usage**

Following is the usage of subelement 020 (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	•

---

Reversal Request/0400	C	•	C
Reversal Request Response/0410	CE	•	CE

#### **Values**

Values are assigned by the acquirer.

#### **Application Notes**

This field is required when installment transactions are submitted by participating acquirers in Croatia.

### **Greece—Payment Transactions**

Following are the technical specifications for Authorization/01xx messages for installment payment transactions in Greece.

#### **Subelement 006—Installment Payment Data**

DE 112, Greece, subelement 006 (Installment Payment Data) is used in the Authorization Platform for Greece payment transactions. It must be present in Authorization Request/0100 and Authorization Request Response/0110 messages when DE 48, subelement 95 (Mastercard Promotion Code) contains the value GREECE.

---

#### Attributes

Subelement ID:	006
Data Representation:	ans...10
Length Field:	3
Data Field:	Contents of positions 1–10
Subfields:	N/A
Justification:	N/A

---

#### **Values**

Greece payment transactions in the Authorization Request/0100 and Authorization Request Response/0110

Positions	Length	Description
1–2	2	Type of Credit <ul style="list-style-type: none"> <li>• 21 = Merchant Financed</li> </ul>
3–4	2	Number of Installments <ul style="list-style-type: none"> <li>• 01 to 99</li> </ul>

---

5–7	3	Grace Period Before First Payment in UZZ format where <ul style="list-style-type: none"> <li>• U indicates unit type               <ul style="list-style-type: none"> <li>– N = No grace period</li> <li>– D = Days</li> <li>– W = Weeks</li> <li>– M = Months</li> </ul> </li> <li>• ZZ indicates the number of days, weeks or months               <ul style="list-style-type: none"> <li>– 00 to 99</li> </ul> </li> </ul>
8–10	3	<p>Transaction Currency Code. Must be same value as provided in DE 49 (Currency Code, Transaction).</p> <p>This is the local currency of the acquirer or source location of the transaction. It specifies the currency used in Amount Transaction DE 4.</p> <ul style="list-style-type: none"> <li>• 978 = Euro (EUR)</li> </ul>

---

### **Subelement 008—Installment Payment Response Data**

DE 112, Greece, subelement 008 (Installment Payment Response Data) is used in the Authorization Platform for Greece payment transactions in the Authorization Request Response/0110.

---

#### Attributes

---

Subelement ID:	008
Data Representation:	ans...23
Length Field:	3
Data Field:	Contents of positions 1–23
Subfields:	N/A
Justification:	N/A

---

#### Values

---

Greece payment transactions in the Authorization Request Response/0110

Positions	Length	Description
1–12	12	Installment amount (with two decimal places) including any issuer-calculated interest, insurance, or other charges.
13–18	6	Due date of first installment (in DDMMYY format).

---

---

19–21	3	Financing Currency Code. This is the currency in which the issuer will finance the transaction.  It specifies the currency using in Installment Amount above. <ul style="list-style-type: none"><li>• 978 = Euro (EUR)</li></ul>
22–23	2	Payment Plan. Reserved for future use. Insert all zeros.

---

## Japan—Payment Transactions

Following are the technical specifications for Authorization/01xx messages for Japan National Data payment transactions within Japan.

### Subelement 030—Japan Domestic POS Data

Subelement 030 (Japan Domestic POS Data) is used in the Authorization System to provide data required by acquirers and issuers in Japan for intracountry processing.

---

<b>Attributes</b>			
Subelement ID:	030		
Data Representation:	ans-138		
Length Field:	3		
Data Field:	Contents of Positions 1–138		
Subfields:	N/A		
Justification:	Right with leading zeros		

---

### Usage

Following is the usage of subelement 030 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	O	•	C
Authorization Request Response/0110	CE	•	C
Reversal Request/0400	O	•	C
Reversal Request Response/0410	CE	•	C

---

Values	Positions	Format
Terminal ID	01–13	ans-13
JIS II/ISO	14–82	ans-69  If ISO track data is populated here it must be padded with trailing spaces.
Product Code	83–89	ans-7

---

---

Reserved for future use	90	ans-1 space filled
Acquirer Company Code	91–97	an-7
Issuer Company Code	98–104	an-7
Authorization Transmission Mode	105	n-1
	<ul style="list-style-type: none"> <li>• 1 = Memory</li> <li>• 2 = Online</li> </ul>	
Entry Indicator	106	n-1
	<ul style="list-style-type: none"> <li>• 1 = Back Stripe ISO</li> <li>• 2 = Front Stripe JIS II</li> <li>• 3 = Manual</li> <li>• 4 = N/A (Domestic Private Label)</li> <li>• 5 = IC Chip Data ISO</li> <li>• 6 = IC Chip Data JIS II</li> </ul>	For Reversal Request/0400 messages, if the card is read using the ISO Track (Entry Mode 1), then the track data must be placed in the field JIS II/ISO instead of DE 35 (Track 2 Data) as DE 35 is not present in reversal messages. Note that the ISO track data must be padded with trailing spaces when using the field JIS II/ISO due to its reduced length.
Authorization Type	107	n-1
	<ul style="list-style-type: none"> <li>• 1 = Normal</li> <li>• 2 = Authorization Reservations</li> <li>• 3 = Post-Approval Authorization</li> <li>• 4 = Card Validity Check</li> <li>• 5 = Reversal</li> <li>• 6 = Refund</li> <li>• 7 = Reversal of Authorization Reservation</li> <li>• 8 = Reversal of Post-Approval Authorization</li> </ul>	
Approval Number for Post-Approval Authorization	108–113	n-6
Sales Slip Number	114–118	n-5

---

---

Sales Slip Number for Reversal/ Refund	119–123	n-5
		Sales Slip Number for Reversal/ Refund is not required when DE 03 (Processing Code), subfield 1 (Cardholder Transaction Type Code) does not equal 20 (Refund/Correction) in an authorization request message. When required, and must be all zeros when a meaningful value is not available.
Tax Amount	124–130	n-7  Format: nnnnnnn
Local Transaction Date	131–138	n-8  Format: YYYYMMDD

---

### **Application Notes**

Because DE 112, subelement 030 contains unique data specific to acquirers and issuers in Japan, Mastercard does not enforce the use of DE 112, subelement 030.

If provided, Mastercard does not validate the contents of DE 112, subelement 030.

If provided, Mastercard will remove subelement 030 from the Authorization Request/0100, Authorization Request Response/0110, Reversal Request/0400, and Reversal Request Response/ 0410 messages when the acquirer or the issuer country code is not 392 (Japan).

---

### **Subelement 031—Japan Domestic Response Code**

Subelement 031 (Japan Domestic Response Code) is used in the Authorization System to provide data required by acquirers and issuers in Japan for intracountry processing.

---

#### **Attributes**

Subelement ID:	031
Data Representation:	ans-3
Length Field:	3
Data Field:	Contents of Positions 1–3
Subfields:	N/A
Justification:	Right with leading zeros

---

#### **Usage**

---

Following is the usage of subelement 031 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request Response/0110	O	•	C
Reversal Request Response/0410	O	•	C
Values	Positions		Format
Error Code	01–03		ans-3

#### **Application Notes**

---

If present, Mastercard will remove subelement 031 from the Authorization Request Response/0110 and Reversal Request Response/0410 messages when the acquirer or the issuer country code is not 392 (Japan).

---

### **Subelement 032—Japan Payment Options**

Subelement 032 (Japan Payment Options) is used in the Authorization System to provide data for domestic Japan installment payments. The term bonus used in this subelement and related subfields refers to a salary bonus. In Japan, there can be one or two salary bonuses paid per year.

---

#### **Attributes**

Subelement ID:	032
Data Representation:	n-36
Length Field:	3
Data Field:	Contents of subfields 1–8
Subfields:	8
Justification:	See “Subfields”

---

#### **Usage**

Following is the usage of subelement 032 (whether it is mandatory, conditional, optional, or system provided) in applicable messages:

	Org	Sys	Dst
Authorization Request/0100	O	•	C
Authorization Request Response/0110	CE	•	C
Reversal Request/0400	O	•	C
Reversal Request Response/0410	CE	•	C

---

#### **Values**

---

See “Subfields”

---

#### **Application Notes**

---

If subelement 032 is present then all subfields must also be present.

Mastercard provides subelement 032 to facilitate communication of data between the acquirer and issuer. Mastercard does not enforce edits to check the presence of any data. Transactions that do not include DE 112, subelement 032 data will not be rejected.

Mastercard will remove subelement 032 from the Authorization Request/0100, Authorization Request Response/0110, Reversal Request/0400, and Reversal Request Response/0410 messages when the acquirer or the issuer country code is not 392 (Japan).

---

### **Subfield 1—Payment Option Code**

DE 112, subelement 032, subfield 1 (Payment Option Code) indicates how the cardholder wants to pay for the transaction.

---

#### **Attributes**

---

Data Representation	n-2
Data Field	Contents of positions 1–2
Justification	Left

---

#### **Values**

---

10	Single Payment
21	Bonus Pay
22	Bonus Pay (with number of bonuses)
23	Bonus Pay (with bonus month)
24	Bonus Pay (with number of bonuses and bonus month)
31	Bonus Pay with Installments
32	Bonus Pay with Installments (with bonus amount)
33	Bonus Pay with Installments (with number of bonuses, bonus month)
34	Bonus Pay with Installments (with number of bonuses, bonus month, bonus amount)
61	Installments (Twice Pay/Three or More)
80	Revolving

---

#### **Application Notes**

---

This field is required and must contain one of the listed values.

---

---

### **Subfield 2—Bonuses Per Year**

DE 112, subelement 032, subfield 2 (Bonuses Per Year) indicates if the cardholder receives one or two bonuses per year.

---

#### **Attributes**

Data Representation	n-2
Data Field	Contents of positions 3–4
Justification	Right with leading zeros

---

#### **Values**

01	One bonus per year
02	Two bonuses per year
00	Not Applicable

---

#### **Application Notes**

This field must contain values 01 or 02 for Payment Option Codes 22, 24, 33, or 34; otherwise zero filled.

---

### **Subfield 3—First Bonus Month**

DE 112, subelement 032, subfield 3 (First Bonus Month) identifies month of the next bonus payment received by the cardholder following the purchase date.

---

#### **Attributes**

Data Representation	n-2
Data Field	Contents of positions 5–6
Justification	Right with leading zeros

---

#### **Values**

01–12	Month
00	Not Applicable

---

#### **Application Notes**

This field must contain a value 01 to 12 for Payment Option Codes 23, 24, 33, or 34; otherwise zero filled.

---

### **Subfield 4—First Bonus Amount**

DE 112, subelement 032, subfield 4 (First Bonus Amount) indicates the amount of first bonus payment. The currency is the same as the transaction currency.

---

#### **Attributes**

Data Representation	n-12
Data Field	Contents of positions 7–18
Justification	Right with leading zeros
<b>Values</b>	
000000000000–999999999999	Amount of first bonus payment. The currency is the same as the transaction currency. Default is all zeros.
<b>Application Notes</b>	
This field must contain a Bonus Amount for Payment Option Codes 32 and 34; otherwise zero filled.	

### **Subfield 5—Second Bonus Month**

DE 112, subelement 032, subfield 5 (Second Bonus Month) identifies the month of the second bonus payment received by the cardholder following the purchase date.

<b>Attributes</b>	
Data Representation	n-2
Data Field	Contents of positions 19–20
Justification	Right with leading zeros
<b>Values</b>	
01–12	Month
00	Not Applicable
<b>Application Notes</b>	
This field must contain a value of 01 to 12 when Payment Option Code is 24, 33, or 34 and subfield 2 (Bonuses Per Year) indicates 2; otherwise it should be zero filled.	

### **Subfield 6—Second Bonus Amount**

DE 112, subelement 032, subfield 6 (Second Bonus Amount) indicates the amount of second bonus payment. The currency is the same as the transaction currency.

<b>Attributes</b>	
Data Representation	n-12
Data Field	Contents of positions 21–32
Justification	Right with leading zeros
<b>Values</b>	
000000000000–999999999999	Amount of second bonus payment. The currency is the same as the transaction currency. Default is all zeros.

---

### Application Notes

---

This field should contain a Bonus Amount when Payment Option Code is 34 and subfield 2 (Bonuses Per Year) indicates 2; otherwise it should be zero filled.

---

### Subfield 7—Total Number of Installments

DE 112, subelement 032, subfield 7 (Total Number of Installments) indicates the number of installments.

---

#### Attributes

---

Data Representation	n-2
Data Field	Contents of positions 33–34
Justification	Right with leading zeros

---

#### Values

---

01–99	Number of installments
00	Not Applicable

---

#### Application Notes

---

This field must contain a value of 01 to 99 when Payment Option Code is 31, 32, 33, 34, or 61; otherwise zero filled.

---

### Subfield 8—First Installment Month

DE 112, subelement 032, subfield 8 (First Installment Month) indicates the month in which the first installment will be paid.

---

#### Attributes

---

Data Representation	n-2
Data Field	Contents of positions 35–36
Justification	Right with leading zeros

---

#### Values

---

01–12	Month
00	Not Applicable

---

#### Application Notes

---

This field must contain a value of 01 to 12 when Payment Option Code is 31, 32, 33, 34, or 61; otherwise zero filled.

---

## Mexcta—Payment Transactions

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
Data Representation:	n-11
Length Field:	3
Data Field:	Contents of positions 1–11
Subfields:	N/A
Justification:	Right-justified

#### Values

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
Data Representation:	ans-20
Length Field:	3
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

---

Data Representation: ans-4

---

Length Field: 3

---

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

---

Data Representation: ans-9

---

Length Field: 3

---

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:

- 00 (No promotion)
- 03 (Without interest for the cardholder)
- 05 (With interest for the cardholder)
- 07 (Buy today, pay later)

---

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>
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
Data Representation:	ans-23
Length Field:	023
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 484 (Mexican Peso)
Payment Plan (positions 22–23)	Reserved for future use. Insert all zeros.

---

## Netherlands—IBAN—Account Inquiry

Following are the technical specifications for Account Status Inquiry (ASI) Authorization Request Response/0110 messages that enable customers in the Netherlands to share customer data such as the International Bank Account Number (IBAN).

### Subelement 037—Additional Cardholder Information

DE 112 (Additional Data [National Use]), subelement 037 contains cardholder information to help track debit card activity.

---

<b>Attribute</b>	<b>Value</b>
Subelement ID	037
	Additional Cardholder Information
Subelement Length	003
Data Representation	an...076, LLLVAR
Data Field	Contents of subfields 1-2
Number of Subfields	2
	Subfield 01—Primary Cardholder Identifier
	Subfield 02—Secondary Cardholder Identifier

---

### Usage

Following is the usage of subelement 37 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

---

<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
----------------	------------	------------	------------

---

---

### Usage

---

Authorization Request Response/0110

C

•

C

---

### Values

---

See "Subfields"

---

### Application Notes

---

Issuers will add DE 112, SE 037 as part of the ASI Authorization Request Response/0110 messages for the Netherlands and add the IBAN and the four-digit card number on the respective subfields. This will be done only after successfully validating that the ASI Authorization Request/0100 message is received by the issuer is a domestic transit ASI request.

---

### Subfield 01—Primary Cardholder Identifier

DE 112, subelement 037 (Additional Cardholder Information), subfield 01 (Primary Cardholder Identifier) is used by customers to share the unique cardholder identifier.

Attribute		
Subfield ID	01	Primary Cardholder Identifier
Subfield Length	2	
Data Representation	an...34; LLVAR	
Justification	Left	

---

### Values

---

For Netherlands intracountry transit activity issuers will populate this subfield with the 18-digit International Bank Account Number (IBAN) within the ASI Authorization Request Response/0110 message to the acquirer.

Issuers will populate this field only upon successful validation of ASI Authorization Request/0100 message and then respond back with an ASI Authorization Request Response/0110 message with this additional DE 112, SE 037, SF 01.

### Example

The sample below is an example of an International Bank Account Number (IBAN) for the Netherlands:

IBAN	NL91ABAB0XX71XX300
ISO Country Code	NL (The Netherlands)
IBAN Check Digits	91
BBAN	ABAB0XX71XX300
Bank Identifier	ABAB
Account Number	0XX71XX300

The IBAN consists of a two-letter country code, two check digits and a Basic Bank Account Number (BBAN). A BBAN includes information about the domestic bank and account number. The IBAN print format adds one space after every four characters whereas the electronic format contains no spaces.

### Subfield 02—Secondary Cardholder Identifier

DE 112, subelement 037 (Additional Cardholder Information), subfield 02 (Secondary Cardholder Identifier) is used by customers to share the unique cardholder identifier.

Attribute		
Subfield ID	02	Secondary Cardholder Identifier
Subfield Length	2	
Data Representation	an...34; LLVAR	
Justification	Left	

### Values

For Netherlands intracountry transit-related ASI Authorization Request Response/0110 messages will be populated with the four-digit card number information of the cardholder, provided by the issuer to the acquirer, which is then provided to the merchant.

### 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
Data Representation:	ans-4
Length Field	3
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
25	= Crediário
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
25	= Crediário
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 Representation:	ans...32 if format 1 used; ans...4 if format 2 used
Length Field:	3
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

---

#### **Subelement 016—Additional Installment Payment Response Data**

DE 112, Parcelas, subelement 016 (Additional Installment Payment Response Data) is used in the Authorization Platform and Parcelas payment transactions.

---

Attributes	
Subelement ID:	016
Data Representation:	ans-74
Length Field:	3
Data Field:	Contents of positions 1–74
Subfields:	N/A
Justification:	N/A
<b>Values</b>	

---

---

All Authorization Request Response/0110 messages in response to Parcelas Authorization Request/0100 messages must include additional information to identify the total effective cost of installment transactions.

Positions 1–12	Total Effective Cost (TEC) (N12)
Positions 13–19	Taxes (N7)
Positions 20–23	% Taxes of Total Amount (N4)
Positions 24–30	Fee (N7)
Positions 31–34	% Fee of Total Amount (N4)
Positions 35–41	Insurance (N7)
Positions 42–45	% Insurance of Total Amount (N4)
Positions 46–52	Other (N7)
Positions 53–56	% Other of Total Amount (N4)
Positions 57–63	Total Amount to Merchant (N7)
Positions 64–67	% Amount to Merchant of Total Amount (N4)
Positions 68–74	% Total Effect Cost (N7)

## 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
Data Representation:	ans-8
Length Field:	3
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: <ul style="list-style-type: none"> <li>• 0 = No grace period</li> <li>• 1 = One month</li> <li>• 2 = Two months</li> </ul>
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
<b>Percta Payment Transactions in the Authorization Request Response/0110</b>	
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: <ul style="list-style-type: none"> <li>• 0 = No grace period</li> <li>• 1 = One month</li> <li>• 2 = Two months</li> </ul>
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.

---

Attributes	
Subelement ID:	008
Data Representation:	ans–23
Length Field:	023
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.

---

## Spain—Domestic ATM Transactions

Following are the technical specifications for Authorization/01xx messages for domestic ATM transactions within Spain.

### **Subelement 017—ATM Domestic Fee**

DE 112, subelement 017 (ATM Domestic Fee) contains fees charged for ATM domestic transactions in Spain.

---

<b>Attributes</b>	
Subelement ID:	017
Data Representation:	n...48; LLLVAR
Length Field:	3
Data Field:	Contents of subfields 1–3
Subfields:	3
Justification:	See subfields.

---

### **Usage**

Following is the usage of subelement 017 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

---

<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Authorization Request/0100	O	•	O
Authorization Request Response/0110	O	•	O
Reversal Request/0400	O	•	O

---

### **Values**

---

See subfields.

---

### **Subfield 1—ATM Service Fee**

DE 112, subelement 017, subfield 1 (ATM Service Fee) contains fee amount in the currency of DE 49 (Currency Code, Transaction) charged to the issuer to compensate the ATM acquirer for the ATM cost incurred for ATM domestic transactions in Spain.

---

#### **Attributes**

Subfield ID	01
Data Representation	n-12
Length Field	2
Justification	Right with leading zeros

#### **Values**

---

ATM Service Fee amount in transaction currency.

---

### **Subfield 2—ATM Disloyalty Fee**

DE 112, subelement 017, subfield 2 (ATM Disloyalty Fee) contains fee amount in the currency of DE 51 (Currency Code, Cardholder Billing), charged by the issuer to the cardholder for using another bank's ATM for ATM domestic transactions in Spain.

---

#### **Attributes**

Subfield ID	02
Data Representation	n-12
Length Field	2
Justification	Right with leading zeros

#### **Values**

---

ATM Disloyalty Fee amount in Cardholder Billing currency.

---

### **Subfield 3—Credit Card Fee**

DE 112, subelement 017, subfield 3 (Credit Card Fee) contains fee amount in the currency of DE 51 (Currency Code, Cardholder Billing) charged by the issuer to the cardholder for the grant of credit for ATM domestic transactions in Spain.

---

#### **Attributes**

Subfield ID	03
Data Representation	n-12

---

Length Field	2
Justification	Right with leading zeros
<b>Values</b>	
Credit Card Fee amount in Cardholder Billing currency.	

---

## United Kingdom—Debt Repayment Transactions

Following are the technical specifications for Authorization/01xx messages for United Kingdom debt repayment transactions within the U.K.

### Subelement 033—UK Recipient Details

DE 112, subelement 033 (UK Recipient Details) supports the transmission of recipient details in an authorization request from acquirer to issuer.

<b>Attribute</b>	<b>Value</b>		
Subelement ID	n-3		
Subelement Length	n-3		
Data Representation	ans...89; LLLVAR		
Data Field	Contents of subfields 1–4		
Number of Subfields	N/A		
Justification	See subfields		
Values	See subfields		
<b>Usage</b>			
Following is the usage of subelement 033 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.			
<b>Message</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>
Authorization Request/0100	C	•	C

### Subfield 1—Recipient Last Name

DE 112, subelement 033 (UK Recipient Details), subfield 1 (Recipient Last Name) contains the last name of the recipient.

<b>Attribute</b>	<b>Value</b>
Subfield ID	n-2
Subfield Length	2
Data Representation	ans...35; LLVAR

---

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

**Values**

Contains valid last name of the recipient (only the first six letters of the last name are required).

---

**Subfield 2—Recipient Postal Code**

DE 112, subelement 033 (UK Recipient Details), subfield 2 (Recipient Postal Code) contains the postal code of the recipient.

Attribute	Value
Subfield ID	n-2
Subfield Length	2
Data Representation	ans-10
Justification	left-justified with trailing spaces

**Values**

Contains valid location postal code of the recipient. First part represents the district, then space-filled.

---

**Subfield 3—Recipient Date of Birth**

DE 112, subelement 033 (UK Recipient Details), subfield 3 (Recipient Date of Birth) contains the date of birth of the recipient.

Attribute	Value
Subfield ID	n-2
Subfield Length	2
Data Representation	n-8
Justification	N/A

**Values**

Contains valid date of birth of the recipient in the format YYYYMMDD.

---

**Subfield 4—Recipient Account Number**

DE 112, subelement 033 (UK Recipient Details), subfield 4 (Recipient Account Number) contains valid account number of the recipient.

Attribute	Value
Subfield ID	n-2
Subfield Length	2

---

Data Representation	ns...20; LLVAR
Justification	N/A
<b>Values</b>	
Contains the recipient account number.	

---

## 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
Data Representation:	ans...999; LLLVAR
Length Field:	3
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

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>
sale_pending_amt	12	Amount of initial sale
credit_limit_req_amt	12	Amount of requested credit limit

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
Data Representation:	ans...999; LLLVAR
Length Field:	3
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.

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
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  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

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
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.

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
<b>Usage</b>		Consumer Application Request Data recommended usage when: <ul style="list-style-type: none"> <li>• DE 60 = 6500080 (Consumer Application Request)</li> <li>• DE 60 = 6500090 (Business Application Request)</li> </ul>

---

### 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
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_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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
local_id_type	1	Update consumer's local ID type
		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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
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

---

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
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
cons_last_name	20	Consumer's last name
cons_suffix	6	Consumer's suffix; SR, JR, III, PHD
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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
	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.

<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
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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
	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
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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
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
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

---

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
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

---

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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

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 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
Data Representation:	ans...999; LLLVAR
Length Field:	3
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
		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		

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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

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 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.

---

<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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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.

#### **Usage**

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.

<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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>		
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
		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		

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
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

---

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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 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.

<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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
fax_info_sent	1	Y or N—Additional information sent via fax, such as list of authorized buyers, financial statement
fax_info_rcvd	1	Y or N—Additional information received via fax, such as list of authorized buyers, financial statement
appl_status	1	A = Approved D = Declined C = Call 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		
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

---

<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		
bill_city	20	Update billing city		
bill_sub_ctry_maint	1	S = successful, U = unsuccessful		

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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

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)

---



---

## **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
Data Representation:	ans...999; LLLVAR
Length Field:	3
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.

Field Name	Max Length	Description
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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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.

---

<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

---

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
user_suffix	6	User's suffix; SR, JR, III, PHD

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
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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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 data 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.

#### **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

---

Data Representation: ans...999; LLLVAR

---

Length Field: 3

---

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.

Field Name	Max Length	Description
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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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
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

---

<b>Field Name</b>	<b>Max Length</b>	<b>Description</b>
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.		
<b>Usage</b>		
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
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

---

Field Name	Max Length	Description
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
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

Data Representation: ans...999; LLLVAR

---

Length Field:	3
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.

Field Name	Max Length	Description
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

Field Name	Max Length	Description
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.

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

Field Name	Max Length	Description
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

Field Name	Max Length	Description
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 = 6500081 (Consumer Application Status Inquiry)
- DE 60 = 6500082 (Consumer User Lookup Inquiry)
- DE 60 = 6500083 (Consumer Account Lookup Inquiry)
- DE 60 = 6500091 (Business Application Status Inquiry)
- DE 60 = 6500092 (Business User Lookup Inquiry)
- DE 60 = 6500093 (Business Account Lookup Inquiry).
- 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
```

## 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
Data Representation:	ans...999; LLLVAR
Length Field:	3
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**

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 the 0600 message *not* be returned in the 0610 message to avoid the maximum message length constraint of 8k bytes.

### **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

<b>MTI</b>	<b>DE</b>	<b>Presence</b>	<b>Data Description</b>
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

**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

MTI	DE	Presence	Data Description
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

MTI	DE	Presence	Data Description
0600	115	Recommended	Business Account Maintenance Data
0610	115	Recommended	Business Account Maintenance Data

### DE 60 = 6500095 Business Counteroffer Reply

MTI	DE	Presence	Data Description
0600	113	Recommended	Application Generic Data
0610	115	Recommended	Business Application Response Data

### DE 60 = 6500096 Business Preapproved Offer Inquiry

MTI	DE	Presence	Data Description
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

---

Data Representation: ans...999; LLLVAR (supports extended character sets)

---

Length Field:	3
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.

#### Administrative Advice/0620 messages

When DE 120 is present in Administrative Advice/0620 messages, DE 120 contains the following:

- In Administrative Advice/0620 messages, DE 120 includes the new subfields Token Requestor ID, Wallet ID, and Device Type.
- 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—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

---

Data Representation: ans...29

---

Length Field: 2

---

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

---

Data Representation: an-14

---

Length Field: 2

---

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

Data Representation:      an-14

Length Field:      2

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**

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

Data Representation:      an-14

---

---

Length Field:	2
Data Field:	Contents of positions 1–14
Justification:	Left, blank-filled
<b>Values</b>	
<b>Positions 1–9: Postal Code</b>	
Postal Code	Cardholder postal/ZIP code
<b>Positions 10–14: Address (Mastercard)</b>	
Address	Cardholder address
<b>Application Notes</b>	
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.

---

DE 101 (File Name)	DE 91 (Issuer File Update Code)			
	1 Add	2 Update	3 Delete	5 Inquiry
MCC102 (Stand-In Account File)	✓	✓	✓	✓
MCC103 (Electronic Warning Bulletin File)	✓		✓	✓
MCC104 (Local Stoplist File)	✓		✓	✓
MCC105 (Payment Cancellation File)	✓	✓	✓	✓
MCC106 (PAN Mapping File)	✓	✓	✓	
MCC107 (Enhanced Value File)	✓	✓	✓	✓
MCC108 (Product Graduation File)	✓	✓	✓	✓
MCC109 (Application Transaction Counter [ATC] File)	✓			✓
MCC111 (PAN-PAR [Payment Account Reference] Mapping File)		✓		

---

### MCC102—Stand-In Account File

DE 120 (Record Data) contains Stand-In Account file data when DE 101 (File Name) contains MCC102.

Following are the MCC102 data fields that should be included in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Include 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	<p>Number that is embossed or encoded or both on the card. Customers may only input account numbers for BINs assigned to the associated Mastercard-assigned customer ID.</p> <p>Format: Sixteen digit Mastercard account number, followed by three spaces.</p>																														
2 Entry Reason	an-1	<p>Reason for listing this card. Valid values:</p> <table> <tr> <td>C</td> <td>=</td> <td>Credit</td> </tr> <tr> <td>F</td> <td>=</td> <td>Fraud</td> </tr> <tr> <td>G</td> <td>=</td> <td>ATM Premium Listing</td> </tr> <tr> <td>L</td> <td>=</td> <td>Lost</td> </tr> <tr> <td>O</td> <td>=</td> <td>Other</td> </tr> <tr> <td>P</td> <td>=</td> <td>Capture Card</td> </tr> <tr> <td>S</td> <td>=</td> <td>Stolen</td> </tr> <tr> <td>U</td> <td>=</td> <td>Unauthorized Use</td> </tr> <tr> <td>V</td> <td>=</td> <td>Premium Listing</td> </tr> <tr> <td>X</td> <td>=</td> <td>Counterfeit</td> </tr> </table>	C	=	Credit	F	=	Fraud	G	=	ATM Premium Listing	L	=	Lost	O	=	Other	P	=	Capture Card	S	=	Stolen	U	=	Unauthorized Use	V	=	Premium Listing	X	=	Counterfeit
C	=	Credit																														
F	=	Fraud																														
G	=	ATM Premium Listing																														
L	=	Lost																														
O	=	Other																														
P	=	Capture Card																														
S	=	Stolen																														
U	=	Unauthorized Use																														
V	=	Premium Listing																														
X	=	Counterfeit																														
3 Date-Last-Update Activity	n-6	<p>Inquiry only and is ignored on add, change, and delete. (This field is returned in the 0312 response message only for inquiry requests.)</p> <p>Date of the last maintenance activity occurring on this account.</p>																														

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
		<p>Format: MMDDYY</p> <p>MM = month</p> <p>DD = day</p> <p>YY = year</p>
4 Time Last Update Activity	n-4	<p>Inquiry only and is ignored on add, change, and delete. (This field returned in the 0312 response message only for inquiry requests.)</p> <p>Time of the last maintenance activity occurring on this account.</p>
		<p>Format: hhmm</p> <p>hh = hour</p> <p>mm = minute</p>
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.
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 are the MCC103 data fields that should be included in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Include 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. Customers 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. 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.
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	Reason for listing this card. Valid values:  C = Credit F = Fraud O = Other X = Counterfeit
6 Filler	an-25	Reserved for future AMS enhancements.
7 Regional Indicator/ Purge Date	an-7	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  R = Region

Field ID and Name	Attributes	Comments/Valid Values																											
		<p>Valid region values:</p> <table> <tr><td>1</td><td>=</td><td>United States</td></tr> <tr><td>A</td><td>=</td><td>Canada</td></tr> <tr><td>B</td><td>=</td><td>Latin America/Caribbean</td></tr> <tr><td>C</td><td>=</td><td>Asia/Pacific</td></tr> <tr><td>D</td><td>=</td><td>Europe</td></tr> <tr><td>E</td><td>=</td><td>Middle East/Africa</td></tr> <tr><td>YY</td><td>=</td><td>purge date year</td></tr> <tr><td>MM</td><td>=</td><td>purge date month</td></tr> <tr><td>DD</td><td>=</td><td>purge date day</td></tr> </table> <p>Note: To purge an account on the card expiration date, enter that date as the purge date. For additional information on purge dates, refer to the <i>Account Management System User Manual</i>.</p>	1	=	United States	A	=	Canada	B	=	Latin America/Caribbean	C	=	Asia/Pacific	D	=	Europe	E	=	Middle East/Africa	YY	=	purge date year	MM	=	purge date month	DD	=	purge date day
1	=	United States																											
A	=	Canada																											
B	=	Latin America/Caribbean																											
C	=	Asia/Pacific																											
D	=	Europe																											
E	=	Middle East/Africa																											
YY	=	purge date year																											
MM	=	purge date month																											
DD	=	purge date day																											

### MCC104—Local Stoplist File

DE 120 (Record Data) contains Local Stoplist file data when DE 101 (File Name) contains MCC104.

Following are the MCC104 data fields that should be included in DE 120 depending on the value in DE 91 (Issuer File Update Code).

When DE 91 Contains...	Include These Fields in DE 120...
1 Add	Use all applicable fields.
<b>NOTE: Add will update an existing record if the system finds a match on the master file.</b>	
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	<p>Number that is embossed, encoded, or both on the card. Customers may input only those account numbers that contain their assigned prefixes.</p> <p>Format: 16-digit Mastercard account number followed by three spaces.</p>
2 Customer ID	n-6	<p>Mastercard-assigned customer ID, a Mastercard customer may input only an account number with a BIN assigned to it.</p> <p>Format: Right-justified, zero-filled</p>
3 Card Program	a-3	Type of card bearing the account number. 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)</p> <p>or</p> <p>(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>

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
		<p>A = Canada          B = Latin America/Caribbean          C = Asia/Pacific          D = Europe          E = Middle East/Africa</p> <p>Region values must be entered in ascending order (1, A, B, C, D, E)</p>
8 Country	an-3	<p>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.</p> <p>Refer to the <i>Quick Reference Booklet</i> for participating countries. Enter spaces if no country is specified.</p>
9 Subcountry	an-2	<p>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.</p> <p>Refer to the <i>Account Management System User Manual</i>. Enter spaces if no subcountry is specified.</p>
10 Purge Date	n-6	<p>Purge date (format YYMMDD) associated with this account number listing as follows:</p> <p>YY = purge date year          MM = purge date month          DD = purge date day</p>
11 Region	an-1	<p>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).</p>
12 Country	an-3	<p>If applicable, second country associated with this account listing; must be a participating country within the issuer's region.</p>
13 Subcountry	an-2	<p>If applicable, second subcountry associated with this account listing; must be a participating subcountry within the issuer's country.</p>

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
14 Purge Date	n-6	If applicable, second purge date associated with this account number listing.
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.
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.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
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—Payment Cancellation File**

DE 120 (Record Data) contains Payment Cancellation file data when DE 101 (File Name) contains MCC105.

Following are the MCC105 data fields that should be included in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Include These Fields in DE 120...</b>
1 = Add	Use all applicable fields; fields 1–5 are mandatory, fields 6–13 are optional
2 = Update	Use all applicable fields; fields 1–5 are mandatory, fields 6–7 are optional. Fields 8–13 not applicable.
3 = Delete	Use fields 1, 4, and 5; fields 2 and 3 must be filled with spaces. Fields 6–13 not applicable.
5 = Inquiry	Use fields 1, 4, and 5; fields 2 and 3 must be filled with spaces. Fields 6–13 not applicable.

Following is the modified DE 120 Layout for MCC105. Amount fields 6 and 7, when provided, must include a minor unit of currency. For example, USD 100.50 entered as 000000010050. Fields 8–9 are sent in the 0312 response message.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Primary Account Number	an-19	<p>Number that is embossed, encoded, or both on the card. Customers may only input account numbers for BINs assigned to the associated customer ID that Mastercard assigned</p> <p>Format: Left justified, with trailing spaces</p>
2 Entry Reason	an-1	<p>Reason for listing this card. Valid value:</p> <p>A = Payment Cancellation</p>
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	<p>Must be unique per acquirer ICA. Must be a value other than spaces.</p> <p>Note: This field is case sensitive.</p>
6 Transaction Amount (low)	n-12	<p>Optional field. Right justified with leading zeros.</p> <p>Indicates a single transaction amount or the start of a transaction amount range.</p> <p>Transaction amount must be stated in the transaction currency and not the cardholder billing currency.</p>
7 Transaction Amount (high)	n-12	<p>Optional field. Right justified with leading zeros.</p> <p>Indicates the end of a transaction amount range.</p> <p>Do not use this field if specifying a single amount.</p> <p>If used, must be greater than Transaction Amount (low).</p> <p>Transaction amount must be stated in the transaction currency and not the cardholder billing currency.</p>
8 Activity Date	n-6	Format is MMDDYY (Month, Day, Year); Provide spaces in request message if fields beyond Field ID 9 are present. System populates data in the response message.
9 Activity Time	n-4	Format is hhmm (hour, minute); Provide spaces in request message if fields beyond Field ID 9 are present. System populates data in the response message.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
10 Card Acceptor ID Code	ans-15 2	Must be unique per acquirer ICA.
11 Card Acceptor ID Code	ans-15 3	Must be unique per acquirer ICA.
12 Card Acceptor ID Code	ans-15 4	Must be unique per acquirer ICA.
13 Card Acceptor ID Code	ans-15 5	Must be unique per acquirer ICA.

## **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.

- The following guidelines apply for the multiple Card Acceptor ID Codes:
  - Issuers will only be able to provide multiple Card Acceptor ID Codes when PAN (field 1) and Acquirer ICA (field 4) are provided in DE 120.
  - The additional Card Acceptor ID Codes must be added in sequence. For example, if codes are entered in Card Acceptor ID Codes fields 5, 10, and 12, skipping field 11, the 0302 Payment Cancellation MCC105 add request will be rejected with DE 39 = 27 (Edit Error) and DE 44 will contain field number 120011.
  - If issuers provide transaction amount or transaction amount range in the 0302 Payment Cancellation add list request, the transaction amount and transaction amount range will be applicable to all the given Card Acceptor ID Codes in the message.

### **MCC106—PAN Mapping File**

DE 120 (Record Data) contains Token to PAN Mapping File data when DE 101 (File Name) contains MCC106.

Following are the MCC106 data fields that should be included in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Include These Fields in DE 120...</b>
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 contactless account number will be deleted.

Following is the DE 120 Layout for MCC106 in the Issuer File Update Request/0302 Message.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Contactless Account Number	an-19	Number that is assigned to the contactless card or device and transmitted from the card or device to the X terminal. Format: Left justified, with trailing spaces

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
2 PAN	an-19	<p>Number that is embossed, encoded, or both on the card. Customers may only input account numbers for BINs assigned to the associated customer ID that Mastercard assigned.</p> <p>Format: Left justified, with trailing spaces</p>
3 Card Expiration Date (PAN)	n-4	<p>Expiration date that is embossed, encoded, or both on the card that represents the cardholder primary account number.</p> <p>Format: YYMM</p>
4 Contactless account number (replacement)	an-19	<p>Replacement account number that is assigned to the contactless card or device and transmitted from card or device to the contactless terminal.</p> <p>Format: Left justified, with trailing spaces</p>
5 PAN (replacement)	an-19	<p>Number that is embossed, encoded, or both on the replacement card. Customers may only input account numbers for BINs assigned to the associated customer ID that Mastercard assigned</p> <p>Format: Left justified, with trailing spaces</p>

The following DE 120 layout applies to Issuer File Update Request/0302 Messages requesting the replacement of a PAN associated with an individual Mastercard Digital Enablement Service (MDES) token, or with all tokens associated with current PAN, in the MCC106 PAN Mapping File.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Mapping File Indicator	an-1	<p>M = Mastercard Digital Enablement Service Tokens excluding Card on File Tokens</p> <p>A = All Mastercard Digital Enablement Service Tokens including Card on File Tokens</p> <p>Best practice for the issuer to use value A</p>
2 Replacement PAN	an-19	<p>Number replacing the number that is embossed, encoded, or both on the card (the primary account number). Customers may input only account numbers for BINs assigned to the associated customer ID assigned by Mastercard.</p> <p>The issuer has the option to provide a replacement primary account number for association to the token.</p> <p>Format: Left-justified, with trailing spaces</p>

Field ID and Name	Attributes	Comments/Valid Values
3	Replacement PAN Expiration Date	<p>Expiration date that is associated with the number replacing the number that is embossed, encoded, or both on the card that represents the cardholder primary account number.</p> <p>If the issuer has provided a replacement primary account number, this field contains the expiration date that is associated with the replacement primary account number.</p> <p>If the issuer has not provided a replacement primary account number, this field contains the expiration date of the existing primary account number.</p> <p>Format: YYMM</p>
4	Primary Account Card Sequence Number	<p>If the issuer has provided a replacement primary account number, this field will contain the card sequence number associated with the replacement primary account number.</p> <p>If the issuer has not provided a replacement primary account number, this field will contain the card sequence number associated with the original primary account number.</p>
5	Notify Wallet Service Provider Indicator	<p>If the issuer has provided a replacement primary account number and replacement primary account number expiration date, this field indicates whether the Wallet Provider should be notified of the change.</p> <p>Values:</p> <p>0 = Update token mapping information and notify the Wallet Provider with the primary account number information</p> <p>1 = Update token mapping information, but do not notify the Wallet Provider with the primary account number information</p> <p>2 = Do not update token mapping information, but do update the Wallet Provider with the primary account number information</p>

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
6 Token	an-19	<p>Surrogate value for a PAN that is consistent with ISO message requirements and is a 13 to 19-digit numeric value that passes basic validation rules of an account number, including the LUHN check.</p> <p>Format: Left-justified, with trailing spaces If field not present, update shall apply to all token to PAN mappings associated with the PAN as follows:</p> <ul style="list-style-type: none"> <li>• This field is optional. If present, the token to PAN mapping update will only be applied to the specified token. If not present, the token to PAN mapping update will be applied to all tokens associated with the current PAN.</li> </ul>

The following DE 120 layout applies to Issuer File Update Request/0302 Messages requesting the suspension, deactivation, or resumption of an MDES token in the MCC106 PAN Mapping File.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Mapping File Indicator	an-1	<p>M = Mastercard Digital Enablement Service Tokens excluding Card on File Tokens</p> <p>A = All Mastercard Digital Enablement Service Tokens including Card on File Tokens</p> <p>Best practice for the issuer to use value A</p>
2 Action Required	an-1	<p>S = Suspend token</p> <p>D = Deactivate token</p> <p>C = Resume token</p>
3 Notify Wallet Service Provider Indicator	n-1	<p>This field indicates whether the Wallet Provider should be notified of the change.</p> <p>Values:</p> <p>0 = Update token mapping information and notify the Wallet Provider with the primary account number information.</p>

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
4 Token—If Updating a Specific Token	an-19	<p>Surrogate value for a PAN that is consistent with ISO message requirements and is a 13 to 19-digit numeric value that passes basic validation rules of an account number, including the LUHN check.</p> <p>Format: Left-justified, with trailing spaces.</p> <p>If field not present, update shall apply to all token to PAN mappings associated with the PAN.</p>

The following DE 120 layout applies to Issuer File Update Request Response/0312 Messages created by Mastercard in response to an MCC106 PAN Mapping File update request.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Contactless account number	an-19	<p>Number that is assigned to the contactless card or device and transmitted from the card or device to contactless terminal.</p> <p>Format: Left justified, with trailing spaces</p>
2 PAN	an-19	<p>Number that is embossed, encoded, or both on the card. Customers may only input account numbers for BINs assigned to the associated customer ID that Mastercard assigned.</p> <p>Format: Left justified, with trailing spaces</p>
3 Card Expiration Date (PAN)	n-4	<p>Expiration date that is embossed, encoded, or both on the actual card.</p> <p>Format: YYMM</p>
4 Contactless account number (replacement)	an-19	<p>Replacement number that is assigned to the contactless card or device and transmitted from the card or device to contactless terminal.</p> <p>Format: Left justified, with trailing spaces</p>
5 PAN (replacement)	an-19	<p>Number that is embossed, encoded, or both on the replacement card. Customers may only input account numbers for BINs assigned to the associated customer ID that Mastercard assigned.</p> <p>Format: Left justified, with trailing spaces</p>
6 Date-Last-Update Activity	n-6	Format: MMDDYY (Month, Day, Year)

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
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 are the MCC107 data fields that should be included in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Include These Fields in DE 120...</b>
1 = Add	Use fields 1-5, field 2 may contain spaces
2 = Update	Use fields 1-5, field 2 may contain spaces
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.

<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.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
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.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
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.
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 are the MCC108 data fields that should be included in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Include These Fields in DE 120...</b>
1 = Add	Use fields 1–7
2 = Update	Use fields 1–7
3 = Delete	Use field 1 only

---

<b>When DE 91 Contains...</b>	<b>Include These Fields in DE 120...</b>
5 = Inquiry	Use field 1 only

---

Following is the DE 120 Layout for MCC108 in the Issuer File Update Request/0302 message.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
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.
5 Previous Product Code	an-3	Optional. The field will contain the product code from which the account is migrating.  This field must contain spaces if a product code is not provided.
6 Program ID	an-6	Conditional. This field is required if the issuer is registering the account for Enhanced Value.  This field must contain spaces if a program ID is not provided.
7 Customer Specific Index (CSI)	an-7	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.  This field must contain spaces if a CSI number is not provided.

---

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:  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.
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—Application Transaction Counter File**

DE 120 (Record Data) contains Application Transaction Counter file data when DE 101 (File Name) contains MCC109.

Following are the MCC109 data fields that should be included in DE 120 depending on the value in DE 91 (Issuer File Update Code).

<b>When DE 91 Contains...</b>	<b>Include These Fields in DE 120...</b>
1 = Add	Fields 1–4 mandatory
3 = Delete (Note: applicable only when submitting an 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 Contactless Account Number	an-19	Number that is assigned to the contactless card or device and transmitted from the card or device to the contactless terminal  Format: Left justified, with trailing spaces
2 Card Sequence Number	n-1	May be zero
3 Contactless Account Expiration Date	n-4	Expiration date  Format: YYMM
4 Contactless Application Transaction Counter (ATC) Value	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 Contactless Account Number	an-19	Number that is assigned to the contactless card or device and transmitted from the card or device to contactless terminal  Format: Left justified, with trailing spaces
2 Card Sequence Number	n-1	May be zero
3 Contactless Account Expiration Date	n-4	Expiration date  Format: YYMM
4 Contactless Application Transaction Counter (ATC) Value	n-5	Right-justified, leading zeros
5 Filler	an-1	

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
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
9 Creation Date/Time Stamp	n-14	Format: MMDDCCYYHHMMSS
10 Last Transaction Time	n-4	Last transaction time for valid ATC. Format: hhmm

### **MCC111—PAN-PAR (Payment Account Reference) Mapping File**

DE 120 (Record Data) contains PAN to PAR Mapping File data when DE 101 (File Name) contains MCC111.

Only PAN replacement and PAR record deletion actions are allowed. Both are handled as an “update”.

Following are the MCC111 data fields that should be included in DE 120 depending on the combination of values in DE 91 (Issuer File Update Code) and DE 120 subfield 1 (Action Required).

<b>When DE 91 Contains...</b>	<b>Include These Subfields in DE 120...</b>
2 = Update  This is the only valid Issuer File Update Code value for MCC111	Subfield 1 is mandatory  <ul style="list-style-type: none"> <li>• When subfield 1 = U (Update), subfield 2 must contain a replacement PAN</li> <li>• When subfield 1 = D (Delete), all other DE 120 subfields must contain spaces</li> </ul>

The following DE 120 layout applies to Issuer File Update Request/0302 messages requesting the replacement of a PAN associated with a PAR value in the MCC111 PAN-PAR Mapping File. This action should be performed when the issuer is replacing the consumer’s current PAN with a new PAN.

<b>Subfield ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Action Required	an-1	U = Update the PAN-PAR mapping record

<b>Subfield ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
2 Replacement PAN	an-19	<p>Number that is embossed, encoded, or both on the replacement card. Customers may only input account numbers for BINs assigned to the associated customer ID assigned by Mastercard.</p> <p>Format: Left justified, with trailing spaces</p>

The following DE 120 layout applies to Issuer File Update Request/0302 messages requesting the deletion of a PAN-PAR mapping record in the MCC111 PAN-PAR Mapping File. This action should be performed only when the issuer has permanently closed/cancelled the consumer's PAN.

<b>Subfield ID and Name</b>	<b>Attributes</b>	<b>Comments/Valid Values</b>
1 Action Required	an-1	D = Delete the PAN-PAR mapping record associated with the PAN in DE 2 (Primary Account Number)

### **DE 120 Error Codes**

Following are the DE 120 Error Codes.

### **MCC102 Error Codes**

The Authorization Platform returns an Issuer File Update Request Response/0312 message where DE 39 contains the value 27 and DE 44 contains the value 120xxx (xxx indicates the DE 120 field in which the error occurred).

<b>Error Code</b>	<b>Error Message</b>
120001	<p>Primary Account Number (PAN), extended not numeric</p> <p>-Or-</p> <p>BIN in Primary Account Number (PAN), extended not on FIM</p> <p>-Or-</p> <p>Origin of message invalid for BIN in Primary Account Number (PAN), extended</p> <p>-Or-</p> <p>Check digit in Primary Account Number (PAN), extended not correct</p> <p>-Or-</p> <p>Primary Account Number (PAN), extended not on Account File (for delete or inquiry).</p>
120002	Entry Reason not one of the following: (C, F, G, L, O, P, S, U, V, X).

Error Code	Error Message
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 Platform returns an 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 DE 120 field in which 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.

---

Error Code	Error Message
120006	<p>Regional indicator is not 1, A, B, C, D, or E.</p> <p>-Or-</p> <p>Regional indicator is not in ascending order.</p>
120007	<p>Region-requested purge date invalid.</p> <p>-Or-</p> <p>Region-requested purge date not equal to current or future date.</p> <p>-Or-</p> <p>Requested purge date must be at least one day beyond current date if account is not already listed.</p>

---

#### MCC104 Error Codes

The Authorization Platform returns an 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 DE 120 field in which 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.
	When DE 39 contains the value 27, DE 44 contains one of the following error codes:
120001	<p>Primary Account Number (PAN), Extended is not numeric</p> <p>-Or-</p> <p>BIN in Primary Account Number (PAN), Extended is invalid</p> <p>-Or-</p> <p>Check digit in cardholder number is not correct and product code is not equal to PNS (Non-standard)</p> <p>-Or-</p> <p>Origin of message invalid for BIN in Primary Account Number (PAN), Extended.</p>
120002	Issuing ICA (customer ID) is not associated with Primary Account Number (PAN)

---

Error Code	Error Message
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 Platform 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 DE 120 field in which the error occurred).

<b>Error Code</b>	<b>Error Message</b>
120001	<p>Primary Account Number (PAN) not within account range that is a Payment Cancellation 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 Payment Cancellation 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>

Error Code	Error Message
120010–120013	<p>Invalid Card Acceptor ID Code</p> <p>If multiple Card Acceptor ID Code occurrences are not provided in sequence, then Add request will be rejected with edit error on the respective field that has spaces in-between two valid Card Acceptor ID Codes.</p> <p>For example: If fields 5, 10, 12 are provided with valid values and field 11 is provided with spaces, then Add request will be rejected with edit error on field 11, DE44=120011.</p>

### MCC106 Error Codes

DE 39 contains the appropriate value and DE 44 contains value 120xxx (where xxx indicates the DE 120 field in which 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	Contactless account number not on MCC106 (PAN Mapping File) (for update or delete)
120002	PAN not on MCC106 (PAN Mapping File) (for update)
	When DE 39 contains value 27 (Issuer File Update Field Edit Error), DE 44 contains one of the following error codes:
120001	Contactless account number not numeric -Or- Prefix in contactless account number not valid -Or- Check digit in contactless account number not correct -Or- Contactless account number not within account range that is a Contactless Mapping Service participant

Error Code	Error Message
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 contactless account number prefixes do not have same country and product</p> <p>-Or-</p> <p>PAN prefix should not be participating in the Contactless Mapping Service</p>
120003	Invalid PAN card expiration date
120004	<p>Replacement contactless account number not numeric</p> <p>-Or-</p> <p>Prefix in Replacement contactless account number not valid</p> <p>-Or-</p> <p>Check digit in Replacement contactless account number not correct</p> <p>-Or-</p> <p>Replacement contactless account number not within account range that is a Contactless 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 contactless account number prefixes do not have same country and product</p> <p>-Or-</p> <p>Replacement PAN prefix should not be participating in the Contactless Mapping Service</p>
When DE 39 contains value 80 (Duplicate add, action not performed), DE 44 contains the following error code:	
120001	Contactless account number is a duplicate

---

Error Code	Error Message
120004	Replacement contactless account number is a duplicate

---

**MCC107 Error Codes**

DE 39 contains the appropriate value and DE 44 contains value 120xxx (where xxx indicates the DE 120 field in which 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:	

---

---

Error Code	Error Message
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> <p>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</p> <p>-Or-</p> <p>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</p> <p>-Or-</p> <p>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)</p> <p>-Or-</p> <p>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</p> <p>-Or-</p> <p>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</p> <p>-Or-</p> <p>DE 91 contains a value of 2 (Update) and the account is not listed on MCC107</p> <p>-Or-</p> <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>

---

Error Code	Error Message
120002	Primary Account Number (PAN) is not numeric -Or- Primary Account Number (PAN) is not valid -Or- PAN does not begin with 51-56, 36, or 38
120003	Account Category is not valid -Or- Account Category is not valid for the product associated with the account range
120004	Purge Date is not equal to or less than 20 years from the current date -Or- Purge Date is not formatted in CCYYMMDD format
120005	Program ID is not 6 alphanumeric positions -Or- Program ID is not a valid value, as assigned to the issuer by Mastercard
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 DE 120 field in which 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:

Error Code	Error Message
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> <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>

Error Code	Error Message
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
120006	<p>Invalid program ID</p> <p>-Or-</p> <p>The Program ID is not an-6</p> <p>-Or-</p> <p>The Program ID is not provided for an account being registered for Mastercard Enhanced Value Platform (Field 2 Account Category value B)</p> <p>-Or-</p> <p>The Program ID contains all zeros or all spaces for an account being registered for Mastercard Enhanced Value Platform (Field 2 Account Category value B)</p> <p>-Or-</p> <p>The Program ID is not a valid Program ID for the ICA associated with the PAN</p> <p>-Or-</p> <p>The Program ID is provided for an account being graduated to a premium product</p>
120007	<p>Invalid CSI value</p> <p>-Or-</p> <p>The Customer Specific Index (CSI) value provided is not an-7</p> <p>-Or-</p> <p>The CSI value is not valid for the ICA associated with the PAN</p>

The Authorization Platform returns an Issuer File Update Request Response/0312 message where DE 39 contains value 25, 27, or 80 and DE 44 contains value 120xxx (xxx indicates the DE 120 field in which the error occurred).

Error Code	Error Message
<b>When DE 39 contains value 25 (Unable to locate record on file), DE 44 contains the following error code:</b>	
120001	Primary account number not on file.
<b>When DE 39 contains value 27 (Issuer File Update Field Edit Error), DE 44 contains the following error code:</b>	
120001	<p>One of the following:</p> <ul style="list-style-type: none"><li>• Primary Account Number (PAN) is not numeric.</li><li>• PAN is not valid.</li><li>• PAN already listed on MCC108 with a value of P.</li><li>• PAN already listed with a value of P.</li><li>• PAN not listed on MCC108.</li><li>• PAN for an account range that is a non-Moldova range.</li><li>• Invalid country associated with PAN for Account Level Management.</li></ul>
120002	Account Category is not valid for the product associated with the account range.
120003	<p>One of the following:</p> <ul style="list-style-type: none"><li>• Product Code is not valid.</li><li>• Product Code is not valid for the Category Code defined in Field 2.</li><li>• Product Code override is not valid for the product currently maintained at the issuers account range.</li></ul>
120004	<p>One of the following:</p> <ul style="list-style-type: none"><li>• Purge Date is not equal to or less than 20 years from the current date.</li><li>• Purge Date is not formatted in CCYYMMDD format.</li></ul>
120005	Product Code is not valid.
120006	Program ID is not all spaces.
120007	<p>One of the following:</p> <ul style="list-style-type: none"><li>• CSI value provided is not an-7.</li><li>• CSI value is not valid for the ICA associated with the PAN.</li></ul>
<b>When DE 39 contains value 80 (Duplicate add, action not performed), DE 44 contains the following error code:</b>	

Error Code	Error Message
120001	Primary account number is a duplicate.

The Authorization Platform returns an Issuer File Update Request Response/0312 message where DE 39 contains value 25, 27, or 80 and DE 44 contains value 120xxx (xxx indicates the DE 120 field in which the error occurred).

Error Code	Error Message
<b>When DE 39 contains value 25 (Unable to locate record on file), DE 44 contains the following error code:</b>	
120001	Primary account number not on file.
<b>When DE 39 contains value 27 (Issuer File Update Field Edit Error), DE 44 contains the following error code:</b>	
120001	One of the following: <ul style="list-style-type: none"><li>• Primary Account Number (PAN) is not numeric</li><li>• Primary Account Number (PAN) is not valid</li><li>• PAN does not begin with 51–55, 36, or 38</li><li>• PAN for an account range that is a non-U.S. range (the country code associated with the range is not 840)</li><li>• 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</li><li>• DE 91 contains value 1 (Add) and Field 1 contains a PAN that is already listed on MCC108 with Account Category value P</li><li>• 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</li><li>• The country associated with the PAN is not valid for Account Level Management</li></ul>
120002	One of the following: <ul style="list-style-type: none"><li>• Account Category is not valid</li><li>• Account Category is not valid for the product associated with the account range</li><li>• Field 2 does not contain a valid Account Category value. Valid values are: B or space</li><li>• 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</li></ul>

Error Code	Error Message
120003	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Product Code is not valid</li> <li>• Product Code override is not valid for the product currently maintained at the issuers account range</li> <li>• Field 3 does not contain a valid graduated product code</li> </ul>
120004	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Purge Date is not equal to or less than 20 years from the current date.</li> <li>• Purge Date is not formatted in CCYYMMDD format.</li> </ul>
120005	The product code is not a valid product code
120006	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Invalid program ID</li> <li>• The Program ID is not an-6</li> <li>• The Program ID is not provided for an account being registered for Mastercard Enhanced Value Platform (Field 2 Account Category value B)</li> <li>• The Program ID contains all zeros or all spaces for an account being registered for Mastercard Enhanced Value Platform (Field 2 Account Category value B)</li> <li>• The Program ID is not a valid Program ID for the ICA associated with the PAN</li> <li>• The Program ID is provided for an account being graduated to a premium product</li> </ul>
120007	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Invalid CSI value</li> <li>• The Customer Specific Index (CSI) value provided is not an-7</li> <li>• The CSI value is not valid for the ICA associated with the PAN</li> </ul>
<b>When DE 39 contains value 80 (Duplicate add, action not performed), DE 44 contains the following error code:</b>	
120001	Primary account number is a duplicate.

### MCC109 Error Codes

DE 39 contains the appropriate value and DE 44 contains value 120xxx (where xxx indicates the DE 120 field in which 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:	

Error Code	Error Message
120001	Contactless Account Number/Card Sequence Number/Contactless Account Expiration Date not on Contactless Application Transaction Counter (ATC) File (MCC109) (for add or inquiry)
When DE 39 contains value 27 (Issuer File Update Field Edit Error), DE 44 contains one of the following error codes:	
120001	Contactless Account Number not numeric -Or- Prefix in contactless account not valid -Or- Check digit in Contactless Account Number not correct
120002	Card Sequence Number not numeric
120003	Contactless 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	Contactless Account Number/Card Sequence Number/Contactless Account Expiration Date already exists on file (applies to Add)

### MCC111 Error Codes

DE 39 contains the appropriate value and DE 44 contains value 120xxx (where xxx indicates the DE 120 subfield in which the error occurred).

Error Code	Error Message
When DE 39 contains value 25 (Unable to locate record on file [no action taken]), DE 44 contains the following error code:	
120001	The PAN in DE 2 is not associated with a PAR value in the MCC111 PAN-PAR Mapping File and therefore the action requested in subfield 1 cannot be performed.
When DE 39 contains value 27 (Issuer File Update field edit error), DE 44 contains the following error code:	

<b>Error Code</b>	<b>Error Message</b>
120001	<p>The Action Required value in DE 120 subfield 1 is not D (Delete) or U (Update). Value is space or other than D or U.</p> <p>-Or-</p> <p>The Action Required value in DE 120 subfield 1 is D (Delete) but the PAN in DE 2 is associated with a token in the MCC106 Token-PAN Mapping File that is in active or suspended status. Therefore the PAN-PAR mapping record cannot be deleted.</p>
120002	<p>The content of DE 120 subfield 2 is not properly formatted</p> <ul style="list-style-type: none"> <li>• Not numeric (alpha, special, or spaces)</li> <li>• Incorrect length</li> <li>• Invalid check digit</li> </ul> <p>-Or-</p> <p>The Action Required value in DE 120 subfield 1 is U (Update) but no replacement PAN is present in subfield 2.</p> <p>-Or-</p> <p>The Action Required value in DE 120 subfield 1 is U (Update) but the account range of the replacement PAN in subfield 2 is not eligible for association with a PAR value.</p> <p>-Or-</p> <p>The Action Required value in DE 120 subfield 1 is U (Update) but the replacement PAN in subfield 2 is already associated with another PAR value.</p>

---

When DE 39 contains value 80 (Duplicate Add, action not performed), DE 44 contains the following error code:

---

120002	The PAN value in DE 2 is a duplicate of the PAN value in DE 120 subfield 2. The replacement PAN in subfield 2 must be different than the current PAN in DE 2.
--------	---

## **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

---

Data Representation:	ISO:	n...999; LLLVAR
	Mastercard:	n...6; LLLVAR
Length Field:	3	
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**

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).

---

## 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

---

Data Representation: ans...999; LLLVAR

---

Length Field: 3

---

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) only applies to the Swedish Domestic Authorization Switching Service (SASS), Peru, and the Mastercard Installment Payment Service. For 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]). For Peru and Mastercard Installment Payment Service, DE 123 contains a text message to be printed on point-of-sale (POS) sales receipts.

---

### Attributes

---

Data Representation: ISO: ans...999; LLLVAR  
Mastercard: ans...512; LLLVAR

---

Length Field: 3

---

Subfields: N/A

---

Justification: N/A

---

### Usage

---

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**

---

---

For SASS, 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>
<b>WHEN...</b>	<b>THEN the Authorization Platform</b>
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> <p>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.</p>

---

## DE 124—Member-Defined Data

DE 124 (Member-defined Data) is described for general use, MoneySend only, Brazil Maestro only, Bill Payment at the ATM only, and Mastercard Digital Enablement Service use.

**NOTE: For detailed data layout requirements when using DE 124 with the Mastercard Digital Enablement Service, refer to the Mastercard Digital Enablement Service section in the Program and Service Format Requirements chapter of this manual.**

### DE 124—Member-Defined Data (General Use)

DE 124 (Member-defined Data—General Use) may be used to submit up to 299 bytes of customer-defined data. DE 124 can contain program-specific data as defined by the DE 124 subelements.

---

#### Attributes

---

Data Representation: ans...299; LLLVAR

---

Length Field: 3

---

Data Field: Contents of positions 1–299

---

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
Reversal Advice/0420	•	C	C

### **Application Notes**

DE 124 may be required in support of programs to convey information between customers in an authorization message.

#### **Acquirers:**

<b>IF DE 124 is...</b>	<b>THEN...</b>
Up to 299 bytes in acquirer-generated authorization messages	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 299 bytes of data in acquirer-generated authorization messages	The Authorization Platform will only send the first 299 bytes of data to the issuer.

Absolute positioning of data in DE 124 subfields is required; padding will be necessary. Customers 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. Customers must not use all zeros, all low values, or all high values when formatting DE 124.

**Subfields 1–4:** are used for MoneySend transactions. DE 124, subfield 2 (Sender/Payer Name/User ID) and subfield 3 (Sender/Payer Address) are mandatory in MoneySend Payment Transactions. DE 124 is optional in MoneySend Funding Transactions.

**Subfields 6–13:** are used for Maestro credit usage in Brazil.

#### **Issuers:**

<b>IF DE 124 is...</b>	<b>THEN...</b>
Up to 299 bytes in issuer-generated response messages	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 299 bytes of data in issuer-generated response messages	The Authorization Platform will truncate to 299 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:

- 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.
  - 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.
  - 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.
  - Include DE 124 in the Authorization Request Response/0110 message even when the acquirer did not send it in the Authorization Request/0100 message.
- 

## **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 MoneySend transactions. DE 124, subfield 2 (Sender/Payer Name/User ID) and subfield 3 (Sender/Payer Address) are mandatory in MoneySend Payment Transactions. 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: 0555555801215305401

---

## **Subfield 2—Sender/Payer/User ID**

DE 124, subfield 2 (Sender/Payer/User ID) contains sender consumer, business, government, and non-government names, 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 consumer, business, government, and non-government names, payer name, or user ID value up to 24 character spaces. If the consumer name is populated, the format must be (last name, first name).

---

### 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

---

---

Street address (ans-50)

City (ans-25)

State/Province Code (ans-3)

Country Code (ans-3)

Postal Code (ans-10)

Field	Data	Edit
Street Address	ans-50	Must be present  Must not be all blanks or all zeros
State	ans-3	If country is U.S. or Canada, state must be a valid state code for U.S. or a valid province code for Canada  Must not be all blanks or zeros  For all other countries, may contain all spaces or an applicable state code
Country	ans-3	Must be present  Must not be all blanks or all zeros  Must be a valid country code  Must not be a blocked country

---

City and Postal codes must be present if applicable.

---

#### Application Notes

---

Subfield 3 is required for MoneySend Payment Transactions and must be properly formatted. Subfield 3 is optional for MoneySend Funding Transactions

---

**NOTE: Transaction will be declined if the sender Country is subject to comprehensive geographic sanctions published by the Office of Foreign Assets Control (OFAC), <http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx>. The current list of countries subject to such sanctions is Cuba, Iran, North Korea, Sudan, and Syria; however, this list is subject to change.**

#### Subfield 4—Additional Sender Information

DE 124, subfield 4 (Additional Sender Information) contains telephone number, date of birth, or optional message.

---

Attributes

---

Data Representation: ans-65

---

Data Field: Contents of positions 135-199

---

Justification: Left-justified with trailing spaces

---

**Values**

---

Additional sender information is formatted as follows:

Telephone number (n-20)

Date of Birth (n-8) (MMDDYYYY)

Optional message (ans-37)

---

### **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.

---

**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 124—Member-Defined Data (Colombia Domestic Use Only)

DE 124 (Member-defined Data [Colombia Domestic Use Only]) is used only for Colombia domestic activity transactions.

**Subfields 1–11:** are used for Colombia domestic activity.

### Subfield 1—Card Issuer Data

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 1 (Card Issuer Data) defines the FIID and Logical Network associated with the card issuer.

---

#### Attributes

---

Data Representation:	ans-19
----------------------	--------

Data Field:	Contents of positions 1–19
-------------	----------------------------

Justification:	Left-justified with trailing spaces
----------------	-------------------------------------

Usage:	Optional
--------	----------

---

#### Example Values

---

FIID (1–4)

Logical Network ID (5–8) = Examples are as follow: PRO1, MDS, BNET, ASCR, PRO2

- PRO1 = Redeban Multicolor
- MDS or BNET = Mastercard
- ASCR = AScredibanco
- PRO2 = Credibanco

Constant Value (9–19) = zeros

---

### Subfield 2—Tax (IVA)

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 2 Tax (IVA) defines the tax for Colombia domestic activity.

---

**Attributes**

Data Representation:	n-12
Data Field:	Contents of positions 20–31
Justification:	Right-justified with leading zeros
Usage:	Required. If no value, it should contain zero.

**Example Values**

---

Amount is in Colombian pesos and carries an implied two position decimal.

---

**Subfield 3—Tax Amount Base**

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 3 (Tax Amount Base) defines the tax amount base for Colombia domestic activity.

---

**Attributes**

Data Representation:	n-12
Data Field:	Contents of positions 32–43
Justification:	Right-justified with leading zeros
Usage:	Required.

**Values**

---

Amount is in Colombian pesos and carries an implied two position decimal.

---

**Subfield 4—Retailer Data**

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 4 (Retailer Data) defines the local merchant ID for Colombia domestic activity.

---

**Attributes**

Data Representation:	ans-27
Data Field:	Contents of positions 44–70
Justification:	Left-justified with trailing spaces
Usage:	Optional

**Example Values**

---

Each acquirer may elect to provide the merchant ID in their original format. Example to follow:

Unique merchant ID (44–53)

Spaces (54–62)

Terminal Group (63–66)

Retailer Region (67–70)

---

### **Subfield 5—Terminal Acquirer Data**

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 5 (Terminal Acquirer Data) identifies information about the terminal owner for Colombia domestic activity.

---

#### **Attributes**

---

Data Representation: ans-16

---

Data Field: Contents of positions 71–86

---

Justification: Right-justified

---

Usage: Optional

---

#### **Example Values**

---

FID (71–74)

---

Logical Network (75–78)

---

Constant Value = zeros

---

### **Subfield 6—Acquirer Original Processing Code**

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 6 (Original Processing Code) contains the original processing code for Colombia domestic activity.

---

#### **Attributes**

---

Data Representation: n-6

---

Data Field: Contents of positions 87–92

---

Justification: Right-justified

---

#### **Values**

### **Subfield 7—Bill Payment/Top up Data**

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 7 (Bill Payment/Top up Data) provides information related to bill payment for Colombia domestic activity.

---

**Attributes**

---

Data Representation: ans-36

---

Data Field: Contents of positions 93–128

---

Justification: Left-justified with trailing spaces

---

**Values**

Service Code (93–96) = Number used to identify the provider company (for example: 0001 = Bogota Power Light Company)

Service Description (97–126) = Service Provider Bill ID (for example: Invoice number, additional billing information)

Originator Device (127) = Alphanumeric (for example, P)

Filler (128) = space

---

### **Subfield 8—Local POS Data**

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 8 (Local POS Data) present when transaction is a web payment or recurring payment. This field is optional.

---

**Attributes**

---

Data Representation: n-1

---

Data Field: Contents of positions 129

---

Justification: N/A

---

Usage: Optional

---

**Example Values**

---

6 = Preauthorization/recurring payment

---

7 = Web payment, Electronic orders

---

### **Subfield 9—Local Response Codes**

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 9 (Local Response Codes) identifies unique response codes for Colombia domestic activity.

---

**Attributes**

---

Data Representation: ans-2

---

Data Field: Contents of positions 130–131

---

Justification: Left-justified with trailing spaces

---

Usage:	Optional
--------	----------

---

**Example Values**

---

M2 = Invalid national customer identifier

---

## Subfield 10—Original Transaction Data

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 10 (Original Transaction Data) is present for reversal messages to help uniquely identify the original message.

---

**Attributes**

---

Data Representation:	ans-42
----------------------	--------

---

Data Field:	Contents of positions 132–173
-------------	-------------------------------

---

Justification:	Left-justified with trailing spaces
----------------	-------------------------------------

---

Usage:	Optional
--------	----------

---

**Example Values**

---

Original Message Type (132–135) = 0100 or 0200

Sequence Number (136–147)

Original Transaction Date (148–151) = MMDD

Original Transaction Time (152–157) = HHMMSS

Capture Date (158–161) = MMDD

Filler (162–173) = all zeros

---

## Subfield 11—IAC Tax Amount

DE 124, (Member-defined Data [Colombia Domestic Use Only]), subfield 11 (IAC Tax Amount) defines the IAC Tax for Colombia domestic activity.

---

**Attributes**

---

Data Representation:	n-12
----------------------	------

---

Data Field:	Contents of positions 174–185
-------------	-------------------------------

---

Justification:	Right-justified with leading zeros
----------------	------------------------------------

---

**Values**

---

Amount is in Colombian pesos and carries an implied two position decimal.

---

## 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

---

Data Representation: b-8

---

Length Field: N/A

---

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:

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

---

Authorization Request/0100	C	X	C
----------------------------	---	---	---

---

### 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

---

Data Representation: ISO: ans...999; LLLVAR

---

Mastercard: ans...100; LLLVAR

---

Length Field: 3

---

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.

Attribute	Description
Data Representation:	ISO: ans...999; LLLVAR Mastercard: ans...100; LLLVAR
Length Field:	3
Data Field:	Contents of positions 1–100
Subfields:	N/A
Justification:	N/A

---

### Usage

---

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

#### **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

Data Representation:	b-8
Length Field:	2
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.....	837
Permitted Transactions by Card Program.....	837
Value Constraints by Transaction Type.....	841
Account Status Inquiry Service.....	845
Purchase Account Status Inquiry / Recurring Payment Account Status Inquiry.....	845
Payment Account Status Inquiry.....	847
Authorization Platform Edits.....	850
Address Verification Service.....	851
Authorization Request/0100—AVS and Authorization Request.....	852
Authorization Request Response/0110—AVS and Authorization Request.....	853
Network Management Request/0800—AVS Sign-on.....	854
Alternate Processing.....	854
DE 48 and DE 120 Structure in AVS Transactions.....	855
Authorization Platform Edits.....	856
Automated Fuel Dispenser Completion.....	857
AFD Message Scenarios.....	858
Authorization Request/0100—Automated Fuel Dispenser Pre-authorization.....	858
Authorization Advice/0120—Acquirer-Generated (Automated Fuel Dispenser Completion)....	859
Authorization Advice/0120—Acquirer-Generated (Automated Fuel Dispenser Completion).....	860
Authorization Advice Response/0130—Issuer-Generated (Responding to an Acquirer-Generated).....	861
Alternate Processing.....	861
Clearing AFD Transactions.....	862
Account Level Management.....	862
Alternate Processing.....	862
ATM Bill Payment Service.....	864
Authorization Request/0100—ATM Bill Payment, Europe Acquired.....	864
Authorization Request/0100—ATM Bill Payment, Non-Europe Acquired.....	865
Authorization Platform Edits.....	865
ATM Credit Card Cash Advance in Installments.....	866
Authorization Request/0100—ATM Installment Inquiry.....	866
Authorization Request Response/0110—ATM Installment Inquiry.....	867
Authorization Request/0100—ATM Installment Withdrawal.....	868

---

Authorization Request Response/0110—ATM Installment Withdrawal.....	868
Authorization and Preauthorization Processing Standards.....	869
Balance Inquiry—ATM.....	876
Authorization Request/0100—ATM Balance Inquiry.....	876
Authorization Request/0100—ATM Balance Inquiry Edits.....	877
Authorization Request Response/0110—ATM Balance Inquiry.....	878
Authorization Request Response/0110—ATM Balance Inquiry Edits.....	878
Authorization Advice/0120—Acquirer-Generated—ATM Balance Inquiry Edits.....	879
Alternate Processing.....	879
Balance Inquiry—Point-of-Sale.....	880
Authorization Request/0100—POS Balance Inquiry.....	880
Authorization Request Response/0110—POS Balance Inquiry.....	881
Authorization Request/0100—POS Balance Inquiry Edits.....	882
Authorization Request/0110—POS Balance Inquiry Edits.....	884
Authorization Advice/0120—Acquirer-Generated—POS Balance Inquiry Edits.....	885
Alternate Processing.....	885
Balance Inquiry—Short Message Service.....	885
Authorization Request/0100—Short Message Service Balance Inquiry.....	885
Balance Inquiry—Mobile Remote Payments Program.....	886
Authorization Request/0100—Mobile Remote Payments Program Balance Inquiry.....	886
Chip-Specific Value Constraints.....	887
Chip Partial Grade Value Constraints.....	887
Chip Full Grade Value Constraints.....	888
Contact and Contactless Chip Specific Value Constraints.....	889
Canada Region Debit Mastercard Merchant Acceptance.....	890
Acquirers.....	890
Issuers.....	891
Authorization Platform Edits.....	891
Cardholder Authentication Service.....	893
Authorization Platform Edits—Cardholder Authentication Service.....	894
Card Validation Code 2.....	897
Authorization Request/0100—CVC 2 Verified.....	897
Authorization Request/0100—CVC 2 Unverified.....	898
Authorization Request/0100—CVC 2 Processed by Stand-In.....	899
Authorization Request/0100—CVC 2 Processed by X-Code.....	900
CVC 2 DE 48 Structure.....	901
Authorization Request/0100—CVC 2 .....	901
Authorization Request Response/0110—CVC 2 .....	902
Authorization Platform Edits.....	902

---

Card Validation Code 3.....	903
Authorization Request Response/0110—CVC 3 Result.....	903
Contactless CVC 3 Processing Service.....	904
Authorization Request/0100—CVC 3.....	904
Dynamic CVC 3 Application Transaction Counter (ATC) Processing.....	905
Dynamic CVC 3 Application Transaction Counter (ATC) Information.....	906
MCC109 (Application Transaction Counter File).....	907
Authorization Platform Edits.....	907
Card Validation Code Result.....	908
Optional Non-valid CVC 3 Processing.....	908
ATC Data Extract File.....	909
Alternate Processing.....	910
Contactless Mapping Service for Contactless M/Chip and Contact M/Chip Transactions.....	910
Contactless Mapping Service Processing of Contactless M/Chip and Contact M/Chip Transactions.....	911
Authorization Platform Edits.....	912
Cross-Border Fee Manager Service.....	913
Currency Conversion.....	913
Amount-Related Data Elements in Authorization and Reversal Messages.....	914
Dual Message System Processing.....	916
Acquirer Send MTIs in Authorization and Reversal Messages.....	917
Acquirer Receive MTIs in Authorization and Reversal Messages.....	918
Issuer Receive MTIs in Authorization and Reversal Messages.....	918
Issuer Send MTIs in Authorization and Reversal Messages.....	919
Alternate Processing.....	920
Authorization Platform Edits.....	921
Electronic Commerce Processing.....	924
Best Practices for E-Commerce Transactions.....	924
No Security Protocol.....	927
Channel Encryption.....	928
Authorization Request/0100—Electronic Commerce Purchase.....	929
Authorization Request Response/0110—Electronic Commerce Purchase.....	931
Authorization Platform Edits.....	932
Mastercard SecureCode.....	933
Static AAV.....	935
Forgotten Card at ATM.....	936
Reversal Request/0400—Forgotten Card.....	936
Gaming Payment Transactions.....	936
Gaming Payment Transaction Processing in the Europe and Middle East/Africa Regions.....	937

---

Authorization Request/0100—Gaming Payment.....	938
Reversal Request/0400—Gaming Payment.....	938
Authorization Platform Edits.....	939
Gaming Payment Transaction Processing in the United States Region.....	940
ICCR Service.....	940
ICCR Service Overview.....	940
ICCR Enrollment.....	941
Incremental Preauthorization Standards.....	941
Authorization Platform Edits.....	947
Maestro Pre-authorized Transactions.....	950
Authorization Request/0100—Maestro Pre-Authorization.....	950
Authorization Advice/0120—Maestro Pre-Authorization Completion.....	951
Maestro Recurring Payments Program.....	951
Authorization Request/0100—Maestro Recurring Payment.....	952
Authorization Platform Edits.....	953
Magnetic Stripe Compliance.....	954
Authorization Request/0100—Magnetic Stripe-read.....	956
Authorization Request Response/0110—Magnetic Stripe-read.....	956
Mastercard Commercial Payments Account.....	957
Authorization Platform Edit to Support MAP in Brazil.....	957
Authorization Platform Edits to Support MAP in Mastercard European Economic Area Subregion.....	957
Mastercard Digital Enablement Service.....	959
Message Layouts—Pre-digitization Payment Network Messages.....	959
Authorization Request/0100—Tokenization Eligibility.....	960
DE 124 Subfields in Authorization Request/0100—Tokenization Eligibility.....	962
Authorization Request Response/0110—Tokenization Eligibility.....	966
DE 124 Subfields for Authorization Request Response/0110—Tokenization Eligibility.....	967
Authorization Request/0100—Tokenization Authorization.....	970
DE 124 Subfields in Authorization Request/0100—Tokenization Authorization.....	974
Authorization Request Response/0110—Tokenization Authorization.....	978
DE 124 Subfields in Authorization Request Response/0110—Tokenization Authorization...	979
Authorization Request/0100—Activation Code Notification.....	983
DE 124 Subfields in Authorization Request/0100—Activation Code Notification.....	986
Authorization Request Response/0110—Activation Code Notification.....	988
Authorization Request/0100—Tokenization Complete Notification.....	988
DE 124 Subfields in Authorization Request/0100—Tokenization Complete Notification....	991
Authorization Request Response/0110—Tokenization Complete Notification.....	993
Authorization Request/0100—Tokenization Event Notification.....	993

---

DE 124 Subfields in Authorization Request/0100—Tokenization Event Notification.....	995
Authorization Request Response/0110—Tokenization Event Notification.....	998
Issuer File Update Request/0302—Maintenance (Token/PAN Update).....	998
DE 120 Layout for MCC106 Mastercard Digital Enablement Service (Token Update).....	998
DE 120 Layout for MCC106 Mastercard Digital Enablement Service (PAN Update—Deactivate/Suspend/Resume Token).....	1000
Issuer File Update Request Response/0312—Issuer Token Maintenance Response (Token/PAN Update).....	1001
Administrative Advice/0620—Issuer Token Notification Advice.....	1002
DE 120 Layout for Administrative Advice/0620—Issuer Token Notification Advice for Activation Code Notification.....	1003
DE 120 Layout for Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Complete Notification.....	1006
DE 120 Layout for Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Event Notification.....	1009
Administrative Advice Response/0630—Issuer Token Notification Advice Response.....	1012
MDES for Merchants.....	1012
Mastercard Fraud Scoring Services.....	1014
Expert Monitoring for Issuers.....	1015
For More Information.....	1015
Fraud Rule Manager.....	1015
To Participate.....	1016
For More Information.....	1016
Decision Intelligence.....	1016
Overview.....	1016
How it Works.....	1016
Issuers' Potential Benefit from Decision Intelligence.....	1017
Message Specification Requirements.....	1017
To Participate.....	1018
For More Information.....	1018
Expert Monitoring for Merchants.....	1018
Benefits.....	1018
To Participate.....	1019
For More Information.....	1019
Authorization Request/0100—Fraud Scoring.....	1019
Alternate Processing.....	1020
Mastercard Hosted Mobile Phone Top-Up ATM Transactions.....	1020
Authorization Request/0100—Mastercard Hosted Mobile Phone Top-Up.....	1020
Authorization Platform Edits.....	1021

---

Mastercard In Control Service.....	1023
Authorization Request/0100—In Control Purchase Control.....	1023
Dual Message System Processing.....	1024
Mastercard In Control Virtual Card Service.....	1025
Mastercard In Control Real Card Spend Control.....	1025
Process of a Mastercard In Control Service Eligible Transaction.....	1025
Authorization Request/0100—In Control Real Card Spend Control.....	1027
Authorization Advice/0120—In Control Real Card Spend Control.....	1028
Mastercard In Control Virtual Card Mapping and Spend Control Service.....	1028
Authorization Request/0100—In Control Virtual Card Mapping and Spend Control Service..	1029
Exception Processing.....	1029
Mastercard Installment Payment Service.....	1030
Mastercard Merchant Presented QR.....	1030
Authorization Platform Edits.....	1031
Alternate Processing.....	1042
Mastercard MoneySend.....	1043
Authorization Request/0100—Mastercard MoneySend Funding Transactions.....	1043
Reversal Request/0400—MoneySend Funding Transaction.....	1044
Authorization Platform Edits.....	1045
Authorization Request/0100—MoneySend Payment Transactions.....	1046
Reversal Request/0400—MoneySend Payment Transaction.....	1048
Authorization Platform Edits.....	1050
Mastercard MoneySend Issuer Transaction Controls.....	1062
Network Blocking.....	1062
Sanction Screening.....	1063
For More Information About Implementing the MoneySend Program.....	1063
Mastercard Safety Net.....	1063
Masterpass Transactions.....	1064
Authorization Request/0100—Masterpass Online Wallet.....	1065
Authorization Advice/0120—Acquirer-Generated.....	1066
Authorization Advice/0120—System-Generated.....	1066
Authorization Platform Edits.....	1066
Merchant Advice Codes.....	1067
Merchant Advice Codes Used with Response Codes.....	1067
M/Chip Processing Services.....	1069
Program use of M/Chip Processing Service Data Elements.....	1069
Chip To Magnetic Stripe Conversion.....	1071
Authorization and Stand-In Processing.....	1072
M/Chip Cryptogram Pre-validation.....	1075

---

Validation of the Application Cryptogram.....	1076
Generation of the Issuer Chip Authentication Data.....	1078
DE 60 (Advice Reason Code).....	1078
Alternate Processing.....	1080
Authorization Platform Edits.....	1080
Combined Service Option.....	1080
M/Chip Cryptogram Validation in Stand-In Processing.....	1080
Validation of the Application Cryptogram.....	1081
Generation of the Issuer Chip Authentication Data.....	1083
DE 60—Advice Reason Code.....	1083
Alternate Processing.....	1084
Authorization Platform Edits.....	1084
MIP Transaction Blocking.....	1085
MIP Transaction Block Setup.....	1086
Authorization Platform Edits.....	1086
Full BIN Block.....	1087
Authorization Platform Edits.....	1088
Mobile Remote Payments.....	1088
Authorization Platform Edits.....	1089
Partial Approvals.....	1090
Authorization Request/0100—Partial Approval.....	1090
Authorization Request Response/0110—Partial Approval.....	1090
Reversal Request/0400—Partial Approval.....	1092
Reversal Advice/0420—Partial Approval.....	1092
Authorization Advice/0120—Acquirer-Generated.....	1093
Alternate Processing.....	1093
Authorization Platform Edits.....	1093
Payment Transactions.....	1096
Authorization Request/0100—Payment Transaction Message.....	1096
Authorization Request Response/0110—Payment Transaction.....	1097
Authorization Platform Edits.....	1098
PIN Management Service.....	1100
Chip PIN Management Service.....	1100
Authorization Request/0100—PIN Change or PIN Unblock (Chip Card).....	1100
Authorization Request Response/0110—PIN Change or PIN Unblock (Chip Card).....	1101
Reversal Request/0400—PIN Change (Chip Card).....	1102
Magnetic Stripe PIN Management Service.....	1103
Authorization Request/0100—PIN Change (Magnetic Stripe Card).....	1103
Authorization Request Response/0110—PIN Change (Magnetic Stripe Card).....	1105

---

Reversal Request/0400—PIN Change (Magnetic Stripe Card).....	1105
Authorization Request/0100 Edits (Magnetic Stripe Card).....	1106
Authorization Advice/0120—Acquirer-Generated Edits (Magnetic Stripe Card).....	1108
Reversal Request/0400 Edits (Magnetic Stripe Card).....	1108
Issuer Response Options to a Magnetic Stripe PIN Change Request.....	1109
PIN Processing for Europe Region Customers.....	1110
PIN Translation Edits.....	1111
PIN Validation.....	1112
PIN Validation Edits.....	1113
PIN Key Management.....	1115
PIN Verification Value/PIN Offset on File Service.....	1116
Processing Transactions Using PVV/PIN Offset.....	1116
Processing Parameters.....	1116
PVV/PIN Offset File Format.....	1117
Alternate Processing.....	1118
PIN Processing for Non-Europe Customers.....	1119
Acquirer Requirements.....	1119
Support either Static or Dynamic PIN Encryption Key (PEK) Exchanges.....	1119
Mastercard Magnetic Stripe Compliance Program Compliance.....	1120
Authorization Request/0100—PIN Transactions.....	1120
Authorization Request Response/0110—PIN Transactions.....	1121
Issuer Requirements.....	1123
Receive Purchase Transactions that Contain a PIN.....	1123
Support Static or Dynamic PEK Exchanges.....	1123
Authorization Request/0100—PIN Messages.....	1124
Authorization Advice/0120—PIN Messages.....	1125
Reversal Advice/0420—PIN Messages.....	1126
Alternate Processing.....	1126
Support for Both Acquiring and Issuing Processing.....	1127
Cleartext Use Prohibited.....	1127
Emergency Static PEK or Emergency KEK Process.....	1127
Previous PEKs.....	1128
PIN Verification Value on File Service.....	1128
PIN Translation and Verification Process.....	1130
Detection of PEK Corruption Using Sanity Checks.....	1134
Authorization Platform Sanity Check Error.....	1134
Issuer Sanity Check Error.....	1136
Private Label Processing.....	1137
Authorization Request/0100—Private Label Processing.....	1137

---

Card Activation for Private Label Processing.....	1138
Authorization Request/0100 and Reversal Request/0400—Card Activation at Point of Sale.....	1138
Alternate Processing.....	1140
Authorization Platform Edits.....	1140
Card Activation Plus Initial Load for Private Label Processing.....	1142
Product Inquiry Service.....	1143
Authorization Request/0100—Product Inquiry Service.....	1144
Proximity Payments.....	1145
Authorization Request/0100—Proximity Payments.....	1145
Purchase of Goods or Services with Cash Back.....	1146
Authorization Request/0100—Purchase of Goods or Services with Cash Back.....	1146
Issuer Response Options.....	1147
Reversal Request/0400.....	1148
Reversal Advice/0420.....	1149
Authorization Advice/0120.....	1149
Authorization Advice/0120—Acquirer-Generated.....	1149
Alternate Processing.....	1149
Authorization Platform Edits.....	1150
Real-Time Substantiation.....	1153
Participation in Real-Time Substantiation.....	1154
Merchant Terminal Verification.....	1154
Real-Time Substantiation Amounts.....	1155
Transaction Processing Examples.....	1156
Authorization Platform Edits.....	1161
Reversal Processing.....	1163
Best Practices for Authorization Reversal Processing.....	1163
Full Reversals.....	1167
Partial Reversals.....	1167
Reversals of Balance Inquiry Transactions.....	1167
Reversals of Purchase of Goods or Services with Cash Back Transactions.....	1167
Alternate Processing.....	1168
Authorization Platform Edits.....	1169
Visa Transaction Processing.....	1171
Visa Custom Payment Service.....	1171
Authorization Request/0100—Visa Custom Payment Service.....	1171
Authorization Request Response/0110—Visa Custom Payment Service.....	1173
DE 48 Structure in a Visa Custom Payment Service Transaction.....	1174
Visa Programs.....	1175

Visa CVV2.....	1175
Visa Fleet Card ID.....	1176
Visa Commercial Card Inquiry.....	1177
Visa Token Processing.....	1178
Authorization Request/0100—Visa Token Request.....	1179
Authorization Request Response/0110—Visa Token Request Response.....	1180

## Product Value Constraints

Product value constraints list types of transactions permitted by card program, and the interrelated 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:

- Mastercard (MCC)
- Debit Mastercard (DMC)
- Maestro (MSI)
- Cirrus (CIR)
- Mastercard Electronic (MCE)
- Private Label (PVL)

### Permitted Transactions by Card Program

Following are the types of transactions permitted by card program and the interrelated value constraints for certain data elements in Authorization Platform messages.

The interrelated data elements are:

- DE 3 (Processing Code)
- DE 22 (Point-of-Service [POS] Entry Mode)
- DE 52 (Personal ID Number [PIN] Data)
- DE 61 (Point-of-Service [POS] Data)

### Permitted Transactions by Card Program

Use the reference number in the Ref column in the following table with the specific value constraints in the “Value Constraints by Transaction Type” table.

Ref	Transaction Type	PAN Entry Mode	CVM	MCC	DMC	MSI	CIR	MCE	PVL
<b>ATM Withdrawal</b>									
1.1	ATM <sup>31</sup>	Magnetic Stripe	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X	X		
1.2	ATM <sup>31</sup>	Chip	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X <sup>a</sup>	X		
<b>Cash Advance</b>									

<sup>31</sup> For this message, DE 18 must contain value 6011 (Automated Cash Disbursements)

<b>Ref</b>	<b>Transaction Type</b>	<b>PAN Entry Mode</b>	<b>CVM</b>	<b>MCC</b>	<b>DMC</b>	<b>MSI</b>	<b>CIR</b>	<b>MCE</b>	<b>PVL</b>
2.1	Cash Advance <sup>32</sup>	Manual	Signature	X	X				
2.2	Cash Advance <sup>32</sup>	Magnetic Stripe	Signature	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	
2.3	Cash Advance <sup>32</sup>	Magnetic Stripe	Online PIN	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	
2.4	Cash Advance <sup>32</sup>	Chip	Offline PIN	X	X			X	
2.5	Cash Advance <sup>32</sup>	Chip	Online PIN	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	
2.6	Cash Advance <sup>32</sup>	Chip	Signature	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	
2.7	Electronic Cash Advance <sup>32</sup>	Magnetic Stripe	Online PIN				X	X	
2.8	Electronic Cash Advance <sup>32b</sup>	Chip	Offline PIN				X	X	
2.9	Electronic Cash Advance <sup>32</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 <sup>ac</sup>		X <sup>ac</sup>	
3.4	Purchase	Chip	Offline PIN	X <sup>a</sup>	X <sup>a</sup>	X <sup>ac</sup>		X <sup>a</sup>	
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 <sup>ac</sup>		X <sup>a</sup>	
3.7	Purchase	Chip	No CVM			X <sup>a</sup>			
3.8	Purchase	Credential on File	No CVM	X	X	X			
3.9	MO/TO	Manual	No CVM	X	X	X		X	

<sup>32</sup> For this message, DE 18 must contain value 6010 (Manual Cash Disbursements)

<b>Ref</b>	<b>Transaction Type</b>	<b>PAN Entry Mode</b>	<b>CVM</b>	<b>MCC</b>	<b>DMC</b>	<b>MSI</b>	<b>CIR</b>	<b>MCE</b>	<b>PVL</b>
3.10	MO/TO	Credential on File	No CVM	X	X	X			
3.11	Recurring Payment	Credential on File	N/A	X	X	X			
3.12	CAT Level 1	Magnetic Stripe	Online PIN	X <sup>a</sup>		X <sup>a</sup>			
3.13	CAT Level 1	Chip	Online PIN	X <sup>a</sup>		X <sup>a</sup>			
	CAT Level 1	Chip	Offline PIN						
3.14	CAT Level 1	Chip	Offline PIN						
3.15	CAT Level 2	Magnetic Stripe	No CVM	X <sup>a</sup>		X <sup>a</sup>		X	
3.16	CAT Level 2	Chip	No CVM	X <sup>a</sup>		X <sup>a</sup>		X	
3.17	CAT Level 3	Magnetic Stripe	No CVM	X <sup>a</sup>		X <sup>a</sup>		X	
	CAT Level 3	Chip	Offline PIN						
3.18	CAT Level 3	Chip	No CVM	X <sup>a</sup>		X <sup>a</sup>		X	
3.19	CAT Level 4	Magnetic Stripe	No CVM	X <sup>a</sup>		X <sup>a</sup>		X	
3.20	CAT Level 4	Chip	No CVM	X <sup>a</sup>		X <sup>a</sup>		X	
3.21	CAT Level 6	Credential on File	No CVM	X		X	X		
3.22	CAT Level 6	Electronic Commerce	No CVM	X		X	X	X <sup>d</sup>	X
3.23	CAT Level 6	Electronic Commerce	Offline PIN	X		X	X		
3.24	CAT Level 6	Electronic Commerce	Online PIN	X		X	X		
3.25	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 <sup>a</sup>		X <sup>a</sup>	X	X	X
<b>PIN Change Management</b>									

<b>Ref</b>	<b>Transaction Type</b>	<b>PAN Entry Mode</b>	<b>CVM</b>	<b>MCC</b>	<b>DMC</b>	<b>MSI</b>	<b>CIR</b>	<b>MCE</b>	<b>PVL</b>
5.1	ATM PIN unblock <sup>31</sup>	Chip	Online PIN	X	X	X	X	X	
5.2	ATM PIN change <sup>31</sup>	Chip	Online PIN	X	X	X	X	X	
5.3	ATM PIN change <sup>31</sup>	Magnetic Stripe	Online PIN	X	X	X	X	X	
<b>Balance Inquiry</b>									
6.1	ATM Balance Inquiry <sup>31g</sup>	Magnetic Stripe	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X <sup>a</sup>	X	X <sup>a</sup>	
6.2	ATM Balance Inquiry <sup>31g</sup>	Chip	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X <sup>a</sup>	X	X <sup>a</sup>	
6.3	POS Balance Inquiry	Magnetic Stripe	Signature	X <sup>a</sup>	X <sup>a</sup>	X <sup>a</sup>		X <sup>a</sup>	X
6.4	POS Balance Inquiry	Magnetic Stripe	Online PIN	X <sup>a</sup>	X <sup>a</sup>	X	X	X <sup>a</sup>	X
6.5	POS Balance Inquiry	Chip	Offline PIN	X	X	X		X	X
6.6	POS Balance Inquiry	Chip	Signature	X <sup>a</sup>	X <sup>a</sup>			X <sup>a</sup>	X
6.7	POS Balance Inquiry	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				
<b>Purchase with Cash Back (PWCB)</b>									
7.1	PWCB	Magnetic Stripe	Signature		X <sup>h</sup>	X <sup>a</sup>			
7.2	PWCB	Magnetic Stripe	Online PIN		X <sup>h</sup>	X			
7.3	PWCB	Chip	Offline PIN		X <sup>h</sup>	X			
7.4	PWCB	Chip	Online PIN		X <sup>a</sup>	X <sup>a</sup>			
7.5	PWCB	Manual	Signature			X			
<b>Refund</b>									
8.1	Refund	Manual	Signature	X	X			X	

Ref	Transaction Type	PAN Entry Mode	CVM	MCC	DMC	MSI	CIR	MCE	PVL
8.2	Refund	Magnetic Stripe	Signature	X <sup>a</sup>	X <sup>a</sup>	X			X
8.3	Refund	Magnetic Stripe	Online PIN			X			
8.4	Refund	Chip	Signature	X <sup>a</sup>	X <sup>a</sup>				
8.5	Refund	Chip	Online PIN			X <sup>a</sup>			
8.6	Refund	Chip	Offline PIN	X	X				
8.7	Refund	Chip	No CVM			X <sup>a</sup>			

**Table Key:**

<sup>a</sup> Contactless transactions permitted. No CVM is required for non-ATM transactions under contactless CVM 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> Approved domestic countries, as indicated in *Mastercard Rules*.

## Value Constraints by Transaction Type

Following are value constraints by transaction type.

### 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>33</sup>	010000	901, 91x (or P 801)		0 or 1

<sup>33</sup> For this message, DE 18 must contain value 6011 (Automated Cash Disbursements)

<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>
1.2	ATM, Chip, Online PIN <sup>33</sup>	010000	051, 071	P	0 or 1
<b>Cash Advance</b>					
2.1	Cash Advance, Manual, Signature <sup>34</sup>	170000	00x, 01x (or 79x)	S	0
2.2	Cash Advance, Magnetic Stripe, Signature <sup>34</sup>	170000	90x, 91x (or 80x)	S	0
2.3	Cash Advance, Magnetic Strip, Online PIN <sup>34</sup>	170000	90x, 91x (or 80x)	P	0
2.4	Cash Advance, Chip, Offline PIN <sup>34</sup>	170000	051	S	0
2.5	Cash Advance, Chip Online PIN <sup>34</sup>	170000	051, 071	P	0
2.6	Cash Advance, Chip, Signature <sup>34</sup>	170000	05x, 07x	S	0
2.7	Electronic Cash Advance, Magnetic Stripe, Online PIN <sup>34</sup>	010000	901	P	0
2.8	Electronic Cash Advance, Chip, Offline PIN <sup>34</sup>	010000	051	S	0
2.9	Electronic Cash Advance, Chip Online PIN <sup>34</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, 91x (or 80x)	S	0
3.3	Purchase, Magnetic Stripe, Online PIN	00xx00	901, 911 (or 80x)	P	0
3.4	Purchase, Chip, Offline PIN	00xx00	051	S	0
3.5	Purchase, Chip, Signature	00xx00	05x, 07x	S	0
3.6	Purchase, Chip, Online PIN	00xx00	051, 071	P	0
3.7	Purchase, Chip, No CVM	00xx00	05x, 07x	None	0
3.8	Purchase, Credential on File, No CVM	00xx00	10x	None	0
3.9	MO/TO, Manual, No CVM	00xx00	01x, 10x	None	0
3.10	MO/TO, Credential on File, No CVM	00xx00	10x	None	0

<sup>34</sup> For this message, DE 18 must contain value 6010 (Manual Cash Disbursements)

<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>
3.11	Recurring Payment, Credential on File, No CVM	00xx00	10x	No CVM	0
3.12	CAT Level 1, Magnetic Stripe, Online PIN	00xx00	901, 911 (or 801)	P	1
3.13	CAT Level 1, Chip, Online PIN	00xx00	051, 071	P	1
3.14	CAT Level 1, Chip, Offline PIN	00xx00	051	S	1
3.15	CAT Level 2, Magnetic Stripe, No CVM	00xx00	90x, 91x (or 80x)	None	2
3.16	CAT Level 2, Chip, No CVM	00xx00	05x, 07x	None	2
3.17	CAT Level 3, Magnetic Stripe, No CVM	00xx00	90x, 91x (or 80x)	None	3
3.18	CAT Level 3, Chip, No CVM	00xx00	05x, 07x	None	3
3.19	CAT Level 4, Magnetic Stripe, No CVM	00xx00	90x (or 80x)	None	4
3.20	CAT Level 4, Chip, No CVM	00xx00	05x, 07x	None	4
3.21	CAT Level 6, Credential on File, No CVM	00xx00	10x	None	6
3.22	CAT Level 6, Electronic Commerce, No CVM	00xx00	10x, 81x, 82x	None	6
3.23	CAT Level 6, Electronic Commerce, Offline PIN	00xx00	10x, 81x	S	6
3.24	CAT Level 6, Electronic Commerce, Online PIN	00xx00	10x, 81x, 82x	P	6
3.25	CAT Level 7	00xx00	No constraints	Any constraints	7
<b>Payments</b>					
4.1	Payment Transactions, No CVM	280000	No constraints	None	No constraints
<b>PIN Change Management</b>					
5.1	ATM PIN unblock, Chip, Online PIN <sup>33</sup>	910000	051	P	0 or 1
5.2	ATM PIN change, Chip, Online PIN <sup>33</sup>	920000	051	P	0 or 1
5.3	ATM PIN change Magnetic Stripe, Online PIN	920000	021, 901	P	0 or 1
<b>Balance Inquiry</b>					

<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>
6.1	ATM Balance Inquiry, Magnetic Stripe, Online PIN <sup>33</sup>	30xx00	901, 911	P	0 or 1
6.2	ATM Balance Inquiry, Chip, Online PIN	30xx00	051, 071	P	0 or 1
6.3	POS Balance Inquiry, Magnetic Stripe, Signature	300000 or 303000	90x, 91x (or 80x)	S	0
6.4	POS Balance Inquiry, Magnetic Stripe, Online PIN	300000 or 303000	901, 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, 07x	S	0
6.7	POS Balance Inquiry, Chip, Online PIN	300000 or 303000	051, 071	P	0
6.8	SMS Balance Inquiry				
<b>Purchase with Cash Back (PWCB)</b>					
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, 01x	S	0
8.2	Refund, Magnetic Stripe, Signature	20xx00	90x, 91x (or 80x)	S	0

<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>
8.3	Refund, Magnetic Stripe, Online PIN	20xx00	901 (or 801)	P	0
8.4	Refund, Chip, Signature	20xx00	05x, 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.

The Account Status Inquiry Service supports purchase account status inquiry transactions and payment account status inquiry transactions for Mastercard® credit, Debit Mastercard®, and Maestro® acceptance brands.

In addition to Mastercard products, Account Status Inquiry Service transaction processing supports the following types of acceptance brands:

- American Express
- Diners
- Discover
- JCB
- Private label cards
- Visa

The Account Status Inquiry Service does not provide any chargeback rights in the event of a dispute.

## Purchase Account Status Inquiry / Recurring Payment Account Status Inquiry

A Purchase Account Status Inquiry (ASI) or a Recurring Payment ASI is an optional service that allows merchants to validate that a cardholder account is open and the account is not listed in the Electronic Warning Bulletin—without negatively affecting a cardholder's funds availability when establishing a recurring or bill payment relationship, validating a card-not-present purchase before fulfillment, or before submitting an authorization request for the full amount of a recurring payment. A Recurring Payment ASI must comply with all existing recurring payment transaction identification requirements.

## Account Status Inquiry Transaction Process

1. The acquirer submits an Account Status Inquiry transaction request in the Authorization Request/0100 message containing:

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 00 (Purchase)
- DE 4 (Amount, Transaction) with a transaction amount of zero
- DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service Request), value 52 (AVS and Authorization Request/0100) for AVS requests (optional)
- DE 48, subelement 92 (CVC 2 Value), CVC 2 value (optional)
- DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI])

If Recurring Payment ASI:

- DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence), value 4 (Standing order/recurring transactions)
2. The issuer, at its discretion, sends the acquirer an Authorization Request Response/0110 message where DE 39 (Response Code) may contain either value 00 (Approved or completed successfully), 05 (Do not honor), 85 (Not declined), or other valid business decline responses. Invalid business declines include values 03 (Invalid merchant), 12 (Invalid transaction), 13 (Invalid amount), 30 (Format error) on DE 4 (Amount, Transaction), 51 (Insufficient funds/over credit limit), 57 (Transaction not permitted to issuer/cardholder), and 58 (Transaction not permitted to acquirer/terminal).

If the issuer is unable to reply, the acquirer will receive a response code of 91 (Authorization System or issuer system inoperative).

**NOTE: The acquirer should consider any DE 39 value, other than 00 or 85, a decline response.**

3. If applicable, the issuer provides the applicable AVS response in DE 48, subelement 83 (Address Verification Service Response), and provides a valid CVC 2 response in DE 48, subelement 87 (Card Validation Code Result) in the Authorization Request Response/0110 message.

**NOTE: Product Inquiry messages do not include address verification and/or CVC 2 validation requests. See separate description of Product Inquiry Service.**

Acquirers are prohibited from placing a value of one major unit of currency or any other nominal test amount (including equivalent units of local currency such as EUR 1 or JPY 1) that does not represent an actual purchase amount in DE 4 of the Authorization Request/0100 message.

Transactions occurring at an automated fuel dispenser in the U.S. region identified with MCC 5542 may continue to submit USD 1 (or local currency equivalent) authorization requests.

Contactless transit aggregated transactions generated by the transit authority and held for a period of time before being cleared may continue to submit an authorization request for USD 1 or an amount up to the cardholder verification method (CVM) limit amount published in the *Chargeback Guide* on the day of the transaction (or local currency equivalent) authorization requests.

## Country- and Currency-Related Data in MDES Pre-Digitization and ASI Messages

Issuers that use the country-level authorization service for cards designated for local use only and have chosen to receive MDES pre-digitization and ASI messages must be aware that when a funding account range is configured for local use only, Mastercard will modify the country- and currency-related data fields in the MDES pre-digitization and ASI messages to match the issuer country code and primary currency code (as applicable) of the funding account range, according to the configurations provided by the issuer during the onboarding process. The country- and currency-related data fields include the following:

- DE 43 (Card Acceptor Name/Location for All Transactions), subfield 5 (Card Acceptor State or Country Code)
- DE 49 (Currency Code, Transaction)
- DE 61 (Additional POS Data), subfield 13 (POS Country Code)

Issuers that are not configured for local use only will continue to see the MDES pre-digitization and ASI messages with the United States country and currency codes.

## Payment Account Status Inquiry

A Payment Account Status Inquiry (Payment ASI) enables payers to verify that issuers will accept a Payment Transaction on behalf of a payee (recipient) for the actual transaction amount for a particular recipient card account before collecting funds from the sender and initiating the Payment Transaction authorization to credit an account.

### Benefits

Issuers can provide a response to an inquiry sent by the payer, indicating whether the issuer will accept a subsequent Payment Transaction authorization for a particular recipient account and amount. Obtaining a successful Payment ASI helps to eliminate the need for a payer to return funds to the sender and can be useful in cases where returning funds to the sender is impractical or difficult.

The Payment ASI helps improve the payer's experience when confirming a recipient's card account for future use. Issuers can clearly identify:

- The difference between a Payment ASI transaction and a Payment Transaction authorization, so that they can respond and act accordingly.
- The difference between a Payment ASI transaction and a Purchase ASI transaction.

### How It Works

Acquirers can submit an ASI transaction for a payment to determine whether an issuer will post the specified amount to a particular card account before collecting funds from the sender.

Payment ASI transactions are non-financial transactions. Issuers must not credit the receiving cardholder account based on the amount provided in the Payment ASI request.

- When an issuer receives a Payment ASI transaction of zero, the issuer should confirm that the recipient's card account exists and can be used in the future for receiving funds.

- When an issuer receives a Payment ASI transaction for greater than zero, the issuer should confirm that the amount specified does not exceed a prepaid load limit or other types of limits they may have for Payment Transactions.
- When the issuer provides an approval response to the Payment ASI for the receiving account, the issuer is indicating that it is expecting to approve a subsequent Payment Transaction request message when it is received for the account.

**NOTE: The receiving issuer may reject the subsequent Payment Transaction if circumstances for the account have changed.**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
A Payment ASI qualifies for a Mastercard® MoneySend™ Payment Transaction	Applies regular MoneySend Payment edits.
A Payment ASI request response from the issuer is either not provided or the issuer is not available	Sends the acquirer an Authorization Request Response/0110 message where DE 39 = 91 (Authorization System or issuer system inoperative).
An acquirer advice Payment ASI is initiated	Sends the acquirer an Authorization Advice/0130 message where DE 39 = 12 (Invalid transaction).
An acquirer reversal of a Payment ASI is initiated	Sends the acquirer a Reversal Request Response/0410 message where DE 39 = 12 (Invalid transaction).

### **Payment Account Status Inquiry Transaction Messages**

Following is a list of the data elements and values applicable to Payment ASI Authorization Request/0100 messages.

<b>Data Element</b>	<b>Value</b>	<b>Comment</b>
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	28	Payment
DE 4 (Amount, Transaction)	Equal to or greater than 0	Equal to or greater than zero
DE 48 (Additional Data—Private Use), subelement 77 (Funding/Payment Transaction Type Indicator)	C01, C02, C03, C04, C05, C06, C09	
DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service Request)	52	Optional AVS

Data Element	Value	Comment
DE 48 (Additional Data—Private Use), subelement 92 (CVC 2)	CVC 2	Optional CVC 2
DE 61 (Point-of-Service [POS] Data), subfield 87 (POS Transaction Status)	8	Account Status Inquiry Service (ASI)

### **MoneySend Payment ASI Transaction Messages**

Following is a list of the data elements and values applicable to MoneySend Payment ASI Authorization Request/0100 messages.

Data Element	Value	Comment
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	28 (Payment Transaction)	
DE 4 (Amount, Transaction)	Equal to or greater than 0	For transaction-value limits, refer to the <i>MoneySend Program Guide</i> .
DE 18 (Merchant Type)	MCC 6536 (MoneySend Intracountry)  MCC 6537 (MoneySend Intercountry)	
DE 48 (Additional Data—Private Use), subelement 77 (Funding/Payment Transaction Type Indicator)	C07 (MoneySend Person-to-Person)  C52 (MoneySend Account-to-Account Transfers)  C53 (MoneySend Agent Cash Out)  C54 (MoneySend Credit Card Bill Payment)  C55 (MoneySend Business Disbursement)  C56 (MoneySend Government/Non-profit Disbursement)  C57 (MoneySend Acquirer Merchant Settlement)	MoneySend Funding/ Payment Transaction Type Indicators

Data Element	Value	Comment
DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service Request) Request)	52 (AVS and Authorization Request/0100)	Optional AVS
DE 48 (Additional Data—Private Use), subelement 92 (CVC 2)	CVC 2	Optional CVC 2  If the originating institution does not have CVC data for push payment transactions on the Mastercard Network, this field should be left blank. The receiving institution must not decline MoneySend payment transactions on the basis that the CVC data is not populated.
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status)	8 (Account Status Inquiry Service [ASI])	
DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level)	0 (Not a CAT transaction)	
DE 108 (MoneySend Reference Data)		Transactions are optional for all MoneySend funding transactions and certain fields are required for MoneySend ASI Transactions. For technical requirements, refer to the <i>MoneySend Program Guide</i> .
DE 124, subfields 1–4		Subfields 2 and 3 are mandatory; subfields 1 and 4 are optional.

## Authorization Platform Edits

The Authorization Platform performs the following edits on Account Status Inquiry transactions.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains value 8 (Account Status Inquiry Service [ASI]) 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 [ASI]) 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 AVS. 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.

**NOTE:**

- For more information about issuer and acquirer participation in AVS, requirements, and service options, refer to the *Customer Interface Specification* and *Authorization Manual*.
- The Global Safety and Security Standards mandate that issuers, acquirers, and processors must code for the Authorization security fields that are required to support the Address Verification service. The service themselves are not mandate, but issuers, acquirers, and processors must code for the authorization message field that support this service.

## 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>

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 120, subfield 1 (AVS Service Indicator 1)	M	•	C	Postal code (an-9) Address (ans...20 Mastercard) Address (ans...20 Visa) 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).
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.**

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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 of this manual.
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.

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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 of this manual.
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.**

### **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**

---

**WHEN...**

**THEN the Authorization Platform....**

---

### **Authorization Request/0100—Request and Address Verification Service**

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.

<b>LLL            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>mandatory</b>							
<b>1002 maximum bytes (LLL + TCC + AVS Data)</b>							

The following table illustrates DE 120 contents for subfield 01 (AVS Service Indicator 1).

<b>LLL            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 was discontinued 28 June 2011.**

<b>WHEN the acquirer...</b>	<b>THEN the Authorization Platform...</b>
DE 48, subelement 82 (AVS Request Data) = 51 (AVS-Only)	Sends the acquirer an Authorization Request Response/0110 message where: DE 39 = 12 (Invalid Transaction)

The Authorization Platform performs the following edit for AVS and Authorization Request/0100 messages.

<b>WHEN the acquirer...</b>	<b>THEN the Authorization Platform...</b>
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>

The Authorization Platform performs the following edits for AVS and Authorization Request Response/0110 messages.

<b>WHEN the issuer...</b>	<b>THEN the Authorization Platform...</b>
Sends an Authorization Request Response/0110 message where DE 39 is 00 (Approved) or 08 (Honor with ID) or 85 (Not declined) and DE 48 subelement 82 is 52 (AVS Request) DE 48, subelement 83 (AVS Response) is present with a value not equal to X, Y, A, W, Z, N, U, R, S.	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 = 048083 (indicating the data element in error)</li> </ul>

<b>WHEN the issuer...</b>	<b>THEN the Authorization Platform...</b>
<p>Sends an Authorization Request Response/0110 message with either an Approved or Declined response where:</p> <ul style="list-style-type: none"> <li>• DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service Request) contains value 52 (AVS and Authorization Request/0100)</li> </ul> <p>and</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 83 (Address Verification Service Response) is present with a value not equal to A (Address matches, postal code does not), N (Neither address nor postal code matches), 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), 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), and Z (For U.S. addresses, five-digit postal code matches, address does not)</li> </ul>	<p>Will set the default value as U and will forward the Authorization Request Response/0110 message to the acquirer.</p> <p>and</p> <p>Will not send the issuer an Authorization Response Negative Acknowledgement/0190 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format Error)</li> <li>• DE 44 (Additional Response Data) = 048083 (indicating the data element in error)</li> </ul>
<p>Sends an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 82 contains value 52</li> </ul> <p>and</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 83 is not present</li> </ul>	<p>Will set the default value as U and will forward the Authorization Request Response/0110 message to the acquirer.</p>

## **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) 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](#).

**NOTE: The Data Integrity Automated Fuel Dispenser (AFD) edit for acquirers of AFD merchants that are located in the U.S. region is described in the *Data Integrity Monitoring Program* manual.**

## AFD Message Scenarios

Mastercard is supporting the following usage scenarios for AFD authorization messages.

WHEN the AFD Authorization Request Response/0110 contains...	THEN the AFD acquirer...
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 that is less than or equal to 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, or an Authorization Advice/0120 message with a DE 04 zero amount, 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 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	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, or 1 = Authorized Level 1 CAT if PIN used

### **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.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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 63 (Trace ID) to further assist issuers in matching an AFD completion advice to the original preauthorization
  - 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, refer to the Data Element Definitions chapter of 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.

Data Element	Org	Sys	Dst	Values/Comments
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.

### **Clearing AFD Transactions**

Mastercard recommends that the Trace ID (DE 15 [Settlement Date] and DE 63 [Network Data]) of the completion advice response be used within the clearing presentment.

As an alternative, if the Trace ID of the original preauthorization is used for clearing presentment, that same Trace ID must be included in the AFD completion advice message within DE 48, subelement 63 (Additional Data, Trace ID).

## **Account Level Management**

---

Mastercard Account Level Management is a platform that enables specialized processing so that Mastercard can manage capabilities at the individual card account level.

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. The following are the key capabilities of Account Level Management functionality. Availability of, and distinctions of, are based on location:

- Enhanced Value (United States, Canada, and select countries in the Europe region)
- Product Graduation Plus (United States, Australia, and select countries in the Europe region)
- Product Graduation Select (select countries in the Latin America and Caribbean and Europe regions)
- High Value (United States)
- Spend Shortfall (World Mastercard and World Elite Mastercard) (United States)
- Small Business Spend Processing (United States)

Refer to the *Account Level Management User Manual* for detailed information.

### **Alternate Processing**

Both the Stand-In System and the X-Code System will verify that DE 38, position 6 in the Authorization Request Response/0110 message contains the value provided by the Authorization Platform in DE 48, subelement 38 of the Authorization Request/0100 message.

### **Stand-In Support for Product Graduation**

Stand-In processing supports Product Graduation. For product graduated accounts, Stand-In processing will use the product code in DE 63, subfield 1 instead of the product code associated with the authorization account range when applying Stand-In limits at the product code level.

Mastercard offers issuers two options for defining Stand-In parameters for graduated accounts:

- **Graduated Product Code Limits**

Issuers can establish limits at the authorization account range level for each product code supported for Product Graduation. These limits will apply specifically to accounts within that account range that are graduated to that product and can be different from the limits that the issuer establishes for an account range that is associated to the same product code. If the issuer takes no action to establish limits for product codes supported for Product Graduation, the Mastercard default limits for the graduated product will apply. Mastercard provides the Stand-In Processing Transaction Category Code Global Parameters (Form 041g) available on Mastercard Connect™ for issuer defined limits.

- **Customer-Specific Index (CSI)**

A CSI allows issuers to establish and associate a unique set of Stand-In limits directly to specific product graduated accounts and not the authorization account range or product. Assignment of a CSI is flexible—a single CSI can be used for one account, or it can be assigned to multiple accounts, across multiple ICAs and account ranges for an issuer's given parent ICA. If an issuer identifies a condition that is not addressed by an existing CSI, the issuer can request a new CSI to meet that condition and assign it to the applicable accounts.

Issuers have the option to associate CSI limits with one or more product codes. If the issuer does not choose to associate CSI limits with a product code, the CSI limits will be applied to all accounts assigned to that CSI, regardless of product code.

If an issuer chooses to associate CSI limits with a product code, the issuer must ensure that the accounts assigned to that CSI during Mastercard Product Graduation account registration are graduated to the same product code. If an account assigned to a given CSI is not graduated to the same product code associated with the CSI's limits, Stand-In will not apply CSIs limits. Stand-In will apply issuer-defined limits, which could include account range limits for the graduated product or ICA level limits. If the issuer has not established these other limits, the Stand-In System will apply the Mastercard default limits for the graduated product.

Issuers can establish CSIs only for product-graduated accounts. To apply a CSI set of Stand-In limits, the transaction must be identified as eligible for Product Graduation and have an assigned CSI.

Mastercard provides the Stand-In Processing Transaction Category Code Global Parameters (Form 041g) available on Mastercard Connect for issuer defined limits.

Issuers will be able to define their own unique identifier (an-7) for each CSI they establish in DE 120 (Record Data) for MCC108. This field is optional. Issuers will populate this field with the unique identifier they have associated with a specific CSI to assign the CSI to the cardholder account in the file maintenance request. If issuers do not populate this field with a CSI value, it must be populated with spaces.

The following examples demonstrate how the Stand-In System determines the appropriate limits for a product graduated account:

- If the issuer has registered the graduated account with a CSI, the Stand-In System will use the unique Stand-In limits defined by the issuer for the given CSI.

- If the issuer has not registered the graduated account with a CSI, and the product associated with the primary account number (PAN) does not match the product associated with the authorization account range, Stand-In will apply issuer-defined limits, which could include account range limits for the graduated product or ICA level limits. If the issuer has not established these other limits, Stand-In will apply the Mastercard default limits for the graduated product.

### X-Code Processing

If the product code in DE 63, subfield 1 is different than the product code assigned to the authorization account range, the X-Code System will apply product code limits using the product code in DE 63, subfield 1.

## 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.

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

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 61 (Point-of-Service [POS] Data), M subfield 10 (Cardholder-Activated Terminal Level Indicator)		•	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.

<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 18 (Merchant Type)	M	•	M	Must contain value 6539 = Funding Transaction, Excluding MoneySend
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	U = Unique
DE 61 (Point-of-Service [POS] Data), M subfield 10 (Cardholder-Activated Terminal Level Indicator)		•	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.

<b>WHEN the acquirer...</b>	<b>THEN the Authorization Platform...</b>
Sends an Authorization Request/0100, Authorization Advice/0120, or Reversal Request/0400 message containing DE 18 (Merchant Type), value 6539 (Funding Transaction, Excluding MoneySend)	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.

Data Element	Org	Sys	Dst	Values/Comments
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

---

<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	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
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

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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
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.
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.

## Authorization and Preauthorization Processing Standards

The following standards are in effect for authorizations initiated by card acceptors in all regions, unless stated otherwise. Preauthorization volumes are expected to continue to grow at steady rates in the near future, fueled by continued growth of international travel and e-commerce.

**NOTE: All authorizations initiated by card acceptors in the Asia/Pacific, Europe, and Middle East/Africa regions must clearly be distinguished as a final authorization or a preauthorization. Authorizations initiated by card acceptors in all other regions must be distinguished as a preauthorization, final authorization, or undefined authorization.**

For additional detail on Authorization and Preauthorization Processing Standards refer to the *Authorization Manual*.

## Rule Improvements

The following six rule improvements for authorization and preauthorization processing are currently in effect:

- Authorizations must be reversed within 24 hours of a transaction cancellation or of a finalization of the transaction for an amount lower than the authorized amount.
- Merchants must inform the cardholder of the amount to be authorized when the Mastercard authorization request is for an estimated amount and must obtain the cardholder's consent before processing the preauthorization request.
- Transactions no longer benefit from the 15/20 percent tolerance between authorization and clearing (except for card-not-present based tipping in the U.S. region for MCC 5812 Eating Places, Restaurants and MCC 5814 Fast Food Restaurants; and signature-based tipping, where the 20 percent tolerance remains applicable).
- The issuer chargeback protection period is redefined, and its duration is limited to a maximum. The period now starts counting as of the authorization date. Its duration is limited to a maximum of 30 calendar days for Mastercard and Debit Mastercard authorizations properly identified as preauthorizations, and seven calendar days for all other Mastercard and Debit Mastercard authorizations.
- Financial authorizations may be coded as preauthorizations, final authorizations, or undefined authorizations, except in Asia/Pacific, Europe, and Middle East/Africa where financial authorizations must be coded as final authorizations or preauthorizations.
- Use of incremental preauthorizations is applicable for all merchant types.

For details on Incremental Preauthorization, refer to the separate section Incremental Preauthorization Standards in this chapter of this manual.

## Final Authorization Message Processing Standard

Final authorizations not meeting the seven calendar day clearing requirement will be flagged as non-compliant. Non-compliant transactions are included in the Authorization Processing Integrity Acquirer Detail Report (AB605010-AA). A fee for non-compliance may be assessed in regions where non-compliance assessments are already in effect.

Undefined authorizations not meeting the seven calendar day clearing requirement will be flagged as non-compliant. Non-compliant transactions are included in the Authorization Processing Integrity Acquirer Detail Report (AB605010-AA). A fee for non-compliance may be assessed in regions where non-compliance assessments are already in effect.

## Authorization Processing Integrity Acquirer Detail Reporting

The Authorization Processing Integrity Acquirer Detail Report for Dual Message System (Authorization) acquirers enables enhanced merchant reporting of the processing integrity fees. The report provides acquirers with detailed transaction activity for each customer ID/ICA number identifying authorizations that were assessed a processing integrity fee. Acquirers may optionally choose to receive this report.

Mastercard generates the report weekly. The report is delivered each Monday at 18:30 (St. Louis, Missouri, USA time).

The report is available via bulk file in data or image file format. The image file is also available via Mastercard Connect™ eService Online Reporting.

**NOTE: There is a size restriction applicable to any eService report; therefore, if it is likely to be large (in excess of 350,000 lines), delivery via bulk is recommended.**

- Report ID: AB605010-AA—Authorization Processing Integrity Acquirer Detail Report (image file format)
  - Bulk ID: T852
  - eService

**NOTE: If a subscribing acquirer has no non-compliant authorizations to report within a billing period, the image format report (AB605010-AA) is not generated.**

- Report ID: AB605010-FF—Authorization Processing Integrity Acquirer Detail Data File (data file format)
  - Bulk ID: TKR8

**NOTE: If a subscribing acquirer has no non-compliant authorizations to report on a given day, the data file format report (AB605010-FF) will be generated and include a trailer record with a record count of zero.**

Acquirers can request to receive the report by contacting Global Customer Service.

For more information about the Authorization Processing Integrity Acquirer Detail Report and Data File refer to the *Authorization Manual*.

## Reversal Requirements

Acquirers must ensure that their merchants submit a reversal message to the issuer within 24 hours of the cancellation of a previously authorized transaction or of the finalization of a transaction with a lower amount than previously approved. The reversal may be a full or partial reversal, as appropriate. In the case of finalization of a transaction with a lower amount, a partial reversal is not required if the clearing message is submitted within 24 hours of the finalization of the transaction. Any authorized amount not reversed must correspond to the Transaction Amount of DE 4 (Amount, Transaction). This requirement does not apply to card acceptor business code (MCC) 5542 (Fuel Dispenser, Automated) transactions, Mastercard contactless (formerly Mastercard® PayPass™) transit aggregated or transit debt

recovery transactions, or to preauthorizations or authorizations with an expired chargeback protection period.

Cancellation of a previously authorized transaction or finalization of the Transaction Amount should occur within no more than seven calendar days of the authorization date for undefined authorizations and within no more than 30 calendar days of the authorization date for preauthorization messages.

### **Requirement to Inform Cardholder of Preauthorization Amount**

For Mastercard transactions, merchants must inform the cardholder of the estimated amount for which preauthorization will be requested and must obtain the cardholder's consent before processing the preauthorization request. This requirement enables cardholders to more effectively manage their open-to-buy and addresses cardholders' and regulators' concerns with current preauthorization practices.

The information requirement is automatically met when the terminal displays the amount to be authorized or when the amount to be authorized corresponds to an amount otherwise approved by the cardholder as the final transaction amount.

The merchant may also use any appropriate and effective manner of its choice to inform the cardholder (for example, verbal communication, or appropriate and visible written signage near the terminal). The amount may be communicated as a precise currency amount (for example, EUR 250). Alternatively, the merchant can explain how the amount is calculated, using a simple-to-understand formula.

This requirement does not apply to preauthorizations of MCC 5542 transactions or to Post-Authorized Aggregated Mastercard Contactless Transactions.

### **Authorization Amount Tolerances**

Mastercard lodging, vehicle rental, and cruise lines transactions no longer benefit from the 15 percent tolerance between the authorized amount and the clearing amount for Mastercard transactions.

In addition, certain Mastercard transactions no longer benefit from the 20 percent tolerance between authorization and clearing for gratuities. Details follow.

Where these tolerances are eliminated, issuers must ensure that they no longer block the cardholder's account for any amount in excess of the approved amount. These rules changes enable a more accurate management of the card account's open-to-buy.

In certain scenarios, described as follows, the practice of including the gratuity or an estimated provision for incidentals directly into the amount to be authorized continues to be supported. Mastercard reminds acquirers of the prohibition on including amounts to cover loss, theft, or damage in the provision for incidentals.

The rule for amount tolerance between the authorization amount and clearing amount with respect to gratuities is applied as follows.

The transaction amount must not exceed the authorized amount for the purpose of adding a gratuity, and any gratuity must be included in the authorization request if:

- The transaction is a card-not-present transaction or a contactless transaction; or
- The transaction is a Chip/PIN transaction.

**NOTE: An exception to this rule is allowed for card-not-present transactions when the merchant is located in the United States region identified with MCC 5812 (Eating Places, Restaurants) or MCC 5814 (Fast Food Restaurants).**

When a preauthorization or, where permitted, an undefined authorization is obtained, the transaction amount may exceed the authorized amount by 20 percent for the purpose of adding a gratuity if:

- The transaction is a key-entered or magnetic stripe transaction; or
- The transaction is a Chip transaction completed with signature or no cardholder verification method (CVM).

### **Time Limit for Payment Guarantee Related to Authorization**

The issuer payment guarantee period is redefined and its duration is limited to a maximum period counting from the authorization or preauthorization date. This maximum period is 30 calendar days for Mastercard authorizations properly coded as preauthorizations and is seven calendar days for all other Mastercard authorizations and for all Maestro and Cirrus authorizations and preauthorizations. This rule does not require issuers to hold the approved amount on the cardholder's account for seven or 30 calendar days; only limits the maximum duration of any such hold to a maximum duration of seven or 30 calendar days.

Transactions presented for clearing after the payment guarantee period has expired can be charged back by the issuer under reason code 4808 (Authorization-Related Chargeback) if the card account is permanently closed (Europe region issuers) or statused (issuers in all other regions). This chargeback right is available to issuers in all regions.

At the latest when the payment guarantee period expires, issuers must release any block they may have placed on the cardholder's account in relation to the authorization.

This rule change clearly defines the issuer payment guarantee exposure period for all transaction scenarios and limits the maximum period of issuer exposure.

The expiry of the payment guarantee does not affect other types of chargeback rights. For example, a transaction cannot be charged back under reason codes 4837 (No Cardholder Authorization) or 4863 (Cardholder Does Not Recognize—Potential Fraud) just because the transaction presentment was made after the payment guarantee has expired. Acquirer-financed installment billing transactions are exempt from the Mastercard rules providing for expiry of the payment guarantee. When the full transaction amount has been authorized, the merchant must be able to submit the corresponding installments according to the agreed payment schedule, which may be longer than 30 calendar days.

### **Authorization Chargeback Protection Period Extension Request**

In support of the time limit for chargeback protection related to Dual Message System authorizations, Mastercard offers an Authorization Chargeback Protection Period Extension

Request for use by Dual Message System acquirers, which is a non-financial (zero amount) incremental preauthorization request/0100 message.

For details on Authorization Chargeback Protection Period Extension Request, including Authorization Platform edits, refer to the separate section on Incremental Preauthorization Standards in this chapter of this manual, or to the *Authorization Manual*.

### **Data Integrity**

To support the gradual transition of Asia/Pacific, Canada, Latin America and the Caribbean, and United States region merchants and acquirers to the new message coding standards, Mastercard has implemented two new data integrity monitoring edits to support the transition of message coding of authorizations from undefined to preauthorization or final authorization for authorization transactions processed on the Mastercard Network. Support of the new message coding standards provides issuers the opportunity to apply different processing or cardholder messaging to different types of authorizations. Data integrity monitoring and reporting will begin on 1 June 2017 while standard data integrity non-compliance assessments will begin on 1 November 2017. Customers wanting to receive non-compliance notifications and view reporting must be registered for Data Integrity Online through Mastercard Connect™. Refer to the *Data Integrity Program* manual for additional information.

**NOTE: Acquirers in the Europe and Middle East/Africa regions are not impacted by the new data integrity programs and non-compliance assessments.**

### **Preauthorization Message Data Integrity**

The first data integrity edit will help ensure that not more than 25 percent of an acquirer's total approved financial authorizations, per child ICA, per month are coded as preauthorization unless there is a particular merchant or market need to do so. This program will help ensure that an acquirer does not start coding all authorizations as preauthorization in order to take advantage of the extended chargeback protection period.

The following types of transactions are excluded from the compliance validation process.

- Private Label transactions and transactions of card brands other than Mastercard (including Debit Mastercard), Maestro, and Cirrus
- Transactions that are approved offline
- Installment transactions
- Incremental authorizations
- Cross-border transactions
- e-commerce (POS PAN Entry, DE 22 subfield 1 = 81)
- Merchant Category exclusions (MCC, DE 18): 5542 (AFD), 3000–3350 (Airlines), 3351–3500 (Rental Car), 3501–3999 (Hotels), 7512 (Generic Car Rental), 4511 (Generic Airline), 7011 (Generic Hotels), MCCs 5812, 5813, 5814, 7230 (Gratuity categories)

### **Undefined Authorization Data Integrity**

The second data integrity edit will help ensure that for acquirers that process at least 100,000 approved financial domestic transactions on the Mastercard Network that not more than 50 percent of an acquirer's total domestic transaction authorizations, per ICA, per month remain coded as undefined. This program will help ensure that acquirers make the overall transition of coding authorizations as either preauthorization or final authorization for their domestic transaction activity.

The focus on domestic transactions in this edit is due to the fact that these transactions, unlike cross-border transactions, do not require currency conversion, which may result in a difference between the authorized and cleared cardholder billing amount that an issuer may use to manage cardholder balances.

The following types of transactions are excluded from the compliance validation process.

- Private Label transactions and transactions of card brands other than Mastercard (including Debit Mastercard), Maestro, and Cirrus
- Transactions that are approved offline
- Installment transactions
- Cross-border transactions

#### **Assessments for Not Reversed or Cleared Undefined Authorization and Preauthorization Processing Integrity Programs in the Asia/Pacific, Canada, Latin America and the Caribbean, and United States Regions**

Effective May 2017, acquirers in the Asia/Pacific, Canada, Latin America and the Caribbean, and United States regions will be subject to a processing integrity fee under the processing integrity programs and non-compliance assessments for Not Reversed or Cleared Undefined Authorization and Preauthorization. The fee will be applied for each approved authorization that is not cleared or fully reversed by an acquirer within 30 calendar days of the authorization date for preauthorizations and within seven calendar days of the authorization date for undefined financial authorizations.

Acquirers in the Europe region are not impacted by the processing integrity programs and non-compliance assessments for Not Reversed or Cleared Undefined Authorization and Preauthorization.

#### **Assessments for Preauthorization Transaction Fee and Final Authorization, Undefined Authorization, and Preauthorization Processing Integrity Programs in the Middle East/Africa Region**

Effective May 2017, acquirers in the Middle East/Africa region will be subject to processing integrity fee assessments for non-compliant final authorizations, undefined authorizations, and preauthorizations.

Starting with the billing invoice dated 8 January 2017, acquirers in the Middle East/Africa region will be impacted by a new preauthorization transaction fee. Starting with the billing invoice dated 28 May 2017, acquirers will be impacted by assessments for three processing integrity programs: Final Authorizations Not Meeting Requirement, Undefined Authorizations

With and Without Final Authorization Characteristics, and not reversed or cleared preauthorizations.

### Frequently Asked Questions on Authorization and Preauthorization Rules

#### Question: How should installment payment authorization messages be coded?

**Answer:**

##### ***Issuer-financed installment transactions:***

Acquirers submitting issuer-financed installment transactions should consider coding authorizations as **Final** if the authorization can be presented for clearing within seven calendar days of the authorization date and for the amount and currency authorized.

##### ***Merchant-financed and Acquirer-financed installment transactions:***

Acquirers submitting merchant-financed or acquirer-financed installment transactions should consider coding authorizations as **Undefined** if the total installment amount is known and the first installment can be presented for clearing within seven calendar days of the authorization date.

Acquirers submitting merchant-financed or acquirer-financed installment transactions should consider coding authorizations as **Preauthorization** if the installment amount is an estimate, or the first installment requires more than seven calendar days from the authorization date to present for clearing.

## 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 Global Customer Service 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.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 18 (Merchant Type)	M	•	M	MCC must be one of the following values: 6010 (Member Financial Institution—Manual Cash Disbursements) 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	
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

---

IF...	THEN the Authorization Platform...
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
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.

---

IF...	THEN...
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 System 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.

Acquirers in the U.S. region must support POS balance inquiry transaction type and functionality for all prepaid Mastercard credit and Debit Mastercard card account ranges.

Prepaid card issuers in the U.S. region must support online POS balance inquiries for all prepaid Mastercard credit and Debit Mastercard account ranges.

Issuer participation in POS balance inquiry is optional. To request participation, issuers must submit the *Point-of-Sale (POS) Balance Inquiry Participation Request Form* (Form 771) to Global Customer Service.

### 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.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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.

### **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).

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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.

<b>IF...</b>	<b>THEN the Authorization Platform...</b>
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).

IF...	THEN the Authorization Platform...
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, 10, 80, 82, 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—POS Balance Inquiry message  Except  If DE 22, subfield 1 = 10 or 81	Returns the Authorization Request Response/0110 message containing:  DE 39 = 30  DE 44 = 035

**NOTE: This edit is exempt when DE 22, subfield 1 contains values 10 or 81.**

<b>IF...</b>	<b>THEN the Authorization Platform...</b>
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.

<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.

IF...	THEN...
The acquirer submits an Authorization Advice/0120—Acquirer-generated message containing DE 3 (Processing Code), value 30 (Balance Inquiry)	<p>The Authorization Platform will reject the message and forward the acquirer an Authorization Advice Response/0130 message containing:</p> <p>DE 39 = 30</p> <p>DE 44 = 003</p>

## 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 System 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

<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), subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), position 3 (UCAF Collection Indicator)	M	•	M	zero

## **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 Disbursements) 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 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

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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)
DE 48 (Additional Data—Private Use), subelement 48 (Mobile Remote Payments Program Indicators), subfield 2 (Mastercard Mobile Remote Payment Transaction Types)	M	•	M	Must be valid value 1–9.

## Chip-Specific Value Constraints

The Authorization Platform supports the authorization of chip transactions—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

Data Element	Requirements
DE 22	<p>For chip transactions, acquirers must provide value 05x.</p> <p>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.</p> <p>For a chip transaction where manual PAN entry was used as a fallback technology, acquirers may provide the value 79x.</p>
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	<p>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.</p> <p>For chip transactions, acquirers must provide DE 35 EMV tag 57 if the data object was present on the ICC.</p> <p>For a chip transaction where the magnetic stripe was used as a fallback technology, DE 35 must contain the actual Track 1 or Track 2 data from the magnetic stripe, or in the case of Maestro the actual Track 2 data because only Track 2 is present on the card.</p>
DE 52	DE 52 must be provided if the Cardholder verification method was Online PIN.

### 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 35	<p>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.</p> <p>For chip transactions, acquirers must provide DE 35 EMV tag 57 if the data object was present on the ICC.</p> <p>For a chip transaction where the magnetic stripe was used as a fallback technology, DE 35 must contain the actual Track 1 or Track 2 data from the magnetic stripe, or in the case of Maestro the actual Track 2 data because only Track 2 is present on the card.</p>

<b>Data Element</b>	<b>Requirements</b>
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 tag-length-value (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 PAN Entry Mode). DE 22, subfield 1 values indicate the method by which the PAN was entered.

<b>Values</b>	
3	= Contactless M/Chip (Proximity Chip)  Value 3 indicates that the terminal supports contactless M/Chip and contactless magnetic stripe transactions. The terminal may also support other card input types, including contact transactions.  DE 22, subfield 1 applicable values: <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)</li></ul>
4	= Contactless Magnetic Stripe (Proximity Chip) only  Value 4 indicates that the terminal supports contactless magnetic stripe transactions. The terminal may also support other card input types, including contact transactions.  DE 22, subfield 1 applicable value: <ul style="list-style-type: none"><li>• 91 (PAN auto-entry via contactless magnetic stripe)</li></ul>
5	= EMV specification (compatible chip reader) and magnetic stripe reader.  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>

---

### Values

---

8	=	EMV specification (compatible chip reader), 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>• 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 DE 22, subfield 1 applicable value: <ul style="list-style-type: none"><li>• 05 (PAN auto-entry via chip)</li></ul>

---

## Canada Region Debit Mastercard Merchant Acceptance

---

The Dual Message System (Authorization) allows the issuance of the Debit Mastercard® brand by Canada region issuers and allows Canada region merchants to accept domestically issued Debit Mastercard cards.

The Authorization Platform prevents the accidental acceptance of Canada region-issued Debit Mastercard cards and allows issuers to issue Debit Mastercard cards either as stand-alone cards or as cards bearing other acceptance marks.

### Acquirers

Canada region acquirers that have established an agreement with their merchants to process Debit Mastercard transactions must support DE 48 (Additional Data—Private Use), subelement 18 (Service Parameters), subfield 01 (Canada Domestic Indicator) and DE 39 (Response Code), value 81 (Domestic Debit Transaction Not Allowed).

For merchants that accept Canada region-issued Debit Mastercard cards, acquirers in Canada must:

- Include DE 48, subelement 18 (Service Parameters) in the Authorization Request/0100 message indicating the merchant has agreed to process Debit Mastercard.
- Support DE 39, response code value 81 (Domestic Debit Transaction Not Allowed) in the Authorization Request Response/0110 message indicating a transaction has been declined.

## Issuers

Canada region issuers that choose to issue new Debit Mastercard cards must notify Mastercard Customer Implementation Services (CIS) if the account ranges bear other acceptance marks.

Issuers in Canada must:

- Notify Customer Implementation Services (CIS):
  - When the Debit Mastercard BIN being implemented will bear other acceptance marks.
  - The point-of-interaction (POI) environments (face-to-face or non-face-to-face) in which other acceptance marks will exist.
- Ensure Debit Mastercard cards comply with the Canada Region chapter in *Mastercard Rules*.
- Immediately notify Mastercard through CIS of any change in the account ranges affecting compliance with Mastercard Rules.

## Authorization Platform Edits

The Authorization Platform will perform the following edits on transactions that are acquired in Canada and on a card issued in Canada and the acceptance brand of that card is Debit Mastercard.

For transactions with a Canada region-issued Debit Mastercard card that bears other acceptance marks with international only Debit Mastercard routing.

WHEN...	THEN...the Authorization Platform
The country code of the merchant in DE 61 (Point-of-Service [POS] Data), subfield 13 (POS Country Code) is the same as the issuer	Rejects the transaction where DE 39 (Response Code) = 81 (Domestic Debit Tran Not Allowed).

For transactions with a Canada region-issued Debit Mastercard card bearing other acceptance marks with only domestic face-to-face functionality for the other acceptance marks on the card.

<b>WHEN...</b>	<b>THEN...the Authorization Platform</b>
<ul style="list-style-type: none"> <li>The country code of the merchant in DE 61 (Point-of-Service [POS] Data), subfield 13 (POS Country Code) is the same as the issuer</li> <li>DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) is value 00 (Purchase), 09 (Purchase with Cash Back), or 28 (Payment Transaction)</li> <li>DE 61, subfield 4 (POS Cardholder Presence) is value 0 (Cardholder present) or value 1 (Cardholder not present, unspecified)</li> </ul>	Rejects the transaction where DE 39 (Response Code) = 81 (Domestic Debit Tran Not Allowed).

For transactions with a Canada region-issued Debit Mastercard card bearing other acceptance marks with domestic non-face-to-face functionality for the other acceptance marks on the card.

<b>WHEN...</b>	<b>THEN...the Authorization Platform</b>
<ul style="list-style-type: none"> <li>The country code of the merchant in DE 61 (Point-of-Service [POS] Data), subfield 13 (POS Country Code) is the same as the issuer</li> <li>DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) is value 00 (Purchase), 09 (Purchase with Cash Back), or 28 (Payment Transaction)</li> <li>DE 61, subfield 4 (POS Cardholder Presence) is value 2 (Mail/facsimile order), 3 (Phone/ARU order), 4 (Standing order/recurring transactions), or 5 (Electronic order [home PC, Internet, mobile phone, PDA])</li> <li>DE 48 (Additional Data—Private Use), subelement 18 (Service Parameters), subfield 1 (Canada Domestic Indicator) is not present or is value other than Y</li> </ul>	Rejects the transaction where DE 39 (Response Code) = 81 (Domestic Debit Tran Not Allowed).

For transactions with a Canada region-issued Debit Mastercard card not containing other acceptance marks.

WHEN...	THEN...the Authorization Platform
<ul style="list-style-type: none"><li>The country code of the merchant in DE 61 (Point-of-Service [POS] Data), subfield 13 (POS Country Code) is the same as the issuer</li><li>DE 48 (Additional Data—Private Use), subelement 18 (Service Parameters), subfield 1 (Canada Domestic Indicator) is not present or is a value other than Y</li></ul>	Rejects the transaction where DE 39 (Response Code) = 81 (Domestic Debit Tran Not Allowed).

## Cardholder Authentication Service

Mastercard offers the capability to indicate the result of biometric authentication to global customers. The Cardholder Authentication Service is an optional service for issuers.

### Overview

To help reduce identity fraud, Mastercard has expanded the capability to indicate the result of biometric verification to global issuers participating in the Cardholder Authentication Service.

The authentication indicator (in association with Biometric Card solution) indicates that the cardholder:

- Is the user of the card; and
- Was present at the time of the transaction.

The Cardholder Authentication Service is an optional service that helps participating issuers reduce fraud and increase approvals through biometric verification of the cardholder's identity. With the Cardholder Authentication Service, participating issuers are notified when a transaction is successfully authenticated through the verification of a cardholder's biological trait—such as a thumbprint—with a biometric-enabled card.

### Data Requirements

Mastercard will populate the indicator in DE 48 (Additional Data—Private Use), subelement 17 (Authentication Indicator) based on the presence of the biometric authentication result values in DE 55 (Integrated Circuit Card [ICC] System-Related Data), subelement 9F10, CVR byte1, bit1 and byte2, bit2.

The biometric authentication result values available for DE 55, subelement 9F10, CVR byte1, bit1 are as follows:

- 0—Not successful
- 1—Successful

Mastercard will forward the biometric verification result indicators to the issuer in the following messages:

- Authorization Request/0100
- Authorization Advice/0120 (Acquirer-generated and System-generated)

Mastercard will only populate DE 48, subelement 17 with an authentication indicator if the biometric authentication is successful.

### **Acquirers**

Acquirers globally must support receiving DE 48, subelement 17 in the following authorization response messages:

- Authorization Request Response/0110
- Authorization Advice Response/0130—Issuer-generated (Responding to Acquirer-generated 0120)

### **Issuers**

In addition to the standard chip data validation processing for chip transactions, issuers that have registered for or are already participating in the Cardholder Authentication Service must verify DE 55, subelement 9F10, CVR byte1, bit1 and byte2, bit2 to use the final cardholder authentication result in DE 48, subelement 17 in the following messages:

- Authorization Request/0100
- Authorization Advice/0120 (Acquirer-generated and System-generated)

### **Authorization Platform Edits—Cardholder Authentication Service**

The Authorization Platform will perform the following system edits related to the Cardholder Authentication Service.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>An Account Status Inquiry Transaction for account ranges participating in the Cardholder Authentication Service - the Authorization Request/0100 message contains:</p> <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) setup for Type 1 Authentication Service, and</li> <li>• DE 4 (Amount, Transaction) has a value of zero, and</li> <li>• DE 23 (Card Sequence Number) contains a value of 01X, and</li> <li>• DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI]), and</li> <li>• DE 55 (Integrated Circuit Card [ICC] System-Related Data) is present and tag 9F10: <ul style="list-style-type: none"> <li>– CVR byte1, bit1 is present with a value other than 1 (successful), or</li> <li>– CVR byte2, bit2 is present with a value other than 1 (biometric).</li> </ul> </li> </ul>	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 05 (Do not honor), and</li> </ul> <p>Sends the issuer an Authorization Advice/0120 message with DE 60 (Advice Reason Code):</p> <ul style="list-style-type: none"> <li>• Subfield 1 (Advice Reason Code) value 160 (Authentication Advice to Issuer), and</li> <li>• Subfield 2 (Advice Detail Code) value 0078 (M/ Chip Biometric Data not present)</li> </ul>
<p>An Account Status Inquiry Transaction for account ranges participating in the Cardholder Authentication Service - the Authorization Advice/0120—Acquirer-generated message contains:</p> <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) setup for Type 1 Authentication Service, and</li> <li>• DE 4 (Amount, Transaction) has a value of zero, and</li> <li>• DE 23 (Card Sequence Number) contains a value of 01X (X can be any number from 0 to 9 inclusive), and</li> <li>• DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI]), and</li> <li>• DE 55 (Integrated Circuit Card [ICC] System-Related Data) is present and tag 9F10: <ul style="list-style-type: none"> <li>– CVR byte1, bit1 is present with a value other than 1 (successful), or</li> <li>– CVR byte2, bit2 is present with a value other than 1 (biometric).</li> </ul> </li> </ul>	<p>Sends the acquirer an Authorization Advice Response/0130 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format Error), and</li> <li>• DE 44 (Additional Response Data) = 055 (indicating the data element in error)</li> </ul>

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
An Account Status Inquiry Transaction for account ranges participating in the Cardholder Authentication Service - the Authorization Request/0100 message contains: <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) setup for Type 2 Authentication Service, and</li> <li>• DE 4 (Amount, Transaction) has a value of zero, and</li> <li>• DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI]), and</li> <li>• DE 55 (Integrated Circuit Card [ICC] System-Related Data) is present and tag 9F10: <ul style="list-style-type: none"> <li>– CVR byte1, bit1 is present with a value other than 1 (successful), or</li> <li>– CVR byte2, bit2 is present with a value other than 1 (biometric).</li> </ul> </li> </ul>	Sends the acquirer an Authorization Request Response/0110 message where: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 05 (Do not honor), and</li> </ul> Sends the issuer an Authorization Advice/0120 message with DE 60 (Advice Reason Code): <ul style="list-style-type: none"> <li>• Subfield 1 (Advice Reason Code) value 160 (Authentication Advice to Issuer), and</li> <li>• Subfield 2 (Advice Detail Code) value 0078 (M/ Chip Biometric Data not present)</li> </ul>
An Account Status Inquiry Transaction for account ranges participating in the Cardholder Authentication Service - the Authorization Advice/0120—Acquirer-generated message contains: <ul style="list-style-type: none"> <li>• DE 2 (Primary Account Number [PAN]) setup for Type 2 Authentication Service, and</li> <li>• DE 4 (Amount, Transaction) has a value of zero, and</li> <li>• DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI]), and</li> <li>• DE 55 (Integrated Circuit Card [ICC] System-Related Data) is present and tag 9F10: <ul style="list-style-type: none"> <li>– CVR byte1, bit1 is present with a value other than 1 (successful), or</li> <li>– CVR byte2, bit2 is present with a value other than 1 (biometric).</li> </ul> </li> </ul>	Sends the acquirer an Authorization Advice Response/0130 message where: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format Error), and</li> <li>• DE 44 (Additional Response Data) = 055 (indicating the data element in error)</li> </ul>

---

## Card Validation Code 2

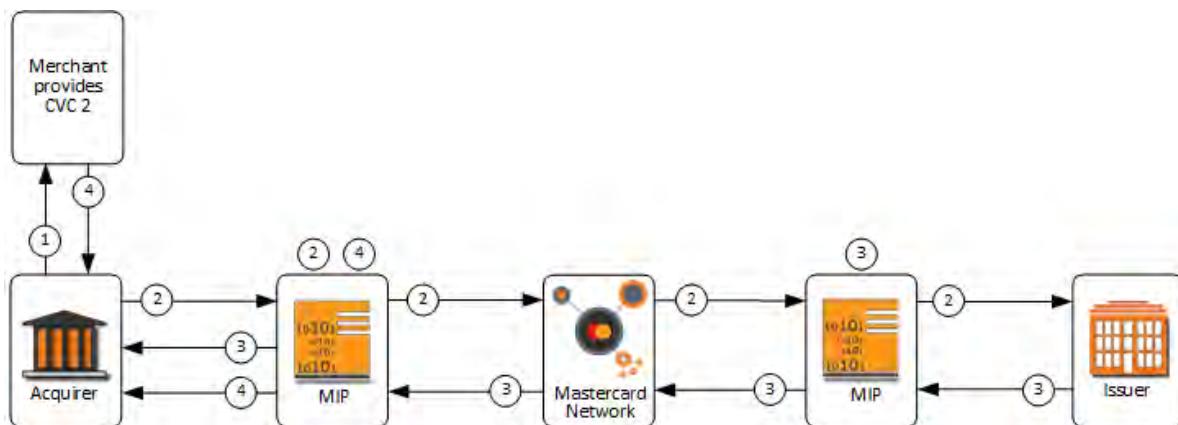
To comply with card validation code 2 (CVC 2) requirements, acquirers and issuers must process transactions according to the guidelines in this topic.

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

### Authorization Request/0100—CVC 2 Verified

Following are the stages of an Authorization Request/0100—CVC2 transaction when the value is verified.

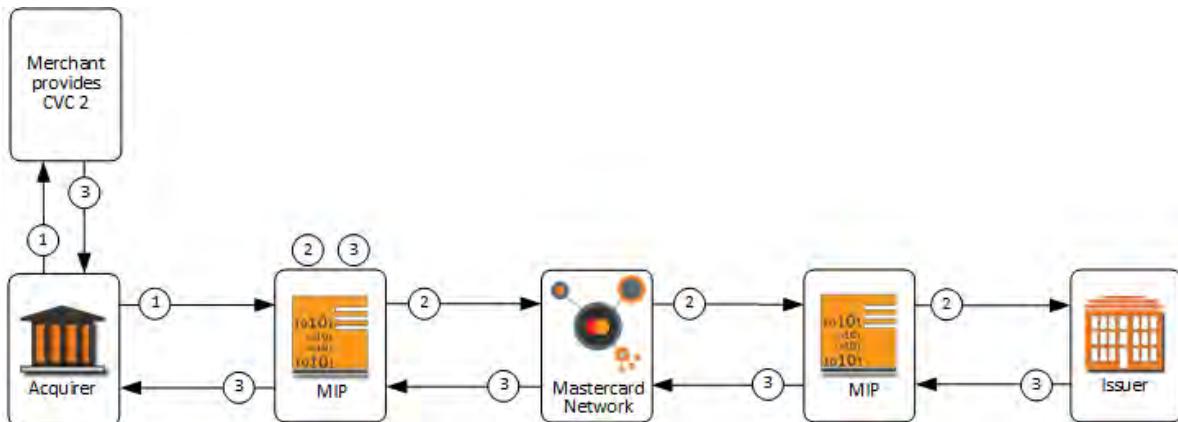


1. The merchant provides the CVC 2 value, and the acquirer generates an Authorization Request/0100 message with the CVC 2 value in DE 48, subelement 92.
2. The acquirer MIP forwards the Authorization Request/0100 message to the issuer.
3. After the issuer transmits the Authorization Request Response/0110 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... 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
No response or an invalid response	Approved	The acquirer MIP forwards the Authorization Request/0100 message to the alternate authorization service provider for processing.

### 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).



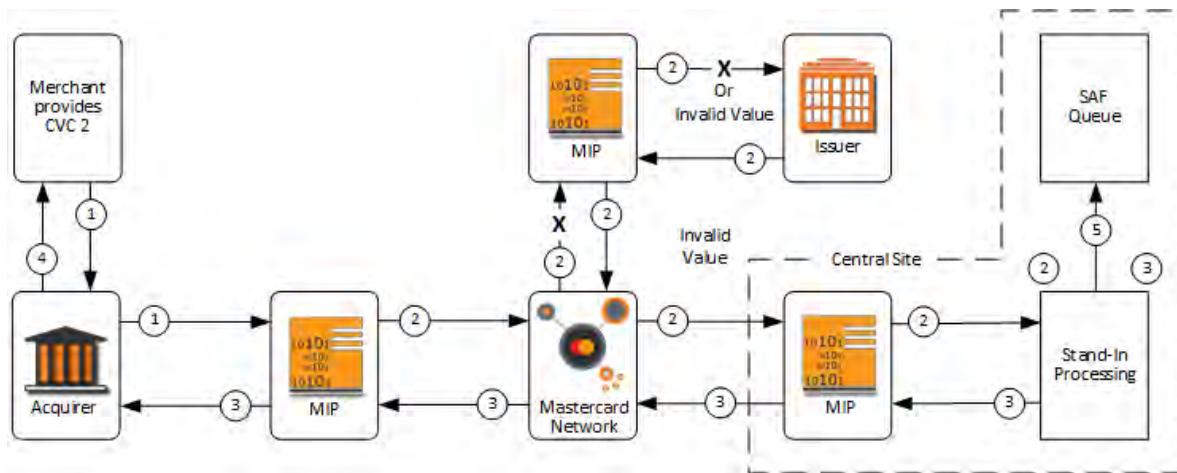
1. The merchant provides the CVC 2 value, and the acquirer generates an Authorization Request/0100 message with the CVC 2 value in DE 48, subelement 92.
2. The acquirer MIP forwards the Authorization Request/0100 message to the issuer, but the issuer is temporarily unable to receive the CVC value. The MIP forwards the Authorization Request/0100 message to the issuer without DE 48, subelement 92.

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.

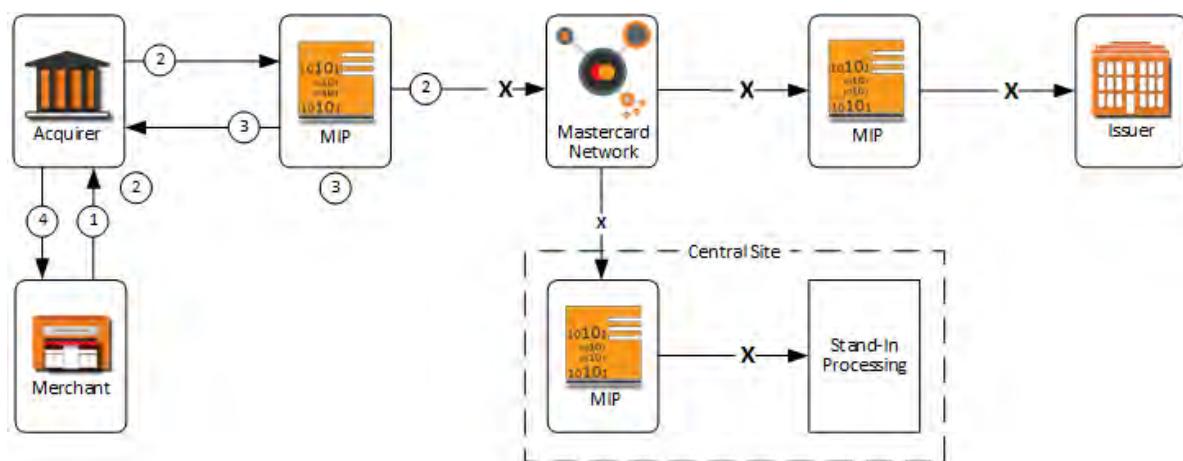
<b>WHEN the issuer is...</b>	<b>THEN the Authorization Platform...</b>
Temporarily unable to receive the CVC 2 value	Places value U (CVC 2 unverified—Mastercard use only) in DE 48, subelement 87 and forwards the Authorization Request Response/0110 message to the acquirer.

WHEN the issuer is...	THEN the Authorization Platform...
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.

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.

## CVC 2 DE 48 Structure

The following diagram illustrates DE 48 subelements related to CVC 2 transactions.

LLL "VAR"							
3 bytes	1 byte	2 bytes	2 bytes	3 bytes	2 bytes	2 bytes	1 byte
Total Data Element Length	TCC 92	SE ID	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	C	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)

Data Element	Org	Sys	Dst	Values/Comments
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.

## Authorization Platform Edits

The Authorization Platform performs the following edit for CVC 2.

---

**IF DE 48, subelement**

**87 (Card Validation**

**Code Result)**

**contains...**

**AND if the**

**transaction was...**

**THEN...**

**And Then...**

No response or an invalid response	Approved	Mastercard forwards the Authorization Request Response/0110 message to the acquirer with DE 48, subelement 87, value P (CVC 2 not processed—issuer temporarily unavailable)	The issuer will not receive an Authorization Response Negative Acknowledgement/0190 message
------------------------------------	----------	---	---

## 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 contactless 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.

Data Element	Org	Sys	Dst	Values/Comments
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

## Contactless CVC 3 Processing Service

Mastercard provides contactless processing services to assist issuers processing contactless 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:

- **Dynamic CVC 3 Pre-validation Service**—This is an optional, stand-alone service for issuers with contactless-enabled authorization systems that do not support dynamic CVC 3 validation. The Contactless Mapping Service may be used with the Dynamic CVC 3 Prevalidation 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 a mandated service for issuers with contactless-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.

The Contactless Mapping Service is for issuers with non-contactless-enabled authorization systems that are not able to support the processing of a separate contactless account number and the validation of dynamic CVC 3 value.

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, refer to 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 contactless 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 contactless 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	15 = Dynamic CVC 3 Pre-validation (with or without Contactless 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 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 CVC 3  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 contactless card that increments with every authorization request that occurs at a contactless-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 contactless 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 Contactless 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 (Application Transaction Counter File)

The MCC109 (Application Transaction Counter [ATC] file) contains a range of ATC values for a contactless account number/card sequence number/expiration date combination for contactless 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 (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 contactless 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 contactless ATC File.

Field ID and Name	Authorization Edit
1 Contactless Account Number	<ul style="list-style-type: none"><li>• Contactless account number must be present</li><li>• Contactless account number is numeric</li><li>• Contactless account number prefix is valid</li><li>• Contactless account number check digit is correct</li><li>• Contactless account number required in the Application Transaction Counter (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 ATC File (MCC109) for additions and inquiries</li></ul>
3 Contactless Account Expiration Date	<ul style="list-style-type: none"><li>• Contactless Account Expiration Date is valid YYMM format</li><li>• Contactless Account Expiration Date is required in the ATC File (MCC109) for additions and inquiries</li></ul>

Field ID and Name	Authorization Edit
4 Contactless Application Transaction Counter (ATC) Value	<ul style="list-style-type: none"><li>• Contactless ATC is numeric (may be zero)</li><li>• Contactless ATC is required in the 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, refer to 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> <li>• DE 48, subelement 71 with the appropriate values</li> <li>• DE 48, subelement 87, value E, P, or Y</li> <li>• DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code), value 115 (Transaction processed via MIP On-behalf Service Decision)</li> <li>• DE 60, subfield 2 (Advice Detail Code), one of the following values: <ul style="list-style-type: none"> <li>– 0042 (CVC 3 Unable to process)</li> <li>– 0043 (CVC 3 ATC outside allowed range)</li> <li>– 0044 (CVC 3 Invalid)</li> <li>– 0045 (CVC 3 Unpredictable number mismatch)</li> <li>– 0046 (CVC 3 ATC Replay)</li> </ul> </li> </ul>
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 contactless 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 Global Customer Service 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.

---

**IF DE 48, subelement 71,  
subfield 2 contains the value... THEN DE 60, subfield 2 will contain...**

---

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.

## Contactless Mapping Service for Contactless M/Chip and Contact M/Chip Transactions

---

The Contactless 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 Contactless 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 Contactless Mapping Service and that issue contactless 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.

## Contactless Mapping Service Processing of Contactless 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 Contactless Mapping Service transactions.

WHEN the message contains...	THEN the Authorization Platform...
DE 22, subfield 1, value 05 (PAN auto-entry via chip) and The Contactless Mapping Service was performed on the transaction	Changes the value in DE 22, subfield 1 from 05 to 06, indicating that the Contactless Mapping Service occurred.
DE 22, subfield 1, value 07 (PAN auto-entry via contactless M/Chip) and The Contactless Mapping Service was performed on the transaction	Changes the value in DE 22, subfield 1 from 07 to 08, indicating that the Contactless Mapping Service occurred.

The Contactless Mapping Service occurs on Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, and Reversal Request/0400 messages. The following example describes the Contactless 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 contactless M/Chip or contact M/Chip card eligible for the Contactless Mapping Service.

1. When a cardholder initiates an eligible contactless M/Chip or contact M/Chip transaction on a contactless M/Chip or contact M/Chip terminal, the contactless M/Chip PAN or contact M/Chip PAN is passed to the terminal.
2. The acquirer sends an Authorization Request/0100 message containing the contactless M/Chip PAN or contact M/Chip account number to the Authorization Platform.
3. The Authorization Platform maps the contactless 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 Contactless Mapping Service applied) or 06 (PAN auto-entry via chip Contactless Mapping Service applied)

- DE 23 (Card Sequence Number) containing the contactless 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 (Contactless Mapping Information) containing contactless M/Chip or contact M/Chip PAN information
  - DE 48, subelement 71 (On-behalf Services), identifying the Contactless 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 contactless M/Chip or contact M/Chip account number and places the cardholder's PAN in DE 48, subelement 33, and then sends the contactless M/Chip or contact M/Chip account number in DE 2 to the acquirer.
  6. The acquirer forwards the contactless M/Chip or contact M/Chip account number and other authorization response information to the contactless terminal.

The Contactless Mapping Service for contactless 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 Contactless 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 contactless M/Chip and contact M/Chip transactions that are eligible for the Contactless Mapping Service.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The expiration date in DE 14, DE 35, or DE 45 (whichever data element is first to contain the expiration date) is expired</p> <p>and</p> <p>DE 22, subfield 1 is value 05 or 07</p> <p>and</p> <p>The account is part of an account range that participates in the Contactless Mapping Service</p>	<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).</p>

## Cross-Border Fee Manager Service

The Cross-Border Fee Manager service is an optional service that gives issuers the flexibility to set markup rates for both currency-conversion and cross-border transactions, taking into account a variety of parameters.

### Overview

Through this service, Mastercard offers three different methods (Currency Conversion Method, Cross Border Cost Method, and Cross Border Flex Method) with which issuers may add a markup in DE 6 (Amount, Cardholder Billing) based on the following parameters:

- Account range for Mastercard®, Debit Mastercard®, Maestro®, and Cirrus® acceptance brands
- Processing code
- Region differentiation
- Card-present and card-not-present

Participating issuers may implement any combination of the following methods and add the associated fees to the total cardholder billing amount:

- Currency Conversion Method—Allows issuers to charge cardholders a percentage rate, fixed amount, or both by applying a markup to currency-converted transactions that may be further filtered by setup parameters.
- Cross Border Cost Method—Allows issuers to charge cardholders a percentage rate based on their transaction amount by applying markup to cross-border transactions that may be further filtered by setup parameters.
- Cross Border Flex Method—Allows issuers to charge cardholders an additional percentage rate, fixed amount, or both by applying a markup to cross-border transactions that may be further filtered by setup parameters.

### Enrollment

Issuers that want to participate in the Cross-Border Fee Manager service must contact their Mastercard implementation representative.

**NOTE: Issuers may only participate in the Currency Conversion Method, Cross Border Cost Method, and the Cross Border Flex Method where permitted by local regulations.**

## 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).

Customers that want to receive the currency conversion settlement amount-related data elements must complete the *Currency Conversion Parameters-Acquirer Issuer Form*. Please contact a Global Customer Service 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

<b>DE</b>	<b>Acquirer Sends</b>	<b>Issuer Receives</b>	<b>Issuer Returns</b>	<b>Acquirer Receives</b>
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
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

<b>DE</b>	<b>Acquirer Sends</b>	<b>Issuer Receives</b>	<b>Issuer Returns</b>	<b>Acquirer Receives</b>
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 (not an echo of what the acquirer sent)	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 amount-related data elements  DE 95, subfield 3 in issuer's cardholder billing currency  DE 95, subfield 4 zero-filled	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 amount-related data elements  DE 95, subfield 3 in issuer's cardholder billing currency  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			
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 MTIs in Authorization and Reversal messages.

<b>DE</b>	<b>Note</b>	<b>0110</b>	<b>0130</b>	<b>0410</b>
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
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
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.

<b>DE</b>	<b>Note</b>	<b>0110</b>	<b>0120</b>	<b>0130</b>	<b>0410</b>	<b>0430</b>
4	Acquirer's transaction currency	P	P	P	P	P
5	Always U.S. dollars	X	P	X	X	X

<b>DE</b>	<b>Note</b>	<b>0110</b>	<b>0120</b>	<b>0130</b>	<b>0410</b>	<b>0430</b>
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			
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

## 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.

IF...	THEN the Authorization Platform...
<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>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

---

<b>IF...</b>	<b>THEN the Authorization Platform...</b>
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
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

---

#### **Authorization Request Response/0110**

---

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
---	--

---

<b>IF...</b>	<b>THEN the Authorization Platform...</b>
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
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™)

## Best Practices for E-Commerce Transactions

Mastercard provides best practices for the management of electronic commerce (e-commerce) transactions.

The following sections provide recommended processing for authorization, authorization reversal, and clearing when dealing with estimated amounts and multi-item purchases where all items may or may not be delivered or are not delivered at the same time. These best practices are intended to help guide dual message acquirers, issuers, and processors in the usage of these transactions.

## Background

E-commerce authorizations are intended to reserve funds for subsequent clearing presentations once online purchases are dispatched (for example, physical items shipped or electronic content delivered). The following information may also be applied to mail order/telephone order (MOTO) (non-Travel and Entertainment [T&E]) transactions.

## Guiding Principles

The following is provided as guidance for e-commerce processing. Note that unless otherwise specified, these are best practices and not mandatory:

- An approved e-commerce authorization will have only one first presentment, unless multi-clearing processing is utilized with the proper message reason codes indicating that the issuer should maintain hold of funds for subsequent presentments.

**NOTE: As specified in the *Chargeback Guide*, airline ticket and installment purchases are allowed multiple first presentments against one approved authorization.**

- Mastercard recommends that merchants submit reversals as soon as an adjustment to the original authorization amount is known. For additional detail about reversals, refer to the separate sections on Authorization and Preauthorization Processing Standards, Incremental Preauthorization Standards, and Reversal Processing.

**NOTE: Merchants and acquirers must submit a full or partial reversal (as applicable) within seven calendar days of an original undefined authorization or final authorization request, and within 30 calendar days of an original preauthorization request. Merchants and acquirers must submit a full or partial reversal within 24 hours of transaction cancellation or of the transaction completing for an amount different from the authorized amount.**

**Refer to Authorization and Preauthorization Processing Standards, and Incremental Preauthorization Standards for more information about revised Standards for authorizations and preauthorizations.**

- Issuers must release any hold of funds once a clearing presentment has been matched (using the Trace ID in addition to other data elements) to the original e-commerce authorization, unless multi-clearing processing is utilized.
- If an e-commerce item ships late (beyond the authorization expiration date), merchants may submit a chargeback extension request message to avoid chargeback for message reason code 4808 (Authorization-Related Chargeback). If the issuer approves the extension request, the merchant will be protected from chargeback reason 4808 as long as the item ships prior to the new authorization expiration date.
- If an e-commerce item ships late and the merchant has not requested or did not receive approval of a chargeback period extension request and the authorization chargeback protection period had expired, the merchant must submit a new authorization for the item to be shipped to avoid chargeback message reason code 4808 (Authorization-Related Chargeback). The new authorization will take on the security characteristics of the original authorization within a dispute resolution.

**NOTE: The best practice for extending the payment guarantee and avoiding a chargeback is to submit an incremental preauthorization to refresh the authorization date. A zero amount (USD 0) can be used in the incremental preauthorization. Without Universal Cardholder Authentication Field (UCAF™) data present, a re-authorized transaction must be presented within clearing for non-UCAF interchange (as applicable by region).**

## Specific Scenarios for E-Commerce Transactions

Depending on the merchant's inventory system and the nature of the item being purchased online, an e-commerce transaction may be submitted as either a preauthorization or a final authorization by card acceptors globally.

For more information about preauthorization and final authorization usage requirements, refer to Authorization and Preauthorization Processing Standards, Incremental Preauthorization Standards, and the *Transaction Processing Rules*.

The following describes the recommended processing when dealing with estimated amounts and multi-item purchases where all items may or may not be delivered or are not delivered at the same time.

If...	Then...
The entire e-commerce purchase is canceled (for any reason)	Submit a full reversal.
The initial preauthorization is for an estimated amount based on anticipated sales tax, or estimated shipping weight	Submit partial reversal and present clearing if the effective amount is less than the preauthorization, or submit incremental preauthorization and present clearing if the effective amount is greater. (Merchant could also authorize and clear the difference separately, or just present clearing for the greater amount and risk possible issuer chargeback.)
One item within a multi-item purchase is canceled (customer cancellation or out-of-stock)	Submit a partial reversal and present clearing when the remaining items ship. Refer to the following section Alternate Processing—Canceling a Single Item.
The customer requests split shipment based on inventory availability, or e-commerce aggregator processes order through multiple suppliers	Refer to the following section E-Commerce Split or Partial Shipments.

## Alternate Processing—Canceling a Single Item

Issuers will release any hold of funds once a clearing presentation has been matched (using the Trace ID in addition to other data elements) to the original authorization. Accordingly, a merchant is not required to submit a partial reversal if the lower amount is processed by Mastercard clearing within 24 hours of finalization of the transaction—assuming multi-clearing processing is not utilized.

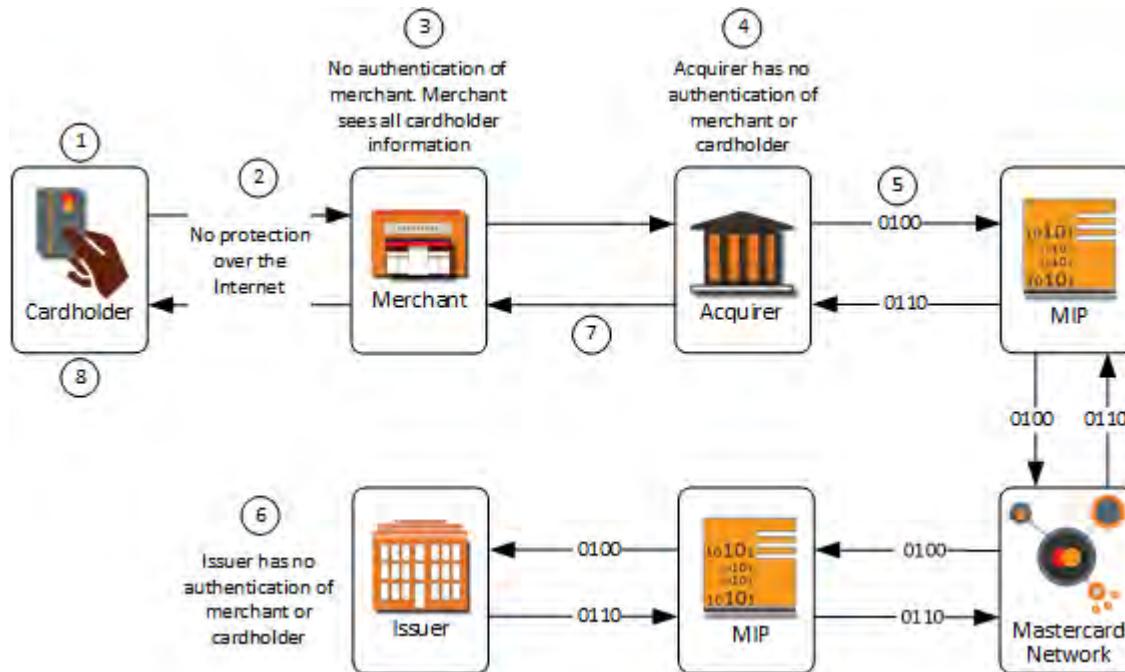
## E-Commerce Split or Partial Shipments

The following are options for managing e-commerce split or partial shipments.

Available Option	Comments
Utilize multi-clearing processing with the proper partial/final presentment message reason code.	This option is the best practice for processing split shipments due to fulfillment delays or multiple suppliers.
Submit partial reversal for unshipped items. Present clearing for shipped items. Separately re-authorize and clear as late items ship.	Merchant risks decline on re-authorization. (Refer to previous note about UCAF security/interchange for re-authorized transactions.)
Do not present clearing on a multi-item purchase until all items ship.	Merchant cash flow may be impacted due to item inventory delays.
Secure consumer permission to bill up front, ahead of the order shipment. Present clearing for entire order upon authorization.	Issuer inquiry or chargebacks could result if merchant billing terms and conditions are not understood.
Submit separate authorizations and clear as each item ships.	Each item is processed as a separate transaction.

## No Security Protocol

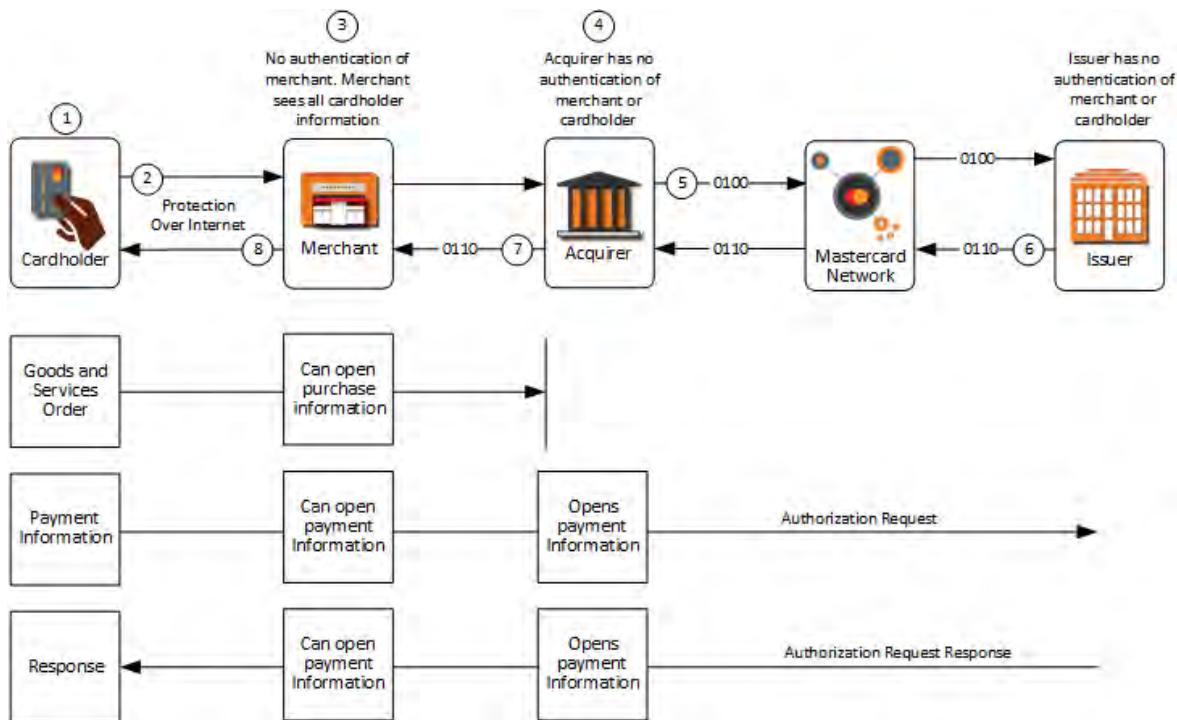
This message flow describes an Authorization Request/0100—Electronic Commerce transaction with no security protocol.



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:
  - 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).

**NOTE: An approved e-commerce authorization must only have one first presentment submitted for clearing unless the authorization is for airline tickets or installment purchases. In the case of airline tickets and installment purchases multiple first presentments against one approve authorization is allowed.**

### **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.

<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

<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	<p>Contains one of the following values:</p> <p>P = Payment Transaction</p> <p>T = Phone, Mail, or Electronic Commerce Order</p> <p>U = Unique</p> <p>X = Airline and Other Transportation Services (irrespective of the transaction origin is face to face or not)</p>
DE 48, subelement 40 (Electronic Commerce Merchant/Cardholder Certificate Serial Number [Visa Only]), subfield 1 (Merchant/Certificate Serial Number)	C	•	C	<p>DE 48 subelement 40 is not required for any Mastercard e-commerce programs.</p> <p>Merchant certificate serial number in binary format</p>
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	<p>Contains security level in positions 1 and 2 and UCAF collection indicator in position 3.</p> <p>Position 1 = Security Protocol</p> <p>Position 2 = Cardholder Authentication</p> <p>Position 3 = UCAF Collection Indicator</p>
DE 48, subelement 43 (Universal Cardholder Authentication) for Mastercard SecureCode issuer or cardholder generated authentication data	C	•	C	Authentication data generated by <i>SecureCode</i> -compliant solution.
DE 48, subelement 43 (Universal Cardholder Authentication) for static AAV program.	C	•	C	A static Accountholder Authentication Value (AAV) assigned by Mastercard for use with this Program.
DE 48, subelement 43 (Universal Cardholder Authentication) for 3-D Secure Electronic Commerce Verification Service (Visa and American Express)	C	•	C	<p>Position 1 (3-D Secure Electronic Commerce Transaction Indicator) 8 = Indicates Secure Electronic Commerce Transaction</p> <p>Position 2–21 (3-D Secure Electronic Commerce Cardholder Authentication Verification Value [CAVV]) = Cardholder Authentication Verification Value (CAVV)</p>

Data Element	Org	Sys	Dst	Values/Comments
DE 48, subelement 44 (Electronic Commerce Transaction Identifier [XID] [Visa and American Express])	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	<p>For a recurring payment arrangement in which the first payment is an electronic commerce transaction, use:</p> <p>4 = Standing order/recurring transactions (required for the first transaction and all subsequent transactions in a recurring payment arrangement)</p> <p>For all other e-commerce transactions use:</p> <p>5 = Electronic order (home PC, Internet, mobile phone, PDA)</p>
DE 61, subfield 7 (POS Transaction Status)	M	•	M	Must not contain value 2 (SecureCode Phone Order).
				<b>NOTE: An e-commerce transaction may be submitted as either a preauthorization (DE 61, subfield 7 value 4) or final authorization (DE 61, subfield 7, value 0 and DE 48, subelement 61, subfield 5, value 1) by card acceptors in the Europe region.</b>
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.

<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 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 and American Express])	CE	•	CE	Must be the same value as in the original Authorization Request/0100 message, if present. (Visa and American Express.)
DE 48, subelement 45 (Three-Domain (3-D) Secure Electronic Commerce Transaction Response Code [Visa and American Express])	C	•	C	Contains the Visa 3-D Secure CAVV Results Code, if present. (Visa and American Express).

## Authorization Platform Edits

Mastercard performs the following edits on Authorization Request/0100 messages for Mastercard Electronic Card transactions.

<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.

<b>WHEN...</b>	<b>THEN The Authorization Platform...</b>
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 = 0480nn (where nn is the subelement number)
DE 48, subelement 42, subfield 1, position 3 contains value 1 (UCAF data collection is supported by the merchant, and UCAF data should be available [DE 48, subelement 43 should be present for Mastercard SecureCode])	Forwards the UCAF™ data in DE 48, subelement 43, if present, to the issuer.

### **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.

Customers must perform AAV validation of Authorization Request/0100 messages, either via their own self-validation process or through the Mastercard SecureCode AAV Verification service.

All customers must participate in 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 a mandated 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 a mandated service.

For more information about *SecureCode*, including detailed transaction flows and participation requirements, refer to the *SecureCode Implementation Guides*.

## Static AAV

Several Mastercard programs enable enrolled merchants that have met specific qualification criteria, to accept Mastercard or Maestro 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.

These Mastercard programs are as follows:

- Maestro Recurring Payments Program
- Mastercard Utility Payment Program
- Maestro Low Risk Merchant Program

As part of these 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 Mastercard or Maestro e-commerce transactions that are processed under the Maestro Recurring Payments Program, the Mastercard Utility Payment Program, or the Maestro Low Risk Merchant Program. These on-behalf services will continue to be performed on Mastercard and 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.

Data Element	Org	Sys	Dst	Values/Comments
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

**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).**

## Gaming Payment Transactions

---

This section describes Gaming Payment Transaction processing in the Europe and Middle East/Africa (MEA) regions and in the United States region.

The Dual Message System (Authorization) supports Gaming Payment Transaction processing for the Mastercard and Maestro card brands in Europe and Mastercard card brands in Middle East/Africa region countries where the crediting of gambling winnings is permitted by law.

The Dual Message System (Authorization) also supports Gaming Payment Transaction processing for the Mastercard and Maestro brands in the United States Region to transfer lottery winnings to a card.

## Gaming Payment Transaction Processing in the Europe and Middle East/Africa Regions

The Dual Message System (Authorization) supports Gaming Payment Transactions in Authorization Request/0100 and Reversal Request/0400 messages for the Mastercard® and Maestro® card brands in the Europe and Mastercard card brands in Middle East/Africa (MEA) regions where online gaming and the crediting of gaming winnings on cards is permitted by law.

Acquirers submit their online Gaming Payment Transaction Authorization Request/0100 and Reversal Request/0400 messages with the following values:

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type), value 28 (Payment Transaction)
- In the Europe region, DE 4 (Amount, Transaction), maximum EUR 50,000. If an acquirer provides a transaction amount exceeding EUR 50,000 or its currency equivalent, the Authorization Platform will decline the request with DE 39 (Response Code), value 13 (Invalid amount).
- In the Middle East/Africa region, DE 4 (Amount, Transaction), maximum EUR 50,000. If an acquirer provides a transaction amount exceeding EUR 50,000 or its currency equivalent, the Authorization Platform will decline the request with DE 39 (Response Code), value 13 (Invalid amount).
- DE 18 (Merchant Type), MCC 7995 (Gambling Transactions)
- DE 22 (Point-of-Service [POS] Entry Mode), subfield 1, value 81 (PAN entry via electronic commerce)
- DE 48 (Additional Data—Private Use), TCC value P (Payment Transaction)
- DE 48, subelement 77, value C04 (Gaming Re-pay)

If an acquirer has not completed an implementation project to submit Gaming Payment Transactions and sends a Gaming Payment Transaction authorization request, the Authorization Platform declines the request with DE 39 (Response Code), value 58 (Transaction not permitted to acquirer or terminal).

Issuers may receive Gaming Payment Transactions if they are located in Europe and Middle East/Africa region countries where online gaming and crediting of gaming winnings on cards is permitted by law. For a list of these Europe region countries, refer to Rule 8.12.1 in Europe Region Rules of the *Mastercard Rules*. For a list of these Middle East/Africa region countries, refer to Payment Transactions and MoneySend Payment Transactions, MEA Region, of the *Transaction Processing Rules*. If an issuer's country is not one of the listed countries that allows gaming, the Authorization Platform declines the Gaming Payment Transaction request with DE 39 (Response Code), value 57 (Transaction not permitted to issuer/cardholder).

## **Alternate Processing**

Gaming Payment Transactions are routed to an alternate issuer host. Gaming Payment Transactions are not routed to the Stand-In System or X-Code System.

When there is either no alternate issuer host or no response from an alternate issuer host, the Authorization Platform will decline the transaction with DE 39 (Response Code), value 91 (Authorization System or issuer system inoperative).

## **For More Information**

For additional details about data requirements, refer to the *Mastercard Rules*.

### **Authorization Request/0100—Gaming Payment**

Following is a list of the data elements and values applicable to this message type for Gaming Payment Transactions in the Europe and Middle East/Africa (MEA) regions. 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	28 = Payment Transaction
DE 4 (Amount, Transaction)	M	•	M	Maximum amount EUR 50,000
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 (Funding/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 for Gaming Payment Transactions in the Europe and Middle East/Africa (MEA) regions. 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 50,000
DE 18 (Merchant Type)	M	•	M	Must contain value 7995 = Gambling Transaction

<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 (Funding/ Payment Transaction Type Indicator)	M	•	M	C04 = Gaming Re-pay

### **Authorization Platform Edits**

The following edits apply to Gaming Payment Transactions in the Europe and Middle East/Africa (MEA) regions.

<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 50,000	Sends the acquirer an Authorization Request Response/0110 or a Reversal Request Response/0410 message where:  DE 39 = 13 (Invalid amount)

## Gaming Payment Transaction Processing in the United States Region

The Authorization Platform supports Gaming Payment Transactions in Authorization Request/0100 and Reversal Request/0400 messages for the Mastercard and Maestro brands in the United States region to transfer lottery winnings to a card.

An acquirer in the United States region submits a Gaming Payment Transaction Authorization Request/0100 and Reversal Request/0400 message with the following values:

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type), value 28 (Payment Transaction)
- DE 4 (Amount, Transaction), maximum USD 10,000
- DE 18 (Merchant Type), MCC 7800 (Government-owned Lottery [U.S. Region Only])
- DE 48 (Additional Data—Private Use), TCC value P (Payment Transaction)
- DE 48, subelement 77, value C04 (Gaming Re-pay)

**NOTE: The Gaming Payment Transaction must not be processed as electronic commerce (e-commerce).**

An issuer in the United States region may receive Gaming Payment Transactions identified as described above.

## Alternate Processing

The Gaming Payment Transaction must not be routed to the Stand-In System or X-Code System. When a Gaming Payment Transaction identified using MCC 7800 is routed to:

- The Stand-In System, the Authorization Request/0100 message will be declined with DE 39 (Response Code), value 05 (Do Not Honor); or
- The X-Code System, the Authorization Request/0100 message will be declined with DE 39 (Response Code), value 01 (Refer to Card Issuer).

## ICCR Service

---

Issuers in the Europe region have the option to enroll in the Issuer Currency Conversion Rate (ICCR) service, which charges the cardholder an additional fee for transactions that require currency conversion.

### ICCR Service Overview

The Issuer Currency Conversion Rate (ICCR) is a parameter-based system that charges cardholders by applying a mark-up called ICCR in clearing.

Issuers in the Europe region can add this supplemental fee to a transaction amount when the transaction currency is different from the cardholder billing currency. This fee is listed under DE 6 (Amount, Cardholder Billing).

Issuers will be able to set their issuer currency conversion rate by account range, which will apply to First Presentment messages.

Issuers can receive daily audit report files of the clearing transactions where the ICCR was applied. A new bulk file type, Bulk File TN70 (On Request Report Data File Transfer Raw Format), which replaces bulk file type TAV8, supports the daily audit report files.

ICCR applies to POS and ATM transactions acquired worldwide.

In the dual message system, all payment transactions (processing code = 28) will be bypassed for ICCR.

## **ICCR Enrollment**

All issuers in the Europe region that choose to enroll in the ICCR service must submit the correct enrollment form.

The *ICCR Service Enrollment Form*, available on Mastercard Connect™, must be completed and submitted before issuers can participate in the ICCR service.

Forms should be submitted to the issuer's local customer delivery manager.

## **Incremental Preauthorization Standards**

---

Incremental Preauthorization provides a means to associate incremental preauthorizations to a single clearing presentment. It is a common practice for specific merchant categories (now available to all merchant categories) to submit incremental preauthorizations and settle those through a single clearing presentment. These standards provide a method for issuers, with certainty, to associate incremental preauthorizations to a single presentment providing them the means to more effectively manage cardholder open-to-buy balances.

**NOTE: All merchant types (MCCs) may use incremental preauthorizations.**

### **Incremental Preauthorization Transaction Processing**

The standards introduced apply to all merchant categories.

Each incremental preauthorization transaction associated with a single cardholder event must reference the original preauthorization. When incremental (additional) Authorization Request/0100 messages are sent for the same transaction, acquirers must include Customer Interface Specification data element (DE) 63 (Network Data) and DE 15 (Date, Settlement) information from the original Authorization Request Response/0110 message in DE 48 (Additional Data—Private Use), subelement 63 (Trace ID) as follows:

- Positions 1–3 = value from DE 63, subfield 1 (Financial Network Code)
- Positions 4–9 = value from DE 63, subfield 2 (Banknet Reference Number)
- Positions 10–13 = value from DE 15 (Date, Settlement)
- Positions 14–15 = blank filled

The First Presentment/1240 message submitted by the acquirer must include information from the original Authorization Request Response/0110 message in Integrated Product Message DE 63 (Transaction Life Cycle ID), subfield 2 (Trace ID). Upon receipt of the clearing record, the

issuer must release holds created by all authorizations properly related to the original preauthorization.

For details on increasing the effective duration of the chargeback protection period of authorizations originally coded as a preauthorization, refer to the following section on Authorization Chargeback Protection Period Extension Request.

## Guiding Principles

This section provides insight into the intent of the Incremental Preauthorization process. The following are an elaboration of the standards.

- The primary intent of an incremental preauthorization is to increase the amount of an original preauthorization. Issuers may contest the settled amount of the transaction using message reason code 4808 (Authorization-Related Chargeback) if the cleared amount exceeds the amount authorized. The authorized amount is equal to the cumulative amount of all authorizations (plus tolerance if applicable). The allowable tolerances are described in the *Chargeback Guide*. Additional information on message reason code 4808 (Authorization-Related Chargeback) chargebacks can be found in the *Chargeback Guide*.
- The original preauthorization is the reference. All attributes associated with the original are inherited by the incremental preauthorizations. The payment guarantee period of the aggregate transaction is 30 calendar days from the date of the last incremental preauthorization. Transactions that would have incremental preauthorizations will likely be submitted as preauthorizations. Any transaction submitted as a final authorization that has an incremental will be subject to a processing integrity fee.
- The usage of incremental preauthorizations is optional. Acquirers can, as an alternative, submit clearing records (presentments) for each individual authorization.
- Incremental preauthorizations are recognized for all MCCs.
- Transactions that may have incremental preauthorizations are recommended to be submitted as preauthorizations. Incremental preauthorizations must be coded as preauthorizations.

## Specific Scenarios

### Typical Usage

The following table depicts the flow of a typical incremental preauthorization. The merchant successfully completes an original preauthorization for 100, followed by an incremental preauthorization of 50. This total amount is then processed as a first presentment.

Message Type	DE 63 (Banknet Reference Number)	DE 15 (Settlement Date)	Trace ID (Authorization—DE 48, subelement 63) (Clearing—DE 63, subfield 2)	DE 4 (Amount, Transaction)
--------------	----------------------------------	-------------------------	---	----------------------------

---

Original Preauthorization (0100/0110) <sup>35</sup>	MCC123ABC	1105	N/A	100
Incremental Preauthorization (0100/0110) <sup>35</sup>	MCC456ABC	1106	MCC123ABC1105	50
First Presentment (1240–200)	N/A	N/A	MCC123ABC1105	150

---

### **Incremental Preauthorization Reversals**

Acquirers are encouraged to recognize the original preauthorization and all related incremental preauthorizations in aggregate in the event they need to reverse part or all of the transaction. The recommended method of submitting reversals is illustrated in the following table.

In the following scenario, the merchant successfully completes an original preauthorization for 100, followed by an incremental preauthorization of 50, but then wants to cancel the transaction.

---

Message Type	DE 63 (Banknet Reference Number)	DE 15 (Settlement Date)	Trace ID (Authorization —DE 48, subelement 63) (Clearing—DE 63, subfield 2)	DE 4 (Amount, Transaction)	DE 95 (Replacement Amount)
Original Preauthorization (0100/0110) <sup>35</sup>	MCC123ABC	1105	N/A	100	N/A
Incremental Preauthorization (0100/0110) <sup>35</sup>	MCC456ABC	1106	MCC123ABC1105 05	50	N/A

---

<sup>35</sup> The Authorization Request/0100 message to issuer, the Authorization Request Response/0110 message to acquirer.

Reversal (0400/0410) <sup>36</sup>	MCC789ABC	1106	MCC123ABC11 05	150	0
---------------------------------------	-----------	------	-------------------	-----	---

In the next scenario, the merchant successfully completes an original preauthorization for 100, followed by an incremental preauthorization of 50. The merchant then reduces the preauthorization by 10 using a partial reversal.

Message Type	DE 63 (Banknet Reference Number)	DE 15 (Settlement Date)	Trace ID (Authorization—DE 48, subelement 63) <b>(Clearing—DE 63, subfield 2)</b>	DE 4 (Amount, Transaction)	DE 95 (Replacement Amount)
Original Preauthorization (0100/0110) <sup>35</sup>	MCC123ABC	1105	N/A	100	N/A
Incremental Preauthorization (0100/0110) <sup>35</sup>	MCC456ABC	1106	MCC123ABC11 05	50	N/A
Reversal (0400/0410) <sup>36</sup>	MCC789ABC	1106	MCC123ABC11 05	150	140
Clearing (1240– 200)	N/A	N/A	MCC123ABC11 05	140	N/A

Acquirers are expected to send reversals once they become aware that an adjustment is necessary. An exception to this is if the acquirer will be processing the first presentment within 24 hours of knowing a reversal is necessary.

---

<sup>36</sup> In the Reversal transaction, DE 90 (Original Data Elements) will contain DE 11 (System Trace Audit Number [STAN]), DE 7 (Transmission Date and Time), DE 32 (Acquiring Institution ID Code), and DE 33 (Forwarding Institution ID Code) from the Authorization Request Response/0110 message that corresponds to the original preauthorization request. The Transaction Amount (DE 4) is recommended to contain 150, while the Replacement Amount (DE 95) is recommended to contain 0, indicating a full reversal.

## Guaranteed Reservations

Guaranteed reservations are common in the hotel, motel, vehicle rental, and cruise line industries. Guaranteed reservations are managed uniquely for each of these segments. The recommended practice for each of these is as follows:

- Vehicle Rental—An account status inquiry is issued at the time of the reservation to confirm the account is in good standing. No advance authorization is issued nor is any amount held or liability assumed for no-shows.
- Cruise Lines—Typically, cruise lines charge the entire amount of the cruise at the time of the reservation. Any charges incurred during the cruise are submitted as a new authorization with incremental preauthorizations as needed.
- Hotel Reservations—A hotel, motel, resort, or other lodging merchant participating in the Guaranteed Reservations service has the option of utilizing the rules in regards to the no-show policies. The cardholder is obligated to cancel a confirmed reservation before 18:00 at the hotel, motel, or resort (merchant's local time). If the cardholder fails to cancel the confirmed reservation, the merchant can charge the cardholder a no-show charge equal to one night's lodging. In this case, it is appropriate for the merchant to authorize and clear the amount that would be charged for one night's lodging if they so choose. Any amount above that would be a violation of Mastercard rules and be at risk for a chargeback.

For details on Authorization Chargeback Protection Period Extension Request, refer to the following section.

## Authorization Chargeback Protection Period Extension Request

In support of the time limit for chargeback protection related to Dual Message System authorizations, Mastercard provides an Authorization Chargeback Protection Period Extension Request for use by Dual Message System acquirers, which is a non-financial (zero amount) incremental preauthorization request/0100 message.

Authorizations originally coded as a preauthorization may require a longer chargeback protection period. To increase the effective duration of the chargeback protection period, the merchant may submit incremental preauthorization requests for either an additional amount or zero amount for the same transaction on later dates. Incremental preauthorizations for an additional amount may be used to increase the authorized amount held against the card account and to extend the chargeback protection period associated with the original preauthorization. Incremental preauthorizations for a zero amount may be used to extend only the chargeback protection period associated with the original preauthorization.

If the issuer declines the chargeback extension request and the original preauthorization subsequently expires, the acquirer must request a new authorization.

**NOTE: Each approved preauthorization has an extended payment guarantee period of 30 calendar days from the authorization approval date. The issuer payment guarantee period is limited to a maximum period counting from the authorization or preauthorization date. This maximum period is 30 calendar days for Mastercard authorizations properly coded as preauthorizations and is seven calendar days for all other Mastercard authorizations and for all Maestro and Cirrus authorizations and preauthorizations.**

Transactions presented for clearing after the chargeback protection period has expired may be charged back by the issuer under message reason code 4808 (Authorization-Related Chargeback) if the card account is permanently closed (the existing Europe region issuer standard) or if the card account is not in good standing (statused, the standard for issuers in all regions, except the Europe region).

Issuers must be prepared to receive and process a chargeback protection period extension request/0100 message.

To increase only the effective duration of the chargeback protection period of an original preauthorization, the merchant may submit an incremental preauthorization request for a zero amount. The acquirer must submit the request as follows.

- Authorization Request/0100 message
- DE 3 (Processing Code), subfield 1 (Transaction Type) = 00 (Purchase)
- DE 4 (Transaction Amount) = 0 (Additional Amount)
- DE 61 (POS Data), subelement 7 (POS Transaction Status) = 4 (Preauthorized)
- DE 61, subelement 4 (POS Cardholder Presence) is not equal to 4 (Standing Order/Recurring)
- DE 48 (Additional Data), subelement 63 (Trace ID) must be present and contain the Trace ID data (DE 15 and DE 63) from the original preauthorization request in positions 1–15

**NOTE: Authorization Chargeback Protection Period Extension Requests are applicable to all types of purchase preauthorization transactions, except Mastercard contactless transit aggregated or transit debt recovery transactions nor to merchant-financed or acquirer-financed installment payment transactions properly coded as preauthorizations. If submitted, the message will be declined.**

Acquirer-generated Advice/0120 and Reversal Request/0400 messages are not applicable for Authorization Chargeback Protection Period Extension Requests. If submitted, the message will be declined.

The issuer, at its discretion, will send the acquirer an Authorization Request Response/0110 message where DE 39 may contain one of the following values.

- 00 (Approved)
- 05 (Do not honor)
- 85 (Not declined)
- Other valid business declines. Examples of other acceptable business declines include values 41 (Lost Card), 43 (Stolen Card), and 54 (Expired Card).

If the issuer is unable to reply, the acquirer will receive a response code of 91 (Authorization System or issuer system inoperative).

When the chargeback protection period of a preauthorization is extended as a result of an incremental preauthorization, it is extended for 30 calendar days from the date of the latest approved incremental preauthorization. Such requests, if approved by the issuer and when properly coded as an incremental preauthorization, will give rise to an extended chargeback protection period and optionally additional approved amounts that may be cleared under the

conditions that would apply to the security parameters when applied to the original authorization. In other words:

- To the extent that interchange levels are determined by the security parameters of the authorization, then the parameters of the original authorization will be taken into account.
- To the extent that chargebacks take into account the security parameters of the authorization, then the parameters of the original authorization will be taken into account.

When the chargeback protection period expires, issuers must release any block they may have placed on the cardholder's account in relation to the authorization.

Several other options may be used when the authorization lifecycle expires before the transaction is finalized:

- Submit a new preauthorization within 30 calendar days of the planned date of the stay. This creates the risk of a declined transaction. If the original preauthorization has not expired, Mastercard recommends that a reversal is sent of the first transaction to instruct the issuer to release the funds in advance of receiving the second transaction.
- Periodically use the Account Status Inquiry Service to confirm that the card is in good standing prior to the stay. An authorization for the anticipated amount may be submitted in advance of the stay (but no earlier than 30 calendar days before).
- Use the Advance Resort Deposit process as described in the *Chargeback Guide* to authorize and clear the transaction at the time of the reservation.

### **Long Running Transactions**

Occasionally, transactions have an extended life. Examples of these scenarios are vehicle rentals for multiple weeks, extended resort stays, or long cruises. Mastercard expects merchants to authorize the estimated amount at the initiation of the service. Incremental preauthorizations would be requested if the permitted tolerance (if applicable) is exceeded. For more information about transactions with permissible tolerances, refer to the *Transaction Processing Rules* manual, Merchant Acceptance section.

With the specific intent of extending the authorization lifecycle, an incremental preauthorization is recommended. As noted earlier, the authorization lifecycle is based on the date of the latest incremental preauthorization.

### **Extending Security Features**

Mastercard® SecureCode™ protocol authentication relates only to the transaction (and any related incremental preauthorizations if applicable) for which they were originally provided. An acquirer may retain these features by submitting an incremental preauthorization transaction with an amount greater than zero.

### **Authorization Platform Edits**

The Authorization Platform will perform the following system edits related to Authorization Chargeback Protection Period Extension requests.

WHEN...	THEN the Authorization Platform...
The acquirer sends an Authorization Chargeback Protection Period Extension Authorization Request/0100 message that contains the following: <ul style="list-style-type: none"><li>• DE 3 (Processing Code), subfield 1 (Transaction Type), value 00 (Purchase)</li><li>• DE 4 (Transaction Amount), value 0</li><li>• DE 48 (Additional Data), subelement 63 (Trace ID) is present</li><li>• DE 61, subelement 4 (POS Cardholder Presence) is not equal to value 4 (Standing Order/Recurring)</li><li>• DE 61 (POS Data), subelement 7 (POS Transaction Status), value 4 (Preauthorized)</li></ul> and the issuer is not available to respond to the request	Rejects the transaction where: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 91 (Authorization System or issuer system inoperative)</li></ul>
The acquirer sends an Authorization Request/0100 message for an Authorization Chargeback Protection Period Extension request: <ul style="list-style-type: none"><li>• DE 3, subfield 1, value 00</li><li>• DE 4, value 0</li><li>• DE 48, subelement 63 is NOT present</li><li>• DE 61, subelement 4 is not equal to value 4, and</li><li>• DE 61, subelement 7, value 4</li></ul>	Rejects the transaction where: <ul style="list-style-type: none"><li>• DE 39 = 30 (Format Error)</li><li>• DE 44 (Additional Response Data) = 0480nn (where nn is the subelement number)</li></ul>

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
If the acquirer sends an Authorization Request/0100 message for an Authorization Chargeback Protection Period Extension request: <ul style="list-style-type: none"><li>• DE 3, subfield 1, value 00</li><li>• DE 4, value 0</li><li>• DE 48, subelement 63 is present</li><li>• DE 61, subelement 4 is not equal to value 4</li><li>• DE 61, subelement 7, value 4</li></ul> <p>And if the values for Contactless Transit Aggregated, Transit Debt Recovery Transactions are present:</p> <ul style="list-style-type: none"><li>• DE 48, subelement 64 (Transit Program), subfield 1 (Transit Transaction Type Individual) = 03 (Post-Authorized Aggregated), 04 (Authorized Aggregated Split Clearing), or 06 (Post-Authorized Aggregated Maestro)</li></ul>	Rejects the transaction where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 061 (Point-of-Service [POS] Data)</li></ul>
If the acquirer sends an Authorization Request/0100 message for an Authorization Chargeback Protection Period Extension request: <ul style="list-style-type: none"><li>• DE 3, subfield 1, value 00</li><li>• DE 4, value 0</li><li>• DE 48, subelement 63 is present</li><li>• DE 61, subelement 4 is not equal to value 4</li><li>• DE 61, subelement 7, value 4</li></ul> <p>And if the values for Transit Debt Recovery Transactions are present:</p> <ul style="list-style-type: none"><li>• DE 48, subelement 64, subfield 1 = 07 (Debt Recovery)</li></ul> <p>Or if the values for an installment payment transaction are present:</p> <ul style="list-style-type: none"><li>• DE 48, subelement 95 (Promotion Code)</li></ul>	Rejects the transaction where: <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 = 004 (Transaction Amount)</li></ul>

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The acquirer sends an Acquirer-Generated Authorization Advice/0120 or Acquirer-Generated Reversal Request/0400 message for an Authorization Chargeback Protection Period Extension request where the message contains the following:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1, value 00</li> <li>• DE 4, value 0</li> <li>• DE 48, subelement 63 is present</li> <li>• DE 61, subelement 4 is not equal to value 4</li> <li>• DE 61, subelement 7, value 4</li> </ul>	<p>Rejects the transaction where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 004</li> </ul>

---

## 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
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.

Data Element	Org	Sys	Dst	Values/Comments
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

The 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 provide 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.
- 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)
- 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
- 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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>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), subelement 32 (Mastercard Assigned ID)	C	•	C	The value assigned by Mastercard

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
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)	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 the Maestro Recurring Payments Program, the Mastercard Utility Payment Program, and the Maestro Low Risk Merchant 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 edits will be applied to the Maestro Recurring Payments 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) 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.

WHEN...	THEN...
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: <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></ul>	DE 48, subelement 43 (Static AAV) must contain the static AAV assigned by Mastercard for the Maestro Recurring Payments Program for e-commerce transactions.
DE 48, subelement 43 (Static AAV) contains the static AAV assigned by Mastercard for the Maestro Recurring Payments Program for e-commerce transactions	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).
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)	For recurring payment e-commerce transactions: <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 Network via a customer processing 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.

<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 Commercial Payments Account

This section describes Authorization Platform edits supporting the introduction of the MAP (Mastercard Commercial Payments Account) product code in Brazil and the Mastercard European Economic Area subregion.

### Authorization Platform Edit to Support MAP in Brazil

Mastercard offers existing product code MAP as a domestic card-not-present commercial payment solution in Brazil.

The Authorization Platform performs the following system edit to ensure product code MAP is used only in card-not-present transactions in Brazil.

WHEN...	THEN the Authorization Platform...
PAN in DE 2 contains issuer account range associated with brand product MAP and the merchant country code is NOT EQUAL to Brazil (BRA) and DE 61, subfield 5 is NOT EQUAL to value 1	Will reject Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages with: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 12 (Invalid Transactions) is returned in Authorization Request Response/0110 and Authorization Advice Response/0130 messages.</li></ul>

### Authorization Platform Edits to Support MAP in Mastercard European Economic Area Subregion

The Authorization Platform will perform the following system edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The product code is MAP and merchant country code is not in the below country list: <ul style="list-style-type: none"><li>• Austria (040)</li><li>• Belgium (056)</li><li>• Bulgaria (100)</li><li>• Croatia (191)</li><li>• Czech Republic (203)</li><li>• France (250)</li><li>• Germany (280)</li><li>• Greece (300)</li><li>• Iceland (352)</li><li>• Ireland (372)</li><li>• Italy (380)</li><li>• Liechtenstein (438)</li><li>• Luxembourg (442)</li><li>• Malta (470)</li><li>• Netherlands (528)</li><li>• Norway (578)</li><li>• Portugal (620)</li><li>• Slovakia (703)</li><li>• Slovenia (705)</li><li>• Sweden (752)</li><li>• United Kingdom (826)</li></ul>	Will reject Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages with: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 12 (Invalid Transaction) returned in Authorization Request Response/0110 and Authorization Advice Response/0130 messages.</li></ul>

WHEN...	THEN the Authorization Platform...
PAN in DE 2 contains issuer account range associated with brand product MAP and Card Present Indicator DE 61 (Point-of-Service [POS] Data), subfield 5 (POS Card Presence) is not equal to value 1 (Card not present), and merchant country code is not in the below country list: <ul style="list-style-type: none"><li>• Austria (040)</li><li>• Belgium (056)</li><li>• Bulgaria (100)</li><li>• Croatia (191)</li><li>• Czech Republic (203)</li><li>• France (250)</li><li>• Germany (280)</li><li>• Greece (300)</li><li>• Iceland (352)</li><li>• Ireland (372)</li><li>• Italy (380)</li><li>• Liechtenstein (438)</li><li>• Luxembourg (442)</li><li>• Malta (470)</li><li>• Netherlands (528)</li><li>• Norway (578)</li><li>• Portugal (620)</li><li>• Slovakia (703)</li><li>• Slovenia (705)</li><li>• Sweden (752)</li><li>• United Kingdom (826)</li></ul>	Will reject Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages with: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 12 (Invalid Transaction) returned in Authorization Request Response/0110 and Authorization Advice Response/0130 messages.</li></ul> <p><b>NOTE: This edit is also applicable with Region C to Region C messages.</b></p>

## Mastercard Digital Enablement Service

---

The Mastercard Digital Enablement Service (MDES) enhances payment security and reduces fraud risk via tokenization. The service generates a token (substitutes primary account number) that can be used in place of a PAN in transactions. Refer to the *MDES Issuer Implementation Guide* (MIIG) for more information.

### Message Layouts—Pre-digitization Payment Network Messages

The following Authorization message layouts support real-time messages for tokenization.

### **Authorization Request/0100—Tokenization Eligibility**

Following is a list of the data elements and values applicable to the Authorization Request/0100 message type for Tokenization Eligibility. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 2 (Primary Account Number)	•	X	M	Cardholder's primary account number
DE 3 (Processing Code)	•	X	M	00 = Purchase
DE 4 (Amount, Transaction)	•	X	M	Will be zero
DE 14 (Date, Expiration)	•	X	C	Cardholder's primary account expiration date
DE 22 (POS Entry Mode)	•	X	M	Subfield 1 (POS Terminal PAN Entry Mode) = 01 (PAN manual entry)  Subfield 2 (POS Terminal PIN Entry Mode) = 0 (Unspecified or unknown)
DE 35 (Track 2 Data)	•	X	C	The Authorization Platform creates and provides Track 2 data for Maestro tokenization messages.
DE 43 (Card Acceptor Name/Location for All Transactions), subfield 5 (Card Acceptor State or Country Code)	•	X	M	The acquirer in these messages is Mastercard, with a three alphanumeric Country Code corresponding to "USA".  For Local-Use-Only account ranges, Mastercard overrides this value to provide the three alphanumeric Country Code of the issuer.
DE 48 Transaction Category Code	•	X	C	T (Phone, Mail, or Electronic Commerce Order)
DE 48 (Additional Data—Private Use), subelement 23 (Payment Initiation Channel)	•	X	C	Value indicating the type of device for which the consumer is requesting tokenization of a primary account number.

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data—Private Use), subelement 26 (Wallet Program Data), subfield 1 (Wallet Identifier)	•	X	C	Contains the identifier associated with the Wallet Provider
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 1 (Account Number Indicator)	•	X	C	Contains the type of PAN mapping account. <ul style="list-style-type: none"> <li>• C = When MDES Secure Element Device Token</li> <li>• H = When MDES Cloud-based Payments Device Token</li> <li>• F = When MDES Card on File Token</li> </ul>
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 2 (Account Number)	•	X	C	Indicates the PAN mapping account
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 6 (Token Requestor ID)	•	X	C	Contains the ID assigned by the Token Service Provider to the Token Requestor.
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 8 (Storage Technology)	•	X	C	Contains a value indicating the Storage Technology of the requested token.

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 49 (Currency Code, Transaction)	•	X	M	<p>Value indicating the local currency of the acquirer or source location of the transaction. The acquirer in these messages is Mastercard, with a three digits Currency Code of "840" corresponding to USD as Currency Code used in USA.</p> <p>For Local-Use-Only account ranges, Mastercard overrides this value to provide the issuer's three digits Currency Code. This corresponds to the local currency used in that country.</p>
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status)	•	X	M	9 = Tokenization Request/Notification
DE 61 (Additional POS Data), subfield 13 (POS Country Code)	•	X	M	<p>Indicates the country of the POS location (not the acquirer location) using ISO-specified codes.</p> <p>The POS Country Code is set to "840", corresponding to USA.</p> <p>For Local-Use-Only account ranges, Mastercard overrides this value to provide the issuer's three digits Country Code.</p>
DE 124 (Member-defined Data)	•	X	M	See layout for DE 124.

### DE 124 Subfields in Authorization Request/0100—Tokenization Eligibility

The following subfields are available in DE 124 for Authorization Request/0100—Tokenization Eligibility.

Absolute positioning of data in DE 124 subfields is required. Subfields not containing values will be populated with spaces when they are followed by subfields that contain values. If one or more subfields at the end of the data element do not contain a value, the subfield(s) will not be present and the total length of DE 124 will be reduced by the subfield length(s).

<b>Subfield</b>		
<b>Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Message Type	an-2	TE = Tokenization Eligibility Request (TER)
Correlation ID	an-14	Identifier assigned by Mastercard to associate related tokenization request/notification messages.
Primary Account Number Source	an-1	<p>Identifies the method by which the cardholder is attempting to tokenize a primary account number.</p> <p>1 = Card on file</p> <p>2 = Card added manually</p> <p>3 = Card added via application</p>
Payment Application Instance ID	ans-48, left-justified, padded with spaces	Identifier associated with the payment application instance installed onto a device.
Number of Active Tokens for the Primary Account Number	ans-2, leading zeros	Number of existing, active tokens for the primary account number, excluding Card on File tokens.

---

<b>Subfield</b>		
<b>Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Wallet Provider Account ID Hash	ans-64	<p>When provided by the Wallet Provider, the issuer may use this hash value to match against known identifiers for the cardholder; for example, their email addresses on file. If the hash values match, this may aid an issuer's digitization decision by providing additional factors to help verify that the Wallet Provider account holder is indeed their cardholder, or to differentiate between primary and secondary cardholders. The Wallet Provider computes the hash over an email address; MDES receives this and includes it in the data sent to the issuer. The issuer computes the hash of the email address on file for the cardholder; if it matches the hash of the one received from the Wallet Provider, the comparison with the hash value received from the Wallet Provider may be used by the issuer to assist determining the digitization decision. Hashing is used to help the issuer verify the cardholder email (or other relevant identifiers that the issuer may have for the cardholder) without the Wallet Provider providing the full email for privacy and security reasons. When the Wallet Provider is Apple Pay, the hash is generated using the PBKDF2 algorithm (PKCS #5). PBKDF2 is performed using 10 iterations, a salt, and the lowercase account ID as the password. The salt is calculated by taking the lower case UTF-8 bytes from the account ID and performing a SHA-256. Hash calculation example:</p> <p>Example: Input (Password): csharp@walletprovider.com</p> <p>Salt: 41404d1bca85ddb59ab21466e277ac1ac5f614 70be120c82a21b1e45b5248123</p> <p>Count: 10</p> <p>Output: 7098014b646d44c6f3b454c5d54f7a32b3b46e 2b0c8e2367f3e5307e3036dfe6</p>

---

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
		<p>For all other Wallet Providers, the field contains the hash resulting from the following “accountIdHash” algorithm, rightpadded with spaces. “accountId” is the lower case UTF-8 bytes of the account ID:</p> <pre>public String accountIdHash (String accountId) {String random8Bytes = 123CCB2F30BA420B return random8Bytes + lessSignificant24bytes(strongerHash(accountId + random8Bytes))} public String strongerHash(String dataToHash) {String currentHash = dataToHash; for (int i = 0; i &lt; 5000; i++) {currentHash = sha256(currentHash);} return sha256(sha256(dataToHash) + currentHash);}</pre> <p><b>NOTE: NOTE: String random8Bytes = 123CCB2F30BA420B" is a fixed value for all Wallet Providers.</b></p> <p>Hash calculation example:</p> <ul style="list-style-type: none"> <li>• email address: cardholdername@walletprovider.com</li> <li>• accountId: 63617264686F6C6465726E61 6D654077616C6C657470726F 7669646 5722E636F6D</li> <li>• random8Bytes: 123CCB2F30BA420B</li> <li>• output: 123CCB2F30BA420B17F837DF 60E2FC9D6965A74476849FC D43A640F 792A2B358</li> </ul>
Cardholder Name	ans-27, left-justified, pagged with spaces	<p>This field may be present and contain the name of the cardholder. The format is either LASTNAME/FIRSTNAME with the names delimited by a slash “/” (Example: SMITH/JOE) or the format is FIRSTNAME LASTNAME (Example: JOE SMITH).</p> <p>If the cardholder's name is longer than 27 positions, the data will be truncated to the maximum length of 27.</p>

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Token Type	an-1	<p>Contains a value indicating the type of requested token.</p> <p>C = Mastercard Cloud-based Payments</p> <p>F = Card on File</p> <p>S = Embedded Secure Element</p>

### **Authorization Request Response/0110—Tokenization Eligibility**

Following is a list of the data elements and values applicable to the Authorization Request Response/0110 message type for Tokenization Eligibility. All mandatory Authorization Request Response/0110 data elements apply.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code)	ME	ME	•	Must be the same value as the original Authorization Request/0100
DE 4 (Amount, Transaction)	ME	ME	•	Must be the same value as the original Authorization Request/0100
DE 39 (Response Code)	M	•	•	<p>One of the following values indicating how the issuer wants Mastercard to proceed with the tokenization process:</p> <ul style="list-style-type: none"> <li>• 00 = Continue</li> <li>• 05 = Decline</li> <li>• 85 = Continue, but require additional authentication</li> </ul>

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 124 (Member-defined Data)	C	•	•	See layout for DE 124. If the issuer responds with DE 39 = 00 or 85, the issuer may optionally provide DE 124. If the issuer responds with DE 39 = 05, DE 124 must not be present.

### DE 124 Subfields for Authorization Request Response/0110—Tokenization Eligibility

The following subfields are available in DE 124 for Authorization Request Response/0110—Tokenization Eligibility.

Absolute positioning of data in DE 124 subfields is required. Each value must be padded with spaces if the length does not fit exactly the length of the subfield. Subfields not containing values must be populated with spaces when they are followed by subfields that contain values. If one or more subfields at the end of the data element do not contain a value, the subfield(s) will not be present and the total length of DE 124 will be reduced by the subfield length(s).

Subfield Name	Attributes	Values/Comments
Issuer Product Configuration ID	ans-10	<p>The unique product configuration identifier provided by the issuer that identifies a particular set of card art, texts and other product related data, provided during the issuer enablement or maintenance process.</p> <p>By specifying the Issuer Product Configuration ID on the Token Eligibility Request Response, an issuer may override the usual Product Configuration assigned as the default at Account Range level. This allows greater control over exactly which card art and related card product data gets applied as part of a specific tokenization process. However, this does not provide a mechanism to override the Issuer Terms and Conditions file which always comes from the default Product Configuration(s) assigned at Account Range level.</p>
Primary Account Number Card Sequence Number	ans-3, leading zeros	The card sequence number associated with the primary account number.

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>	
Token Data and Activation Method(s)	ans...186	When the issuer responds with DE 39 = 85 (Continue, but require additional authentication), the issuer may provide one or more methods by which the consumer can retrieve the activation code. If the issuer responds with DE 39 = 00 (Continue) or 05 (Decline), or if the issuer responds with DE 39 = 85 but uses an issuer-specified default for the activation method, this field will not be present. Each method will consist of:	
	<b>Name</b>	<b>Attributes</b>	<b>Values/ Comments</b>
	Activation Method Type	n-1	1 = Masked mobile phone number 2 = Masked email address 3 = Automated call center phone number 4 = Call center phone number 5 = Website 6 = Mobile application 7 = Masked voice call phone number
	Activation Method Value	ans...183	Refer to the following examples.
	Delimiter	ans...2	If multiple activation methods are provided by the issuer, the issuer must separate each method with the " " delimiter.

Subfield Name	Attributes	Values/Comments
		<p>Following the last character of the final method in the field, the issuer should include two “ ” delimiters.</p> <p>Values:</p> <p>“ ” indicates another Activation Method follows.</p> <p>“  ” indicates the last Activation Method.</p>

## Examples

1(###) ### 4567 |

1 = Masked mobile phone number

The 1 will be followed by the masked mobile phone number, then the delimiter.

2a\*\*\*d@anymail.com |

2 = Masked email address

The 2 will be followed by the consumer's masked email address (the issuer will mask according to their own format), then the delimiter.

3(555) 123 4567 |

3 = Automated call center phone number

The 3 will be followed by the phone number, then the delimiter. This phone number is not masked.

4(555) 123 8901 |

4 = Call center phone number

The 4 will be followed by the phone number, then the delimiter. This phone number is not masked.

5http://www.anybank.com |

5 = Website

The 5 will be followed by the issuer's website URL, then the delimiter.

6com.anybank.mobileapp |

6 = Mobile app

The 6 will be followed by the issuer's mobile app information, the content of which depends upon the mobile device operating system, then the delimiter.

7(###) ### 2345 ||

7 = Masked voice call phone number

The 7 will be followed by the masked voice call phone number. If this were the last Activation Method provided, the value is followed by two delimiters.

---

### **Authorization Request/0100—Tokenization Authorization**

Following is a list of the data elements and values applicable to the Authorization Request/0100 message type for Tokenization Authorization. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 2 (Primary Account Number)	•	X	M	Cardholder's primary account number
DE 3 (Processing Code)	•	X	M	00 = Purchase
DE 4 (Amount, Transaction)	•	X	M	Will be zero
DE 14 (Date, Expiration)	•	X	C	Cardholder's primary account expiration date
DE 22 (POS Entry Mode)	•	X	M	Subfield 1 (POS Terminal PAN Entry Mode) = 01 (PAN manual entry)
				Subfield 2 (POS Terminal PIN Entry Mode) = 0 (Unspecified or unknown)

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 35 (Track 2 Data)	•	X	C	The Authorization Platform creates and provides Track 2 data for Maestro tokenization messages.
DE 43 (Card Acceptor Name/Location for All Transactions), subfield 5 (Card Acceptor State or Country Code)	•	X	M	The acquirer in these messages is Mastercard, with a three alphanumeric Country Code corresponding to "USA".
				For Local-Use-Only account ranges, Mastercard overrides this value to provide the three alphanumeric Country Code of the issuer.
DE 48 Transaction Category Code	•	X	C	T (Phone, Mail, or Electronic Commerce Order)
DE 48 (Additional Data—Private Use), subelement 23 (Payment Initiation Channel)	•	X	C	Value indicating the type of device for which the consumer is requesting tokenization of a primary account number.
DE 48 (Additional Data—Private Use), subelement 26 (Wallet Program Data), subfield 1 (Wallet Identifier)	•	X	C	Contains the identifier associated with the Wallet Provider.

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 1 (Account Number Indicator)	•	X	C	<p>Contains the type of PAN mapping account. Possible values:</p> <ul style="list-style-type: none"> <li>• C = when MDES Secure Element Device Token</li> <li>• H = when MDES Cloud-based Payments Device Token</li> <li>• F = when MDES Card on File Token</li> </ul>
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 2 (Account Number)	•	X	C	Indicates the PAN mapping account.
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 6 (Token Requestor ID)	•	X	C	Contains the ID assigned by the Token Service Provider to the Token Requestor.
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 8 (Storage Technology)	•	X	C	Contains a value indicating the storage technology of the requested token.
DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service)	•	X	C	52 = AVS and Authorization Request/0100
DE 48 (Additional Data—Private Use), subelement 92 (CVC 2)	•	X	C	CVC 2 value from the signature panel of the card when applicable

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 49 (Currency Code, Transaction)	•	X	M	<p>Value indicating the local currency of the acquirer or source location of the transaction. The acquirer in these messages is Mastercard, with a three digits Currency Code of "840" corresponding to USD as Currency Code used in USA.</p> <p>For Local-Use-Only account ranges, Mastercard overrides this value to provide the issuer's three digits Currency Code. This corresponds to the local currency used in that country.</p>
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status)	•	X	M	9 = Tokenization Request/Notification
DE 61 (Additional POS Data), subfield 13 (POS Country Code)	•	X	M	<p>Indicates the country of the POS location (not the acquirer location) using ISO-specified codes.</p> <p>The POS Country Code is set to "840", corresponding to USA.</p> <p>For Local-Use-Only account ranges, Mastercard overrides this value to provide the issuer's three digits Country Code.</p>
DE 120 (Record Data)	•	X	C	AVS postal code and address data in the format specified by the issuer

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 124 (Member-defined Data)	•	X	M	See layout for DE 124.

### DE 124 Subfields in Authorization Request/0100—Tokenization Authorization

These are the subfields available in DE 124 in an Authorization Request/0100 message for Tokenization Authorization.

Absolute positioning of data in DE 124 subfields is required. Subfields not containing values will be populated with spaces when they are followed by subfields that contain values. If one or more subfields at the end of the data element do not contain a value, the subfield(s) will not be present and the total length of DE 124 will be reduced by the subfield length(s).

Subfield Name	Attributes	Values/Comments
Message Type	an-2	TA = Tokenization Authorization Request (TAR)
Correlation ID	an-14	Identifier assigned by Mastercard that can be used by the issuer to associate related tokenization request/notification messages.
Primary Account Number Source	an-1	Identifies the method which the cardholder is attempting to tokenize a primary account number.  1 = Card on file  2 = Card added manually  3 = Card added via application
Payment Application Instance ID	ans-48, left-justified, padded with spaces	Identifier associated with the payment application instance installed onto a device.
Device Source IP Address	ans-12, left-justified, padded with spaces	Variable length IP address. Each octet of the IP address is converted to hex, and joined into one string, with the order maintained.

<b>Subfield</b>		
<b>Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Wallet Service Provider Account ID Hash	ans-64	<p>This field may be present and contain PBKDF2 hash of the consumer's account ID with the Wallet Provider. The Account ID is typically expected to be an email address. PBKDF2 is performed using 10 iterations, a salt, and the lowercase account ID as the password. The salt is calculated by taking the lower case UTF-8 bytes from the account ID and performing a SHA-256.</p> <p>Example: Input (Password): csharp@walletprovider.com</p> <p>Salt: 41404d1bca85ddb59ab21466e277ac1ac5f614 70be120c82a21b1e45b5248123</p> <p>Count: 10</p> <p>Output: 7098014b646d44c6f3b454c5d54f7a32b3b46e 2b0c8e2367f3e5307e3036dfe6</p>
Cardholder Name	ans-27, left-justified, trailing spaces	<p>This field may be present and contain the name of the cardholder. The format is either LASTNAME/FIRSTNAME with the names delimited by a slash "/" (Example: SMITH/JOE) or the format is FIRSTNAME LASTNAME (Example: JOE SMITH).</p> <p>If the cardholder's name is longer than 27 positions, the data will be truncated to the maximum length of 27.</p>
Wallet Provider Tokenization Recommendation	an-1	<p>Tokenization decision suggested by the Wallet Provider. One of the following values:</p> <p>0 = Decline 1 = Approve 2 = Require additional authentication</p>
Wallet Provider Tokenization Recommendation Standard Version	an-2, left-justified, padded with spaces	The version of the standards the Wallet Provider is using to determine the suggested tokenization recommendation.

<b>Subfield</b>		
<b>Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Wallet Provider Device Score	n-1	Score assigned by Wallet Provider for the device. Value between 1 and 5.
Wallet Provider Account Score	n-1	Score assigned by Wallet Provider for the primary account number. Value between 1 and 5.
Number of Active Tokens for the Primary Account Number	ans-2, leading zeros	Number of active or suspended tokens for the primary account number provisioned to consumer devices. Space-filled when requested token digitized to a server.
Wallet Service Provider Tokenization Recommendation Reason Codes	ans-6	<p>Code indicating the specific reason the Wallet Provider is suggesting the tokenization recommendation.</p> <p>The data of this field is a hex-encoded bitmap, whereby each bit corresponds to a specific Reason Code.</p> <p>The bitmap is big-endian with the least significant bit corresponding to Reason Code 01, with the next least significant bit corresponding to Reason Code 02 and so on. For example, if Reason Codes 01, 05, and 16 were encoded, the bitmap would be 000000001000000000010001 and the hex value of this field would be 008011.</p> <p>If the Wallet Provider has no reason, this field will contain spaces.</p>

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Device Location	ans-9	<p>Latitude and longitude where the device the consumer is attempting to tokenize a card onto is located.</p> <p>Device Location Latitude—an-4; hexadecimal encoded degrees with 2 decimal places</p> <p>Device Location Longitude—an-4; hexadecimal encoded degrees with 2 decimal places</p> <p>Device Location Lat/Long Sector—n-1; one of the following values:</p> <ul style="list-style-type: none"> <li>1 = Latitude = N, Longitude = W</li> <li>2 = Latitude = N, Longitude = E</li> <li>3 = Latitude = S, Longitude = W</li> <li>4 = Latitude = S, Longitude = E</li> </ul> <p>This field will contain spaces if the Wallet Provider has not provided this information.</p>
Mobile Number Last 4 Digits	ans-4	<p>Last four digits of the consumer's mobile phone number</p> <p>This field will contain spaces if the Wallet Provider has not provided this information.</p>
Token Type	an-1	<p>Contains a value indicating the type of requested token.</p> <p>C = Mastercard Cloud-based Payments</p> <p>F = Card on File</p> <p>S = Embedded Secure Element</p>
Consumer Identifier	an-88	<p>Unique identifier for each consumer, which financial institutions will then need to verify before a consumer can add their credentials to the payment-enabled devices. Position 212–299 in the DE 124 of the Authorization Request/0100—Tokenization Authorization message only.</p> <p>Issuers and processors will not receive the new Consumer Identifier in DE 124 unless they explicitly opt to receive it.</p>

### **Authorization Request Response/0110—Tokenization Authorization**

Following is a list of the data elements and values applicable to the Authorization Request Response/0110 message type for Tokenization Authorization. All mandatory Authorization Request Response/0110 data elements apply.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code)	ME	ME		<ul style="list-style-type: none"> <li>• Must be the same value as the original Authorization Request/0100</li> </ul>
DE 4 (Amount, Transaction)	ME	ME		<ul style="list-style-type: none"> <li>• Must be the same value as the original Authorization Request/0100</li> </ul>
DE 39 (Response Code)	M		•	<ul style="list-style-type: none"> <li>• One of the following values indicating how the issuer wants Mastercard to proceed with the tokenization process:           <ul style="list-style-type: none"> <li>• 00 = Approve</li> <li>• 05 = Decline</li> <li>• 85 = Approve, but require additional authentication</li> </ul> </li> </ul>
DE 48 Transaction Category Code	CE	CE		<ul style="list-style-type: none"> <li>• Must be the same value as the original Authorization Request/0100</li> </ul>
DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service)	CE	CE		<ul style="list-style-type: none"> <li>• 52 = AVS and Authorization Request/0100</li> </ul>
DE 48 (Additional Data—Private Use), subelement 83 (Address Verification Service Response)	C		•	<ul style="list-style-type: none"> <li>• The AVS response code</li> </ul>
DE 48 (Additional Data—Private Use), subelement 87 (Card Validation Code Result)	C		•	<ul style="list-style-type: none"> <li>• The CVC 2 result code</li> </ul>
DE 48 (Additional Data—Private Use), subelement 92 (CVC 2)	CE	CE		<ul style="list-style-type: none"> <li>• Must be the same value as the original Authorization Request/0100</li> </ul>
DE 56 (Payment Account Data)	C	X	C	PAR value provided by the Issuer when Issuer or its designated service provider is BIN Controller (Mastercard is not BIN Controller).
DE 124 (Member-defined Data)	C		•	<ul style="list-style-type: none"> <li>• See layout for DE 124. If the issuer responds with DE 39 = 00 or 85, the issuer may optionally provide DE 124. If the issuer responds with DE 39 = 05, DE 124 must not be present.</li> </ul>

## **DE 124 Subfields in Authorization Request Response/0110—Tokenization Authorization**

These are the subfields available in DE 124 in an Authorization Request Response/0110 message to support the Tokenization Authorization for the Mastercard Digital Enablement Service.

Absolute positioning of data in DE 124 subfields is required. Subfields not containing values must be populated with spaces when they are followed by subfields that contain values. If one or more subfields at the end of the data element do not contain a value, the subfield(s) will not be present and the total length of DE 124 will be reduced by the subfield length(s).

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Issuer Product Configuration ID	ans-10	<p>The unique product configuration identifier provided by the issuer that identifies a particular set of card art, texts and other product related data, provided during the issuer enablement or maintenance process.</p> <p>By specifying the Issuer Product Configuration ID on the Token Eligibility Request Response, an issuer may override the usual Product Configuration assigned as the default at Account Range level. This allows greater control over exactly which card art and related card product data gets applied as part of a specific tokenization process. However, this does not provide a mechanism to override the Issuer Terms and Conditions file which always comes from the default Product Configuration(s) assigned at Account Range level.</p>
Primary Account Number Card Sequence Number	ans-3, leading zeros	<p>The card sequence number associated with the primary account number.</p>
Token Data and Activation Method(s)	ans...286	<p>The subfield can have zero to multiple groupings of three Token Data and Activation Method Type, Token Data and Activation Method Value, and Delimiter.</p> <p>When the issuer responds with DE 39 = 85 (Approve, but require additional authentication), the issuer may provide one or more activation methods by which the consumer can retrieve the activation code. If the issuer responds with DE 39 = 00 (Approve) or 05 (Decline) activation methods will not be present. If the issuer responds with DE 39 = 85 but uses an issuer-specified default for the activation method, activation methods may not be present.</p> <p>When the issuer responds with DE 39 = 00 (Approve) or DE 39 = 85 (Approved, but require additional authentication), the issuer may provide zero to multiple token personalization data.</p>

Subfield Name	Attributes	Values/Comments
• Token Data and Activation Method Type	an-1	<p>1 = Masked mobile phone number (activation method)</p> <p>2 = Masked email address (activation method)</p> <p>3 = Automated call center phone number (activation method)</p> <p>4 = Call center phone number (activation method)</p> <p>5 = Website (activation method)</p> <p>6 = Mobile application (activation method)</p> <p>7 = Masked voice call phone number (activation method)</p> <p>a = Alternate account identifier</p> <p>t = One or multiple token personalization data items</p>

Subfield Name	Attributes	Values/Comments
• Token Data and Activation Method Value	ans...283	<p>When the Token Data and Activation Method Type is 1, 2, 3, 4, 5, 6, or 7 the issuer must provide values used to specify an activation method. See Examples 1, 2, 3, and 4 for examples of Token Data and Activation Method(s) containing activation method values.</p> <p>Issuers have the option of providing an alternate account identifier in Tokenization Authorization Response messages (Token Data and Activation Method Type = a).</p> <p>An Alternate Account Identifier is a cardholder-friendly reference to a bank account, for example an IBAN (International Bank Account Number). It is typically useful for a Wallet Provider to display a suffix of this identifier to the cardholder to help them identify their tokenized card when they are not aware of their Account PAN.</p> <p>This will enable wallets to display alternate account identifier suffixes depending on the wallet functionality. Issuers must refer to each wallet's documentation to determine if/how the alternate account identifier suffixes are displayed to cardholders.</p> <p>An alternate account identifier is in the format of a string with minimum 9 and maximum 64 characters, with no spaces allowed. An IBAN is an example of an alternate account identifier, as for example, GB82WEST12345698765432.</p> <p>When the Token Data and Activation Method Type is t, the issuer must provide one or multiple proprietary token personalization data items that MDES will include in the token profile. See Example 8 for an example of Token Data and Activation Method(s) containing multiple token personalization data items.</p> <p>Each token personalization data item can have one to multiple instances of couples Token Personalization Data and Separator.</p> <p>Token Personalization Data: Base64 encoded data. Structure and content of data is defined separately per <i>Mastercard Digital Enablement Service (MDES) Issuer Implementation Guide</i>. See Examples 6 and 7.</p>
Separator	ans...1	Each separate token personalization data (including after the last) will be delimited by a “~” character.

Subfield Name	Attributes	Values/Comments
• Delimiter	ans-2	<p>See Example 5 for an example of Token Data and Activation Method(s) containing multiple activation method values and multiple token personalization data items.</p> <p>If multiple Token Data and Activation Methods are provided by the issuer, the issuer must separate each method with the “ ” delimiter.</p> <p><b>NOTE: When at least another grouping of three Token Data and Activation Method Type, Token Data and Activation Method Value, and Delimiter follows, then the Delimiter has attributes of ans-1.</b></p> <p>Delimiter Values:</p> <p>“ ” indicates that another Token Data or Activation Method follows.</p> <p>Following the last character of the final Token Data and Activation Method in the field, the issuer should include two “ ” delimiters.</p> <p>“  ” indicates the last Token Data and Activation Method.</p>

## Examples

Example	Description
1	An example of Token Data and Activation Method(s) subfield containing only a masked mobile phone number activation method: 1(###)###4567
2	An example of Token Data and Activation Method(s) subfield containing the masked email address activation method and the automated call center phone number activation method: 2a***d@anymail.com 3(555)1234567
3	An example of Token Data and Activation Method(s) subfield containing the call center phone number activation method, the website activation method and the masked voice call phone number activation method: 4(555)1238901 5http://www.anybank.com 6com.anybank.mobileapp
4	An example of Token Data and Activation Method(s) subfield containing only a masked voice call phone number activation method: 7(###)###4567

<b>Example</b>	<b>Description</b>
5	An example of Token Data and Activation Method(s) subfield containing mobile application activation method, masked email address activation method and some personalization data for the token profile:  6com.anybank.mobileapp 2a***d@anymail.com tBJ9uCwJQAAEwOQECAwQFX1UCR1I=~CwECAwQFBgc=~
6	An example of Token Personalization Data: "BJ9uCwJQAAEwOQECAwQFX1UCR1I=" that is "049F6E 0B 0250 0001 3039 0102030405 5F55 02 4652" base64 encoded. The purpose of Token Personalization Data is to replace default Third Party Data (9F6E) and add Issuer Country Code (5F55) in Contactless FCI Issuer Discretionary Data.
7	An example of Token Personalization Data: "CwECAwQFBgc=" that is "0B01020304050607" base64 encoded. The purpose of Token Personalization Data is to create a new tag "9F70" (Protected Data Envelope) readable through GET DATA on both Management and Contactless Payment interfaces.
8	An example of Token Data and Activation Method(s) subfield containing multiple token personalization data items: tBJ9uCwJQAAEwOQECAwQFX1UCR1I=~CwECAwQFBgc=~

### **Authorization Request/0100—Activation Code Notification**

Following is a list of the data elements and values applicable to the Authorization Request/0100 message type for Activation Code Notification. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 2 (Primary Account Number)	•	X	M	Cardholder's primary account number
DE 3 (Processing Code)	•	X	M	00 = Purchase
DE 4 (Amount, Transaction)	•	X	M	Will be zero
DE 14 (Date, Expiration)	•	X	C	Cardholder's primary account expiration date
DE 22 (POS Entry Mode)	•	X	M	Subfield 1 (POS Terminal PAN Entry Mode) = 01 (PAN manual entry)  Subfield 2 (POS Terminal PIN Entry Mode) = 0 (Unspecified or unknown)

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 35 (Track 2 Data)	•	X	C	The Authorization Platform creates and provides Track 2 data for Maestro tokenization messages.
DE 43 (Card Acceptor Name/Location for All Transactions), subfield 5 (Card Acceptor State or Country Code)	•	X	M	The acquirer in these messages is Mastercard, with a three alphanumeric Country Code corresponding to "USA".
				For Local-Use-Only account ranges, Mastercard overrides this value to provide the three alphanumeric Country Code of the issuer.
DE 48 Transaction Category Code	•	X	C	T (Phone, Mail, or Electronic Commerce Order)
DE 48 (Additional Data—Private Use), subelement 23 (Payment Initiation Channel)	•	X	C	Value indicating the type of device for which the consumer is requesting tokenization of a primary account number.
DE 48, subelement 26 (Wallet Program Data), subfield 1 (Wallet Identifier)	•	X	C	Contains the identifier associated with the Wallet Provider
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 1 (Account Number Indicator)	•	X	C	Contains the type of PAN mapping account. Possible values: <ul style="list-style-type: none"> <li>• C = When MDES Secure Element Device Token</li> <li>• H = When MDES Cloud-based Payments Device Token</li> <li>• F = When MDES Card on File Token</li> </ul>
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 2 (Account Number)	•	X	C	Indicates the PAN mapping account

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 6 (Token Requestor ID)	•	X	C	Contains the ID assigned by the Token Service Provider to the Token Requestor.
DE 49 (Currency Code, Transaction)	•	X	M	<p>Value indicating the local currency of the acquirer or source location of the transaction. The acquirer in these messages is Mastercard, with a three digits Currency Code of "840" corresponding to USD as Currency Code used in USA.</p> <p>For Local-Use-Only account ranges, Mastercard overrides this value to provide the issuer's three digits Currency Code. This corresponds to the local currency used in that country.</p>
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status)	•	X	M	9 = Tokenization Request/Notification
DE 61 (Additional POS Data), subfield 13 (POS Country Code)	•	X	M	<p>Indicates the country of the POS location (not the acquirer location) using ISO-specified codes.</p> <p>The POS Country Code is set to "840", corresponding to USA.</p> <p>For Local-Use-Only account ranges, Mastercard overrides this value to provide the issuer's three digits Country Code.</p>
DE 124 (Member-defined Data)	•	X	M	See layout for DE 124.

### **DE 124 Subfields in Authorization Request/0100—Activation Code Notification**

These are the subfields available in DE 124 in the Authorization Request/0100 message for Activation Code Notification for the Mastercard Digital Enablement Service.

Absolute positioning of data in DE 124 subfields is required. Subfields not containing values will be populated with spaces when they are followed by subfields that contain values. If one or more subfields at the end of the data element do not contain a value, the subfield(s) will not be present and the total length of DE 124 will be reduced by the subfield length(s).

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Message Type	an-2	AC = Activation Code Notification (ACN)
Correlation ID	an-14	Identifier assigned by Mastercard to associate related tokenization request/notification messages.
Activation Code	ans-8, left-justified, padded with spaces	Activation code assigned by Mastercard that will be provided to the issuer for delivery to the consumer to complete the tokenization process.
Activation Code Expiration Date and Time	n-10	Date and time that the activation code expires specified in UTC units.  Format: YYMMDDhhmm
Consumer's Activation Method Preference	ans..165	This field contains the activation method selected by the consumer, if only one was offered by the issuer, then that activation method. There will be only one method contained within this field. This field will only be present if the cardholder provides a choice.
<b>Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Activation Method Type	n-1	1 = Masked mobile phone number  2 = Masked email address  3 = Automated call center phone number  4 = Call center phone number  5 = Website

---

Subfield Name	Attributes	Values/Comments
		6 = Mobile application
		7 = Masked voice call phone number
	Activation Method Value	ans...164 Refer to the following examples

## Examples

1(###) ### 4567

1 = Masked mobile phone number

The 1 will be followed by the masked mobile phone number.

2a\*\*\*d@anymail.com

2 = Masked email address

The 2 will be followed by the consumer's masked email address (the issuer will mask according to their own format).

3(555) 123 4567

3 = Automated call center phone number

The 3 will be followed by the phone number. This phone number is not masked.

4(555) 123 8901

4 = Call center phone number

The 4 will be followed by the phone number. This phone number is not masked.

5http://www.anybank.com

5 = Website

The 5 will be followed by the issuer's website URL.

6com.anybank.mobileapp

6 = Mobile app

The 6 will be followed by the issuer's mobile app information, the content of which depends upon the mobile device operating system.

7(###) ### 2345

7 = Masked voice call phone number

The 7 will be followed by the masked voice call phone number.

---

### **Authorization Request Response/0110—Activation Code Notification**

Following is a list of the data elements and values applicable to the Authorization Request Response/0110 message type for Activation Code Notification. All mandatory Authorization Request Response/0110 data elements apply.

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code)	ME	ME	•	Must be the same value as the original Authorization Request/0100
DE 4 (Amount, Transaction)	ME	ME	•	Must be the same value as the original Authorization Request/0100
DE 39 (Response Code)	M	•	•	00 = Approved

**NOTE: DE 124 is not present.**

### **Authorization Request/0100—Tokenization Complete Notification**

Following is a list of the data elements and values applicable to the Authorization Request/0100 message type for Tokenization Complete Notification. All mandatory Authorization Request/0100 data elements apply.

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number)	•	X	M	Cardholder's primary account number
DE 3 (Processing Code)	•	X	M	00 = Purchase
DE 4 (Amount, Transaction)	•	X	M	Will be zero

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 14 (Date, Expiration)	•	X	C	Cardholder's primary account expiration date
DE 22 (POS Entry Mode)	•	X	M	Subfield 1 (POS Terminal PAN Entry Mode) = 01 (PAN manual entry)  Subfield 2 (POS Terminal PIN Entry Mode) = 0 (Unspecified or unknown)
DE 35 (Track 2 Data)	•	X	C	The Authorization Platform creates and provides Track 2 data for Maestro tokenization messages.
DE 43 (Card Acceptor Name/Location for All Transactions), subfield 5 (Card Acceptor State or Country Code)	•	X	M	The acquirer in these messages is Mastercard, with a three alphanumeric Country Code corresponding to "USA".  For Local-Use-Only account ranges, Mastercard overrides this value to provide the three alphanumeric Country Code of the issuer.
DE 48 Transaction Category Code	•	X	C	T (Phone, Mail, or Electronic Commerce Order)
DE 48 (Additional Data —Private Use), subelement 23 (Payment Initiation Channel)	•	X	C	Value indicating the type of device for which the consumer is requesting tokenization of a primary account number.
DE 48, subelement 26 (Wallet Program Data), subfield 1 (Wallet Identifier)	•	X	C	Contains the identifier associated with the Wallet Provider.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48 (Additional Data —Private Use), subelement 33 (PAN Mapping File Information), subfield 1 (Account Number Indicator), subfield 2 (Account Number), subfield 3 (Expiration Date), subfield 5 (Token Assurance Level), subfield 6 (Token Requestor ID), and subfield 8 (Storage Technology)	•	X	C	<p>Subfield 1 indicates the type of PAN mapping account.</p> <p>Subfield 2 indicates the PAN mapping account number.</p> <p>Subfield 3 indicates the expiration date of the PAN mapping account.</p> <p>Subfield 5 indicates Token Assurance Level</p> <p>Subfield 6 contains the ID assigned by the Token Service Provider to the Token Requestor.</p> <p>Subfield 8 indicates Storage Technology of the token.</p>
DE 49 (Currency Code, Transaction)	•	X	M	<p>Value indicating the local currency of the acquirer or source location of the transaction. The acquirer in these messages is Mastercard, with a three digits Currency Code of "840" corresponding to USD as Currency Code used in USA.</p> <p>For Local-Use-Only account ranges, Mastercard overrides this value to provide the issuer's three digits Currency Code. This corresponds to the local currency used in that country.</p>
DE 56 (Payment Account Data)	•	X	C	This is only for MDES Tokenization Complete Notifications.

<b>Data Element ID and Name</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)	•	X	M	9 = Tokenization Request/Notification
DE 61 (Additional POS Data), subfield 13 (POS Country Code)	•	X	M	Indicates the country of the POS location (not the acquirer location) using ISO-specified codes.  The POS Country Code is set to "840", corresponding to USA.
				For Local-Use-Only account ranges, Mastercard overrides this value to provide the issuer's three digits Country Code.
DE 124 (Member-defined Data)	•	X	M	See layout for DE 124.

### **DE 124 Subfields in Authorization Request/0100—Tokenization Complete Notification**

These are the subfields available in DE 124 in the Authorization Request/0100 message for Tokenization Complete Notification for the Mastercard Digital Enablement Service.

Absolute positioning of data in DE 124 subfields is required. Subfields not containing values will be populated with spaces when they are followed by subfields that contain values. If one or more subfields at the end of the data element do not contain a value, the subfield(s) will not be present and the total length of DE 124 will be reduced by the subfield length(s).

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Message Type	an-2	TC = Tokenization Complete Notification (TCN)
Correlation ID	an-14	Identifier assigned by Mastercard to associate related tokenization request/notification messages.
Number of Active Tokens for the Primary Account Number	ans-2, leading zeros	Number of active or suspended tokens, including the current token, for the primary account number digitized to consumer devices. Space-filled when token present in DE 48, subelement 33, subfield 2 (Account Number) in an 0100 Tokenization Complete Notification message is digitized to a server.

---

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Issuer Product Configuration ID	ans-10	The unique product configuration identifier provided by the issuer that identifies a particular set of card art, texts and other product related data, provided during the issuer enablement or maintenance process.
Consumer Language	a-2	Language preference selected by the consumer.
Device Name	ans-20, left-justified, padded with spaces	Name that the consumer has associated to the device with the Wallet Provider.
Final Tokenization Decision	ans-1	The final tokenization decision that was used in the tokenization of the card:  1 = Approve 2 = Approve, but require additional authentication
Final Tokenization Decision Indicator	ans-1	The element of the Service that was responsible for determining the final tokenization decision:  1 = Tokenization Eligibility Response 2 = Tokenization Authorization Response 3 = Issuer pre-defined tokenization rules 4 = Mobile Application
T&C Identifier	ans-32, left-justified, padded with spaces	Identifier associated with the version of terms and conditions accepted by the consumer.
T&C Date and Time	ans-10	Date and time that the consumer accepted the terms and conditions of the Service specified in UTC units.  Format: YYMMDDhhmm
Number of Activation Attempts	ans-1	Number of activation code entry attempts by the cardholder. Space-filled when DE 124, subfield 14 (Token Type) value is F.
Token Unique Reference	ans-48, left-justified, padded with spaces	Service-allocated unique reference to the token.
Primary Account Number Unique Reference	ans-48, left-justified, padded with spaces	Service-allocated unique reference to the tokenized Primary Account Number at the wallet level

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Token Type	an-1	<p>Contains a value indicating the type of token present in DE 48, subelement 33, subfield 2 (Account Number) in an 0100 Tokenization Complete Notification message.</p> <p>C = Mastercard Cloud-based Payments F = Card on File S = Embedded Secure Element</p>

### **Authorization Request Response/0110—Tokenization Complete Notification**

Following is a list of the data elements and values applicable to the Authorization Request Response/0110 message type for Tokenization Complete Notification. All mandatory Authorization Request Response/0110 data elements apply.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code)	ME	ME	•	Must be the same value as the original Authorization Request/0100.
DE 4 (Amount, Transaction)	ME	ME	•	Must be the same value as the original Authorization Request/0100.
DE 39 (Response Code)	M	•	•	00 = Approved

**NOTE: DE 124 is not present.**

### **Authorization Request/0100—Tokenization Event Notification**

Following is a list of the data elements and values applicable to the Authorization Request/0100 message type for Tokenization Event Notification. All mandatory Authorization Request/0100 data elements apply.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 2 (Primary Account Number)	•	X	M	Cardholder's primary account number

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code)	•	X	M	00 = Purchase
DE 4 (Amount, Transaction)	•	X	M	Will be zero
DE 14 (Date, Expiration)	•	X	C	Cardholder's primary account expiration date
DE 22 (POS Entry Mode)	•	X	M	Subfield 1 (POS Terminal PAN Entry Mode) = 01 (PAN manual entry)  Subfield 2 (POS Terminal PIN Entry Mode) = 0 (Unspecified or unknown)
DE 35 (Track 2 Data)	•	X	C	The Authorization Platform creates and provides Track 2 data for Maestro tokenization messages.
DE 43 (Card Acceptor Name/Location for All Transactions), subfield 5 (Card Acceptor State or Country Code)	•	X	M	The acquirer in these messages is Mastercard, with a three alphanumeric Country Code corresponding to "USA".  For Local-Use-Only account ranges, Mastercard overrides this value to provide the three alphanumeric Country Code of the issuer.
DE 48 Transaction Category Code	•	X	C	T (Phone, Mail, or Electronic Commerce Order)
DE 48 (Additional Data —Private Use), subelement 23 (Payment Initiation Channel)	•	X	C	Value indicating the type of device for which the consumer is requesting tokenization of a primary account number.
DE 48, subelement 26 (Wallet Program Data), subfield 1 (Wallet Identifier)	•	X	C	Contains the identifier associated with the Wallet Provider.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 1 (Account Number Indicator), subfield 2 (Account Number), subfield 3 (Expiration Date), and subfield 6 (Token Requestor ID)	•	X	C	<p>Subfield 1 indicates the type of PAN mapping account.</p> <p>Subfield 2 indicates the PAN mapping account number.</p> <p>Subfield 3 indicates the expiration date of the PAN mapping account.</p> <p>Subfield 6 contains the ID assigned by the Token Service Provider to the Token Requestor.</p>
DE 49 (Currency Code, Transaction)	•	X	M	<p>Value indicating the local currency of the acquirer or source location of the transaction. The acquirer in these messages is Mastercard, with a three digits Currency Code of "840" corresponding to USD as Currency Code used in USA.</p> <p>For Local-Use-Only account ranges, Mastercard overrides this value to provide the issuer's three digits Currency Code. This corresponds to the local currency used in that country.</p>
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status)	•	X	M	9 = Tokenization Request/Notification
DE 61 (Additional POS Data), subfield 13 (POS Country Code)	•	X	M	<p>Indicates the country of the POS location (not the acquirer location) using ISO-specified codes.</p> <p>The POS Country Code is set to "840", corresponding to USA.</p> <p>For Local-Use-Only account ranges, Mastercard overrides this value to provide the issuer's three digits Country Code.</p>
DE 124 (Member-defined Data)	•	X	M	See layout for DE 124.

#### **DE 124 Subfields in Authorization Request/0100—Tokenization Event Notification**

These are the subfields available in DE 124 in an Authorization Request/0100 message to support Tokenization Event Notification.

Absolute positioning of data in DE 124 subfields is required. Subfields not containing values will be populated with spaces when they are followed by subfields that contain values. If one or more subfields at the end of the data element do not contain a value, the subfield(s) will not be present and the total length of DE 124 will be reduced by the subfield length(s).

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Message Type	an-2	TV = Tokenization Event Notification (TVN)
Correlation ID	an-14	Identifier assigned by Mastercard to associate related tokenization request/notification messages.
Tokenization Event Indicator	n-1	<p>Value indicating the event that has occurred on the Mastercard Digital Enablement Service for the token.</p> <hr/> <p>3 = Deactivate</p> <p>4 = Deleted from consumer device</p> <p>6 = Suspend</p> <p>7 = Resume</p> <p>8 = Tokenization Exception Event</p> <p>9 = Replacement</p>
Tokenization Event Reason Code	an-2	<p>If Tokenization Event Indicator contains value 8 (Tokenization Exception Event), this field contains a value indicating the event reason. If the Tokenization Event Indicator contains a value of 3 (Deactivate), 6 (Suspend), or 7 (Resume), this field will not be present.</p> <hr/> <p>00 = Activation code retries exceeded</p> <p>01 = Activation code expired or invalidated</p> <p>02 = Activation code entered incorrectly by cardholder</p>

<b>Subfield Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
Event Requestor	ans-1	<p>If the Tokenization Event Indicator contains a value of 3 (Deactivate), 6 (Suspend), or 7 (Resume), this field will contain a value indicating the party that requested the event. If the Tokenization Event Indicator contains a value of 8 (Tokenization Exception Event) this field will be space filled.</p> <p>0 = Indicates the Tokenization Event was requested by the Wallet Provider or Token Requestor</p> <p>1 = Indicates the Tokenization Event was requested by the Funding Account issuer</p> <p>2 = Indicates the Tokenization Event was requested by the Cardholder</p> <p>3 = Indicates the Tokenization Event was requested in relation to a systematic event triggered by Mobile PIN Validation security (applicable to Tokenization Event Indicator value of 6 (Suspend), or 7 (Resume) only)</p> <p>4 = Indicates the Tokenization Event was requested in relation to a systematic event triggered by Mobile PIN Change Validation security (applicable to Tokenization Event Indicator value of 6 (Suspend), or 7 (Resume) only)</p> <p>5 = Reserved for future use</p> <p>6 = Reserved for future use</p> <p>7 = Reserved for future use</p> <p>8 = Reserved for future use</p>

Subfield Name	Attributes	Values/Comments
		9 = Reserved for future use

#### **Authorization Request Response/0110—Tokenization Event Notification**

Following is a list of the data elements and values applicable to the Authorization Request Response/0110 message type for Tokenization Event Notification. All mandatory Authorization Request Response/0110 data elements apply.

Data Element ID and Name	Org	Sys	Dst	Values/Comments
DE 3 (Processing Code)	ME	ME	•	Must be the same value as the original Authorization Request/0100
DE 4 (Amount, Transaction)	ME	ME	•	Must be the same value as the original Authorization Request/0100
DE 39 (Response Code)	M	•	•	00 = Approved

**NOTE: DE 124 will not be present.**

#### **Issuer File Update Request/0302—Maintenance (Token/PAN Update)**

Following is a list of the data elements and values applicable to this message type. All mandatory Issuer File Update Request/0302 data elements apply.

Data Element and Name	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number)	M	M	•	Contains the cardholder's primary account number
DE 91 (Issuer File Update Code)	M	M	•	Contains the Issuer File Update function code. Valid value will be 2 (Update).
DE 101 (File Name)	M	M	•	MCC106 (PAN Mapping File)
DE 120 (Record Data)	M	M	•	Contains token and PAN information. Refer to the layout of DE 120.

#### **DE 120 Layout for MCC106 Mastercard Digital Enablement Service (Token Update)**

The following table provides the technical details of DE 120 (Record Data) when DE 101 (File Name) contains the value MCC106 (Mastercard Digital Enablement Service Mapping File PAN Update) in the Issuer File Update Request/0302 message.

<b>Field ID and Name</b>		<b>Attributes</b>	<b>Values/Comments</b>
1	Mapping File Indicator	an-1	<p>M = Mastercard Digital Enablement Service Tokens excluding Card on File Tokens</p> <p>A = All Mastercard Digital Enablement Service Tokens including Card on File Tokens</p> <p>Best practice for the issuer to use value A</p>
2	Replacement PAN	ans-19	<p>Number replacing the number that is embossed, encoded, or both on the card (the primary account number). Customers may input only account numbers for BINs assigned to the associated customer ID assigned by Mastercard.</p> <p>The issuer has the option to provide a replacement primary account number for association to the token.</p> <p>Format: Left-justified, with trailing spaces</p>
3	Replacement PAN Expiration Date	n-4	<p>Expiration date that is associated with the number replacing the number that is embossed, encoded, or both on the card that represents the cardholder primary account number.</p> <p>If the issuer has provided a replacement primary account number, this field contains the expiration date that is associated with the replacement primary account number.</p> <p>If the issuer has not provided a replacement primary account number, this field contains the expiration date of the existing primary account number.</p> <p>Format: YYMM</p>
4	Primary Account Card Sequence Number	ans-3	<p>If the issuer has provided a replacement primary account number, this field will contain the card sequence number associated with the replacement primary account number.</p> <p>If the issuer has not provided a replacement primary account number, this field will contain the card sequence number associated with the original primary account number.</p> <p>Format: Left-justified, padded with leading zeros.</p>

Field ID and Name	Attributes	Values/Comments	
5	Notify Wallet Service Provider Indicator	n-1	If the issuer has provided a replacement primary account number and replacement primary account number expiration date, this field indicates whether the Wallet Provider should be notified of the change.
		Values:	<ul style="list-style-type: none"> <li>• 0 = Update token mapping information and notify the Wallet Provider with the primary account number information</li> <li>• 1 = Update token mapping information, but do not notify the Wallet Provider with the primary account number information</li> <li>• 2 = Do not update token mapping information, but do update the Wallet Provider with the primary account number information</li> </ul>
6	Token—if replacing a specific token	ans-19	<p>Surrogate value for a PAN that is consistent with ISO message requirements and is a 13 to 19-digit numeric value that passes basic validation rules of an account number, including the LUHN check.</p> <p>Format: Left-justified, with trailing spaces</p>
		If field not present, update shall apply to all token to PAN mappings associated with the PAN	

### DE 120 Layout for MCC106 Mastercard Digital Enablement Service (PAN Update—Deactivate/Suspend/Resume Token)

The following table provides the technical details of DE 120 (Record Data) when DE 101 (File Name) contains the value MCC106 (Mastercard Digital Enablement Service Mapping File PAN Update) in the Issuer File Update Request/0302 message.

Field ID	Name	Attributes	Values/Comments
1	Mapping File Indicator	an-1	<p>M = Mastercard Digital Enablement Service tokens excluding Card on File tokens.</p> <p>A = All Mastercard Digital Enablement Service tokens including Card on File tokens.</p> <p>Best practice for the issuer to use value A.</p>

<b>Field ID</b>	<b>Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
2	Action Required	an-1	<p>S = Suspend token</p> <p>D = Deactivate token</p> <p>C = Resume token</p>
3	Notify Wallet Service Provider indicator	n-1	<p>This field indicates whether the Wallet Provider should be notified of the change.</p> <p>Value:</p> <ul style="list-style-type: none"> <li>• 0 = Update token mapping information and notify the Wallet Provider.</li> </ul>
4	Token—If updating a specific token	ans-19	<p>Surrogate value for a PAN that is consistent with ISO message requirements and is a 13–19-digit numeric value that passes basic validation rules of an account number, including the LUHN check.</p> <p>Format: Left-justified, with trailing spaces.</p> <p>If not present, do across the board switch—based on Field 1. If field not present, Update shall apply to all token to PAN mappings associated with the PAN.</p>

#### **Issuer File Update Request Response/0312—Issuer Token Maintenance Response (Token/PAN Update)**

Following is a list of the data elements and values applicable to this message type. All mandatory Issuer File Update Request Response/0312 data elements apply.

<b>Data Element and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 2 (Primary Account Number)	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302.
DE 39 (Response Code)	•	M	M	Indicates disposition of Issuer File Update Request/0302.
DE 44 (Additional Response Data)	•	C	C	May contain additional response information, based on DE 39. Error messages should spell out field in error (ex: 120XXX)
DE 91 (Issuer File Update Code)	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302.
DE 101 (File Name)	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302.

Data Element and Name	Org	Sys	Dst	Values/Comments
DE 120 (Record Data)	•	ME	ME	Must be the same value as in the original Issuer File Update Request/0302.

### **Administrative Advice/0620—Issuer Token Notification Advice**

Mastercard will support new layouts for Administrative Advice/0620 messages to communicate activation codes to issuers in support of token issuance and to notify issuers that Mastercard has assigned a token on their behalf. Following is a list of the data elements and values applicable to this message type. All mandatory Administrative Advice/0620—System-generated data elements apply.

Data Element and Name	Org	Sys	Dst	Values/Comments
Message Type Identifier (MTI)	•	X	M	Constant—0620 (Administrative Advice)
Bit Map, Primary	•	X	M	Mandatory
Bit Map, Secondary	•	X	M	Mandatory
DE 7 (Transmission Date and Time)	•	X	M	Transaction time stamp; UTC date and time that this transaction was entered into interchange
DE 11 (Systems Trace Audit Number [STAN])	•	X	M	Transaction trace number; must be unique value for transaction initiator within each UTC day
DE 33 (Forwarding Institution ID Code)	•	X	M	Identifies the customer, institution, or Authorization Platform facility originating the Administrative Advice/0620 message
DE 42 (Card Acceptor Identification Code)	•	X	M	Identifies the card acceptor.
DE 56 (Payment Account Data)	•	X	C	This is only for MDES Tokenization Complete Notifications.

Data Element and Name	Org	Sys	Dst	Values/Comments
DE 60 (Advice Reason Code)	•	X	M	<p>Indicates the specific reason for the transmission of the Advice message</p> <p>Subfield 1 (Advice Reason Code) = 141 (Mastercard Digital Enablement Service Advice to Issuer)</p> <p>Subfield 2 (Advice Detail Code) = one of the following values:</p> <ul style="list-style-type: none"> <li>• 0250 = Activation Code Notification (ACN)</li> <li>• 0251 = Tokenization Complete Notification</li> <li>• 0252 = Tokenization Event Notification</li> </ul>
DE 63 (Network Data)	•	X	M	Contains the Banknet Reference Number that the Authorization Platform provides as a unique transaction ID.
DE 100 (Receiving Institution ID Code)	•	X	M	Identifies the customer, institution, or Authorization Platform facility that will receive this Administrative Advice/0620.
DE 120 (Record Data)	•	X	M	Contains activation code information. Refer to the associated DE 120 layout.

### **DE 120 Layout for Administrative Advice/0620—Issuer Token Notification Advice for Activation Code Notification**

The following table provides the technical details of DE 120 (Record Data) when DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) contains the value 141 (Mastercard Digital Enablement Service Advice to Issuer) and DE 60, subfield 2 (Advice Detail Code) contains the value 0250 (Activation Code Notification) in the Administrative Advice/0620 message.

Absolute positioning of data in DE 120 subfields is required. Subfields not containing values will be populated with spaces when they are followed by subfields that contain values. If one or more subfields at the end of the data element do not contain a value the subfield(s) will not be present and the total length of DE 120 will be reduced by the subfield length(s).

Field ID and Name	Attributes	Values/Comments
1 Primary Account Number	an-19	Cardholder's primary account number
2 Primary Account Number Expiry Date	n-4	Cardholder's primary account number expiration date

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Values/Comments</b>	
3 Correlation ID	an-14	Identifier assigned by Mastercard to associate related tokenization request/notification messages.	
4 Activation Code	ans-8, left-justified, padded with spaces	Activation code assigned by Mastercard that will be provided to the issuer for delivery to the consumer to complete the tokenization process.	
5 Activation Code Expiration Date and Time	n-10	Date and time that the activation code expires specified in UTC units.  Format: YYMMDDhhmm	
6 Customer's Activation Method Preference	ans-165, left-justified, padded with spaces	This field contains the activation method selected by the consumer, if only one was offered by the issuer, then that activation method will be present. There will be only one method contained within this field. This field will only be present if the cardholder made a selection.	
	Name	Attributes	Values/ Comments
	Activation Method Type	n-1	1 = Masked mobile phone number  2 = Masked email address  3 = Automated call center phone number  4 = Call center phone number  5 = Website  6 = Mobile application  7 = Masked voice call phone number
	Activation Method Value	ans...164	See examples below.
7 Token Requestor ID	n-11	Contains the identifier assigned by the Token Service Provider to the Token Requestor.	
8 Wallet ID	ans-3	Contains the identifier associated with the Wallet Provider. Presence of this field is conditional.	

Field ID and Name	Attributes	Values/Comments
9 Device Type	ans-2	Indicates the type of device used. Presence of this field is conditional.

## Examples

"1(###) ### 4567"

1 = Masked mobile phone number

The "1" will be followed by the masked mobile phone number.

"2a\*\*\*d@anymail.com"

2 = Masked email address

The "2" will be followed by the consumer's masked email address (the issuer will mask according to their own format).

"3(555) 123 4567"

3 = Automated call center phone number

The "3" will be followed by the phone number. This phone number is not masked.

"4(555) 123 8901"

4 = Call center phone number

The "4" will be followed by the phone number. This phone number is not masked.

"5http://www.anybank.com"

5 = Website

The "5" will be followed by the issuer's website URL.

"6com.anybank.mobileapp"

6 = Mobile app

The "6" will be followed by the issuer's mobile app information, the content of which depends upon the mobile device operating system.

“7(###) ### 2345”

7 = Masked voice call phone number

The “7” will be followed by the masked voice call phone number.

---

### **DE 120 Layout for Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Complete Notification**

The following table provides the technical details of DE 120 (Record Data) when DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) contains the value 141 (Mastercard Digital Enablement Service Advice to Issuer) and DE 60, subfield 2 (Advice Detail Code) contains the value 0251 (Tokenization Complete Notification) in the Administrative Advice/0620 message.

Absolute positioning of data in DE 120 subfields is required. Subfields not containing values will be populated with spaces when they are followed by subfields that contain values. If one or more subfields at the end of the data element do not contain a value the subfield(s) will not be present and the total length of DE 120 will be reduced by the subfield length(s).

Field ID and Name	Attributes	Values/Comments
1 Token	an-19	Surrogate value for a PAN that is consistent with ISO message requirements and is a 13 to 19-digit numeric value that passes basic validation rules of an account number, including the LUHN check.  Format: Left-justified, with trailing spaces
2 Token Expiration Date	n-4	Expiration date associated with the token.
3 PAN	an-19	Number that is embossed, encoded, or both on the card (also known as the primary account number). Customers may input only account numbers for BINs assigned to the associated customer ID assigned by Mastercard.  Format: Left-justified, with trailing spaces
4 PAN Expiration Date	n-4	Expiration date that is embossed, encoded, or both on the card that represents the cardholder primary account number (primary account number).  Format: YYMM
5 Token Service Provider Identification	a-1	M = Mastercard Digital Enablement Service
6 Token Assurance Level	n-2	Assurance level assigned to the token (value between 00 and 99).

<b>Field ID and Name</b>		<b>Attributes</b>	<b>Values/Comments</b>
7	Token Requestor ID	n-11	The ID assigned by Mastercard to the token requestor.
8	Contactless Usage	n-1	<p>Contains value indicating if the token is permitted for use in contactless transactions.</p> <p>Values:</p> <ul style="list-style-type: none"> <li>• 0 = Token is not permitted for use in contactless transactions</li> <li>• 1 = Token is permitted for use in contactless transactions</li> </ul>
9	Card on File Electronic Commerce Usage	n-1	<p>Contains value indicating if the token is permitted for use in card on file electronic commerce transactions.</p> <p>Values:</p> <ul style="list-style-type: none"> <li>• 0 = Token is not permitted for use in Card on File electronic commerce transactions</li> <li>• 1 = Token is permitted for use in card on file electronic commerce transactions</li> </ul>
10	Mobile/Digital Wallet Electronic Commerce Usage	n-1	<p>Contains value indicating if the token is permitted for use in mobile/digital wallet electronic commerce transactions.</p> <p>Values:</p> <ul style="list-style-type: none"> <li>• 0 = Token is not permitted for use in mobile/digital wallet electronic commerce transactions</li> <li>• 1 = Token is permitted for use in mobile/digital wallet electronic commerce transactions</li> </ul>
11	Correlation ID	an-14	Identifier assigned by Mastercard to associate related tokenization request/notification messages.
12	Number of Active Tokens for the Primary Account Number	ans-2, leading zeros	Number of active or suspended tokens for the primary account number digitized to consumer devices. Space-filled when token present in DE 48, subelement 33, subfield 2 (Account Number) in an 0100 Tokenization Complete Notification message is provisioned to a server. Presence of this field is conditional.
13	Issuer Product Configuration ID	ans-10	The unique product configuration identifier applied to the token, as provided by the issuer, identifying a particular set of card art, texts, and other product related data, that were provided during the issuer enablement or maintenance process. Presence of this field is conditional.
14	Consumer Language	a-2	Language preference selected by the consumer. Presence of this field is conditional.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
15 Device Name	ans-20, left- justified, padded with spaces	Name that the consumer has associated to the device with the Wallet Provider. Presence of this field is conditional.
16 Final Tokenization Decision	ans-1	The final tokenization decision that was used in the tokenization of the card. <ul style="list-style-type: none"><li>• 1 = Approve</li><li>• 2 = Approve but requires additional authentication</li></ul> Presence of this field is conditional.
17 Final Tokenization Decision Indicator	ans-1	The element of the Service that was responsible for determining the final tokenization decision: <ul style="list-style-type: none"><li>• 1 = Tokenization Eligibility Response</li><li>• 2 = Tokenization Authorization Response</li><li>• 3 = Issuer pre-defined tokenization rules</li><li>• 4 = Mobile Application</li></ul> Presence of this field is conditional.
18 T&C Identifier	ans-32, left justified, padded with spaces	Identifier associated with the version of terms and conditions accepted by the consumer. Presence of this field is conditional.
19 T&C Date and Time	ans-10	Date and time that the consumer accepted the terms and conditions of the Service, specified in UTC units. Format: YYMMDDhhmm
20 Number of Activation Attempts	ans-1	Number of activation code entry attempts by the cardholder. Space-filled when DE124, SF14 (Token Type) value is F. Presence of this field is conditional.
21 Token Unique Reference	ans-48, left justified, padded with spaces	Service-allocated unique reference to the token.
22 Primary Account Number Unique Reference	ans-48, left justified, padded with spaces	Service-allocated unique reference to the tokenized Primary Account Number at the wallet level.

<b>Field ID and Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
23 Token Type	an-1	<p>Contains a value indicating the type of token present in DE 120, field 1 (Token) in an 0620 Tokenization Complete Notification message.</p> <ul style="list-style-type: none"> <li>• C = Mastercard Cloud-Based Payments</li> <li>• F = Card on File</li> <li>• S = Embedded Secure Element</li> </ul>
24 Wallet ID	ans-3	Contains the identifier associated with the Wallet Provider. Presence of this field is conditional.
25 Device Type	ans-2	Indicates the type of device used. Presence of this field is conditional.
26 Storage Technology	an-2	Contains a value indicating the storage technology of the token. Presence of this field is conditional.

**NOTE: The Token Requestor ID is already being included in DE 120, field ID 7 of the Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Complete Notification message.**

#### **DE 120 Layout for Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Event Notification**

The following table provides the technical details of DE 120 (Record Data) when DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) contains the value 141 (Mastercard Digital Enablement Service Advice to Issuer) and DE 60, subfield 2 (Advice Detail Code) contains the value 0252 (Tokenization Event Notification) in the Administrative Advice/0620 message.

Absolute positioning of data in DE 120 subfields is required. Subfields not containing values will be populated with spaces when they are followed by subfields that contain values. If one or more subfields at the end of the data element do not contain a value the subfield(s) will not be present and the total length of DE 120 will be reduced by the subfield length(s).

<b>Field ID</b>	<b>Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
1	Primary Account Number	an-19	Cardholder's primary account number
2	Primary Account Number Expiry Date	n-4	Cardholder's primary account expiration date
3	Token (PAN mapping file information)	an-19	Token
4	Token Expiration Date (PAN mapping file information)	an-4	Token expiration date

<b>Field ID</b>	<b>Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
5	Token Service Provider Identification	a-1	M = Mastercard Digital Enablement Service
6	Correlation ID	an-14	Identifier assigned by Mastercard to associate related tokenization request/notification messages
7	Tokenization Event Indicator	n-1	<p>Value indicating the event that has occurred on the Mastercard Digital Enablement Service for the token</p> <p>3 = Deactivate 4 = Deleted from consumer device 6 = Suspend 7 = Resume 8 = Tokenization Exception Event 9 = Replacement</p>
8	Tokenization Event Reason Code	an-2	<p>If the Tokenization Event Indicator contains value 8 (Tokenization Exception Event), this field contains a value indicating the event reason. If the Tokenization Event Indicator contains a value of 3 (Deactivate), 6 (Suspend), or 7 (Resume), this field will not be present.</p> <ul style="list-style-type: none"> <li>• 00 = Activation code retries exceeded</li> <li>• 01 = Activation code expired or invalidated</li> <li>• 02 = Activation code entered incorrectly by cardholder</li> </ul>
9	Contactless Usage	n-1	<p>Contains value indicating if the token is permitted for use in contactless transactions.</p> <p>Values:</p> <ul style="list-style-type: none"> <li>• 0 = Token is not permitted for use in contactless transactions</li> <li>• 1 = Token is permitted for use in contactless transactions</li> </ul>
10	Card on File Electronic Commerce Usage	n-1	<p>Contains value indicating if the token is permitted for use in card on file electronic commerce transactions.</p> <p>Values:</p> <ul style="list-style-type: none"> <li>• 0 = Token is not permitted for use in Card on File electronic commerce transactions</li> <li>• 1 = Token is permitted for use in card on file electronic commerce transactions</li> </ul>

<b>Field ID</b>	<b>Name</b>	<b>Attributes</b>	<b>Values/Comments</b>
11	Mobile/Digital Wallet Electronic Commerce Usage	n-1	<p>Contains value indicating if the token is permitted for use in mobile/digital wallet electronic commerce transactions.</p> <p>Values:</p> <ul style="list-style-type: none"> <li>• 0 = Token is not permitted for use in mobile/digital wallet electronic commerce transactions</li> <li>• 1 = Token is permitted for use in mobile/digital wallet electronic commerce transactions</li> </ul>
12	Event Requestor	ans-1	<p>If the Tokenization Event Indicator contains a value of 3 (Deactivate), 6 (Suspend), or 7 (Resume), this field will contain a value indicating the party that requested the event. If the Tokenization Event Indicator contains a value of 8 (Tokenization Exception Event) this field will be space filled.</p> <ul style="list-style-type: none"> <li>• 0 = Indicates the Tokenization Event was requested by the Wallet Provider or Token Requestor</li> <li>• 1 = Indicates the Tokenization Event was requested by the Funding Account issuer</li> <li>• 2 = Indicates the Tokenization Event was requested by the Cardholder</li> <li>• 3 = Indicates the Tokenization Event was requested in relation to a systematic event triggered by Mobile PIN Validation security (applicable to Tokenization Event Indicator value of 6 (Suspend), or 7 (Resume) only)</li> <li>• 4 = Indicates the Tokenization Event was requested in relation to a systematic event triggered by Mobile PIN Change Validation security (applicable to Tokenization Event Indicator value of 6 (Suspend), or 7 (Resume) only)</li> <li>• 5 = Reserved for future use</li> <li>• 6 = Reserved for future use</li> <li>• 7 = Reserved for future use</li> <li>• 8 = Reserved for future use</li> <li>• 9 = Reserved for future use</li> </ul>
13	Token Requestor ID	n-11	Contains the identifier assigned by the Token Service Provider to the Token Requestor.
14	Wallet ID	ans-3	Contains the identifier associated with the Wallet Provider. Presence of this field is conditional.
15	Device Type	ans-2	Indicates the type of device used. Presence of this field is conditional.

### **Administrative Advice Response/0630—Issuer Token Notification Advice Response**

Following is a list of the data elements and values applicable to this message type. All mandatory Administrative Advice/0630 data elements apply.

Data Element and Name	Org	Sys	Dst	Values/Comments
Message Type Identifier (MTI)	M	M	•	Constant—0630 (Administrative Advice Response)
Bit Map, Primary	M	M	•	Mandatory
Bit Map, Secondary	M	M	•	Mandatory
DE 7 (Transmission Date and Time)	ME	ME	•	Must be the same value as in the original Administrative Advice/0620
DE 11 (Systems Trace Audit Number [STAN])	ME	ME	•	Must be the same value as in the original Administrative Advice/0620
DE 33 (Forwarding Institution ID Code)	ME	ME	•	Must be the same value as in the original Administrative Advice/0620
DE 39 (Response Code)	M	M	•	Indicates the disposition of the original Administrative Advice/0620
DE 44 (Additional Response Data)	C	C	•	May contain the additional error code information depending on the value in DE 39
DE 63 (Network Data)	ME	ME	•	Must be the same value as in the original Administrative Advice/0620
DE 100 (Receiving Institution ID Code)	ME	ME	•	Must be the same value as in the original Administrative Advice/0620

## **MDES for Merchants**

This section describes enhancements to the Mastercard Digital Enablement Service (MDES) for merchants program that provides a network tokenization service for merchants. The section provides the technical requirements for issuers choosing to participate in the program and for acquirers supporting merchants that are enrolled in the program.

**NOTE: The following is effective 13 October 2017 in the U.S. Region, Canada Region, and Asia/Pacific Region. The effective dates for all other regions will be communicated by Mastercard in a future announcement.**

Mastercard offers specific values and purpose to existing data elements in the Dual Message (Authorization) System to help issuers and acquirers identify the MDES for merchants program and participants throughout the authorization flow.

The following process explains an authorization transaction request when a token transaction is generated by an MDES for merchants participant.

1. When a merchant initiates the token transaction the tokenized transaction data is transmitted to the acquirer.
2. The acquirer initiates an authorization transaction request containing the following data and sends it to the Mastercard Network for initial purchase:
  - DE 2 (Primary Account Number [PAN]) with the token
  - DE 22 (POS Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) value 81 (PAN entry via electronic commerce, including chip)
  - DE 48, subelement 42 containing value 246 indicating Merchant Risk Management Decisioning
  - DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]) with cryptographic data
  - DE 61 (Point of Service [POS] Data), subfield 3 (POS Terminal Location)
    - Value 2 (Off premises), or
    - Value 4 (On premises of card acceptor facility [cardholder terminal including home PC, mobile phone, PDA])

Acquirers submitting recurring payments or partial shipment authorization transaction requests containing the following data:

- DE 2 (Primary Account Number [PAN]) with the token
- DE 22 (POS Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) value 81 (PAN entry via electronic commerce, including chip)
- DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 containing values:
  - Position 1, value 2 (Channel)
  - Position 2, value 4 (Digital Secure Remote Payment [DSRP] with UCAF data)
  - Position 3, value 7 (Partial shipment or recurring payment)
- DE 48, subelement 43 not present
- DE 61, subfield 3 = 2 (Off premises of card acceptor facility [cardholder terminal including home PC, mobile phone, PDA])
- DE 61, subfield 4 = 4 (Standing order/recurring transactions) for recurring payment transactions or = 5 (Electronic order [home PC, Internet, mobile phone, PDA]) for partial shipments.
3. The Dual Message System (Authorization) will attempt to identify a PAN mapping relationship between the token sent by the acquirer, and an account PAN in the PAN mapping database. If the mapping or validation fails, MDES will reject the transaction back to the acquirer and merchant with the appropriate response, then generate an Authorization Advice/0120 response message to inform the issuer of the action. If the MDES services are successful, the Authorization Platform then sends the issuer the authorization transaction request containing:
  - DE 2 (Primary Account Number [PAN]) with the cardholder's primary account number
  - DE 14 (Date, Expiration) with the primary account number's expiration date

- DE 22, subfield 1, value 81 (PAN entry via electronic commerce, including chip)
- DE 48, subelement 26 (Wallet Program Data), subfield 1 (Wallet Identifier) value = 327
- DE 48, subelement 30 (Token Transaction Identifier)
- DE 48, subelement 33 containing:
  - Subfield 1 (Account Number Indicator), value H (Cloud-Based Token)
  - Subfield 2 (Account Number) containing the token
  - Subfield 3 (Expiration Date) containing the token expiration date
  - Subfield 5 (Token Assurance Level) static value 00 to 99
  - Subfield 6 (Token Requestor ID)
  - Subfield 8 (Storage Technology)
- DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 containing value 246 indicating Merchant Risk Management Decisioning
- DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 containing value 247 for subsequent recurring payment and partial shipment transactions

**NOTE: The Authorization Platform will validate or modify to the correct security level indicator (SLI) if needed. See the following for more details.**

- DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]) may be present if issuer has opted-in to receive cryptographic data
  - DE 48, subelement 71 (On-behalf Services) including:
    - 50C = Mastercard Digital Enablement Service PAN Mapping
    - 61V = Mastercard Digital Enablement Service Cloud-Based Payments Chip (EMV-level) Pre-Validation Service
4. The issuer responds with an authorization transaction response message, and the Authorization Platform provides the response to the acquirer containing the following:
    - DE 2 contains the token
    - DE 22, subfield 1, value 81 (PAN entry via electronic commerce, including chip)
    - DE 48, subelement 33, containing:
      - Subfield 1 (Account Number Indicator), value M (Primary Account Number)
      - Subfield 2 (Account Number)
      - Subfield 3 (Expiration Date) containing the expiration date
      - Subfield 5 (Token Assurance Level) static value 00 to 99
      - Subfield 6 (Token Requestor ID)
  5. The acquirer forwards the token and other authorization transaction response information to the merchant.

## Mastercard Fraud Scoring Services

---

This section describes the two Mastercard Fraud Scoring Services: Expert Monitoring for Issuers and Decision Intelligence.

## Expert Monitoring for Issuers

This section describes Expert Monitoring for Issuers.

Mastercard will require all issuing and acquiring processors to code, support, and integrate into their systems the data elements, subelements, and values associated with Expert Monitoring for Issuers. The following provides the *Global Safety and Security Standards* effective dates for each region:

- U.S.: 21 April 2017
- Europe: 13 October 2017
- Latin America and Caribbean: 13 October 2017
- Middle East/Africa: 13 October 2017
- Asia/Pacific: 13 April 2018
- Canada: 13 April 2018

**NOTE:**

**Mastercard does not require acquirers or issuers to enroll in these optional products and services, but they must code their systems to support these fields to leverage such product and services in a timely manner in the event of a security issue.**

**Mastercard currently provides Expert Monitoring for Issuers or Decision Intelligence. The same data elements support both services.**

Expert Monitoring for Issuers provides best-in-class transaction fraud monitoring that enables Mastercard issuers to evaluate and manage the probability of fraud in transactions at the point of interaction. As an integrated, multi-component, transaction fraud monitoring solution, Expert Monitoring for Issuers provides:

- **Network fraud monitoring** that silently scans global authorization activity, monitoring for highly abnormal activity to identify and limit fraud losses from large-scale fraud events.
- **Customized fraud rule management** utilizing individual data elements within the authorization message as well as Mastercard-defined variables to automate precise, highly variable fraud decisions during authorization and enable appropriate actions based on issuer specifications.
- **Finely tuned fraud detection models** segmented to identify specific fraud pattern behaviors for specific products, geographies, and channels.
- **Predictive, real-time fraud scoring** during authorization that indicates the likelihood that the transaction is fraudulent.

### For More Information

For more information about this service, refer to the *Authorization Manual*.

## Fraud Rule Manager

Fraud Rule Manager is an optional service that allows participating issuers to publish and enact business rules specific to their portfolio of accounts. The outcome of the rules may be to introduce a Rule Adjusted Score, Rule Reason Codes, or both into the authorization message when rule criteria authorized by the issuer are met.

## To Participate

Issuers that want to participate in this service must complete a contract and registration form. Issuers interested in registering for this service should contact their Mastercard representative or the Mastercard Risk Solutions Team at [risksolutions@Mastercard.com](mailto:risksolutions@Mastercard.com).

## For More Information

For more information about this service, refer to the *Authorization Manual*.

## Decision Intelligence

This section describes Decision Intelligence, one of the two Mastercard Fraud Scoring Services.

### Overview

This section provides an overview of Decision Intelligence.

Decision Intelligence is a real-time authorization decisioning solution that applies thousands of data points and sophisticated modeling techniques to each transaction, simplifying these insights into a single transaction decision score that helps issuers to fine-tune their authorization decisions with the goal of approving genuine transactions and declining fraudulent ones.

Decision Intelligence ultimately shifts transaction decisioning from the basis of a risk score to a decision score that is based on both the fraud risk and rewards of approving a transaction. With a more comprehensive analysis of the risk and reward factors, Decision Intelligence assesses both negative and positive data points to calculate a single score that shows where the transaction falls on a scale from decline to approve—thus helping issuers authorize more transactions with confidence, increase their profitability, and improve the cardholder experience.

Decision Intelligence supports all Mastercard brands (Mastercard®, Maestro®, Cirrus®), segments (consumer, commercial), and products (credit, debit, prepaid) for transactions processed via the Mastercard Network.

### How it Works

This section briefly describes how Decision Intelligence works.

The value of Decision Intelligence lies in its ability to evaluate multiple factors throughout the shopping experience to decide whether or not a transaction makes sense for a particular consumer. Decision Intelligence evaluates information about consumers, merchants, and issuers during the shopping experience to help issuers decide whether a transaction should be approved or declined.

For each transaction, Decision Intelligence assesses:

- Consumer transaction attributes based on consumer account and device information
- Transaction security based on widespread fraud monitoring, fraud rules, transaction fraud models, and profiles
- Cardholder segmentation based on insights into account spending that help define the value and engagement of the cardholder with their issuer

The resulting decision score shows the transaction on a risk-reward continuum (with a value from 0–999). A lower score signifies an excellent approvability quotient, while a higher score indicates more reasons for declining the transaction. Issuers can easily integrate the decision score into their authorization decision processes and cardholder strategies.

### **Issuers' Potential Benefit from Decision Intelligence**

Decision Intelligence enriches and simplifies the decision management process with insights across multiple key dimensions that can potentially help issuers gain incremental business in revenue by:

- Helping increase approvals of genuine transactions without increasing their risk exposure
- Deepening consumer relationships with a more consistent, satisfying experience across shopping choices

Decision Intelligence potentially helps issuers to save money from:

- Fewer false positive or erroneous declines of genuine transactions
- Less revenue lost from fraud and chargebacks
- Improved productivity and lower costs (operational, IT, customer service, reputational, and so on) of managing fraud
- Decreased customer service costs due to more approved transactions
- Lower operational costs in capital, information technology (IT) development, and customer service by outsourcing decisioning through Mastercard's established, scalable platform

### **Message Specification Requirements**

To limit the development impact on its customers, Decision Intelligence utilizes the pre-existing Expert Monitoring for Issuers data fields. Because many issuers or their processors already process these fields, there may not be additional development effort required to support the fields for this service.

Issuers participating in the Decision Intelligence service must support the following existing fields.

---

#### **On-behalf Service (OBS)**

DE 48 (Additional Data—Private Use)

- Subelement 71 (On-behalf Services)
    - Subfield 1 (On-behalf Service) with a value of 18C (Fraud Scoring Service was performed successfully)
-

### **Fraud Scoring Data**

DE 48 (Additional Data—Private Use)

- Subelement 75 (Fraud Scoring Data)
    - Subfield 1 (Fraud Score) with a default value of 001
    - Subfield 2 (Score Reason Code) with a default value of 00
    - Subfield 3 (Rules Score)
    - Subfield 4 (Rules Reason Code 1)
    - Subfield 5 (Rules Reason Code 2)
- 

### **Security Services Additional Data for Issuers**

DE 48 (Additional Data—Private Use)

- Subelement 56 (Security Services Additional Data for Issuers)
    - Subfield 1 (Security Services Indicator)
    - Subfield 2 (Security Services Data)
- 

### **To Participate**

Issuers interested in participating in Decision Intelligence should contact their Mastercard account representative. To participate, issuers must complete a Service Agreement to indicate the appropriate bank identification numbers (BINs)/account ranges to be configured for the service.

### **For More Information**

For details on the Authorization IQ and Digital Transaction Insights features of Decision Intelligence, refer to DE 48 (Additional Data—Private Use), Subelement 56 (Security Services Additional Data for Issuers)—Valid Subfield 1 (Security Services Indicator) and Subfield 2 (Security Services Data) Value Combinations in the Data Element Definitions chapter of this manual.

### **Expert Monitoring for Merchants**

Expert Monitoring for Merchants provides participating acquirers with a real-time fraud score on U.S.-issued, dual message, card-not-present (CNP) authorization transactions.

#### **Benefits**

Expert Monitoring for Merchants provides the following benefits:

- Provides CNP merchants with a real-time behavior-based fraud score at the time of transaction authorization
- Delivers a predictive fraud score on Mastercard transactions to merchants within the authorization response message
- Uniquely scores transactions using a targeted fraud model that evaluates the current transaction against a comprehensive view of the cardholder's transaction history

- Enables merchants to use the fraud score as a highly predictive data point in their current fraud detection solution to increase fraud detection while reducing chargebacks, fraud losses, and manual review costs

### To Participate

Acquirers that want to participate in Expert Monitoring for Merchants must complete a contract and registration form. Acquirers interested in registering for this service should contact their Mastercard representative.

### For More Information

For more information about this service, refer to the *Authorization Manual*.

## 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 = Fraud Scoring Service was performed successfully U = 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 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 fraud scoring, but the issuer is unavailable and Stand-In processing is invoked. This information applies to both Expert Monitoring for Issuers and Decision Intelligence.

Stand-In and X-code processing do not consider the fraud assessment score when performing an authorization decision for an issuer.

<b>IF...</b>	<b>THEN the Authorization Advice/0120—System-generated message will contain...</b>
If the original Authorization Request/0100 message was successfully scored	<p>DE 48, subelement 75 and DE 48, subelement 71, subfield 1, value 18 and subfield 2, value C indicating Fraud Scoring Service was performed on the transaction</p>
If the original Authorization Request/0100 message was not successfully scored	<p>DE 48, subelement 71, subfield 1, value 18 and Subfield 2, value U indicating Fraud Scoring Service was not performed on the transaction</p>

## 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.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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 System or issuer system inoperative).**

## 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

WHEN the message contains...	THEN the Authorization Platform...
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 = 048013

### Authorization Request Response/0110 Edits

WHEN....	THEN the Authorization Platform...
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 = 048013

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

WHEN the message contains...	THEN the Authorization Platform...
DE 48, subelement 13	Declines the request with an Authorization Advice Response/0130 message where: DE 39 = 30 DE 44 = 048013

## Reversal Request/0400 Edits

WHEN the message contains...	THEN the Authorization Platform...
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 In Control Service

The Mastercard In Control™ 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 In Control 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—In Control 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.

Data Element	Org	Sys	Dst	Values/Comments
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

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48 (Additional Data—Private Use), subelement 33, (PAN Mapping File Information), subfield 1 (Account Number Indicator)	•	X	C	Indicates Mastercard In Control 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 = In Control Virtual Card Service
DE 48, subelement 71 (On-Behalf Services), subfield 2 (On-Behalf [OB] Result 1)	•	X	C	V = Valid
				<b>NOTE: If the Purchase Control service is unsuccessful, refer to Subfield 2—On-behalf Result 1 for a list of other valid values.</b>

---

## Dual Message System Processing

This message describes Dual Message System processing of a Mastercard In Control 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 Network containing the In Control virtual card number in DE 2 (Primary Account Number [PAN]).
2. The Authorization Platform applies unique controls for the In Control 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 (In Control 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 In Control 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 In Control 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 In Control Virtual Card Service**

The Mastercard In Control Virtual Card Service allows issuers to process partial approvals.

Issuers must opt-in to the Mastercard In Control Virtual Card Service when choosing to process partial approvals by registering with Mastercard.

## **Mastercard In Control Real Card Spend Control**

---

The Mastercard In Control 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.

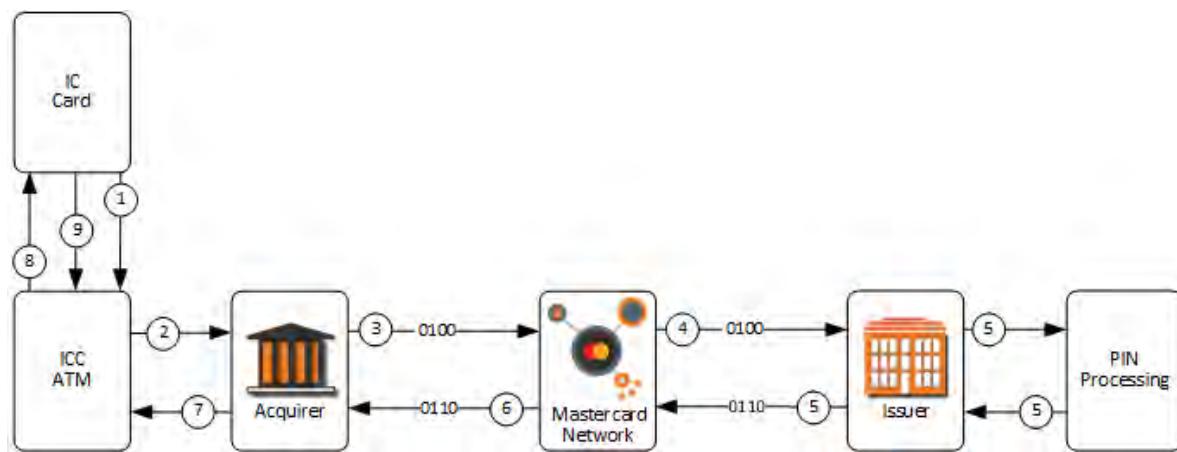
**NOTE: Spend control rules can only be applied to transactions that flow through the Mastercard Network. Spend control rules are not applied to Authorization Advice/0120—Acquirer-generated and Reversal Request/0400 messages.**

## **Process of a Mastercard In Control Service Eligible Transaction**

This message flow describes the stages of the Dual Message System processing for a Mastercard In Control Service-eligible transaction.

The acquirer sends the Authorization Request/0100 message containing the Mastercard In Control real card number in DE 2 (Primary Account Number [PAN]) to the Mastercard Network.

<b>WHEN...</b>	<b>THEN In Control...</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 (In Control—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> <li>• DE 60 (Advice Reason Code): <ul style="list-style-type: none"> <li>– Subfield 1 (Advice Reason Code) contains value 200 (In Control Processing Advice to Issuer)</li> <li>– Subfield 2 (Advice Detail Code) contains a valid advice reason code</li> </ul> </li> </ul> and  Sends the cardholder an alert notification indicating rule failure.
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	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.  and  Sends the cardholder an alert notification indicating rule failure.



**NOTE:** 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 In Control to update the disposition of the transaction.

WHEN...	THEN the Authorization Platform...
Mastercard In Control 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.

## Authorization Request/0100—In Control 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.

Data Element	Org	Sys	Dst	Values/Comments
DE 2 (Primary Account Number)	M	•	M	Account range must participate in Mastercard In Control Real Card Spend Control Service; DE 2 contains the Mastercard In Control real card number
DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 1 (On-behalf [OB] Service)	•	X	C	20 = In Control RCN Spend Control Service

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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—In Control 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 Mastercard In Control 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 = In Control 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 = In Control Processing Advice to Issuer
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 In Control 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 In Control Virtual Card Mapping and Spend Control Service**

The Mastercard In Control platform leverages the same authorization and clearing data elements for mapping virtual card numbers to their real card account numbers as in the Mastercard In Control Purchase Control service and the Mastercard Contactless Mapping service. Issuers currently supporting the Mastercard Contactless Mapping service need only to

recognize new data values in existing data elements to support the Mastercard In Control Virtual Card Mapping and Spend Control service.

## **Authorization Request/0100—In Control 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 a Mastercard In Control Virtual Card Mapping and Spend Control service authorization transaction that was declined by In Control processing.

1. The acquirer sends an Authorization Request/0100 message to the Mastercard Network containing the In Control virtual card number in DE 2 (Primary Account Number [PAN]).
2. The Authorization Platform applies unique controls for the In Control 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 (In Control 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 (In Control Processing Advice to Issuer), subfield 2 (Advice Detail Code) = appropriate advice reason code

## Mastercard Installment Payment Service

The Mastercard Installment Payment Service is a service offered by Mastercard to Dual Message System-connected issuers to support installment payments for authorization and clearing processing. This service enables cardholders to choose to pay for a purchase in installment payments and select the installment payment terms from choices provided at the time of purchase.

For additional guidance on the Mastercard Installment Payment Service, refer to the *Mastercard Installment Payment Service User Guide*, available on Mastercard Connect™.

## Mastercard Merchant Presented QR

This section describes the Mastercard™ Merchant Presented QR (Quick Response) service.

### Overview

Mastercard Merchant Presented QR offers a mobile payment option for person-to-merchant transactions in markets where conventional transactions rely heavily on cash for retail purchases.

Mastercard Merchant Presented QR transactions can only be initiated by customers connected to the Single Message System. Receiving institutions (RI/merchant's bank) that are connected either through the Dual Message System or the Single Message System can receive Mastercard Merchant Presented QR transactions.

Introduced in Release 17.Q4, Mastercard Merchant Presented QR is a consumer-initiated, push payment transaction initiated with a mobile device. Using a smartphone, the consumer makes a cashless payment by scanning a Mastercard Merchant Presented QR code at any merchant location that accepts Mastercard Merchant Presented QR transactions. This product fulfills the need to make payments instantly to merchants in a direct, convenient, and secure method for both the merchant and cardholder.

This product operates in the four-party business model which enables funds to be transferred from a licensed Mastercard originating institution (OI), the consumer's bank, to a receiving institution (RI), the merchant's bank. The transaction originates at the OI and routes to the merchant after successfully authenticating and authorizing the debit from the consumer's account. The RI will process the payment transaction and notify the merchant that the payment has been successfully received. The RI will credit the merchant account after processing the payment transaction.

### For More Information

For more information about Mastercard Merchant Presented QR, refer to the *Mastercard Merchant Presented QR Program Guide*.

## Forms

Forms to support Mastercard Merchant Presented QR enrollment are available on the Forms Library through Mastercard Connect™.

## Authorization Platform Edits

The Authorization Platform will perform the following system edits.

### Mastercard Merchant Presented QR Funding Transaction Processing

The Authorization Platform will validate Mastercard Merchant Presented QR transactions that are identified as follows:

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 28 (Payment Transaction)
- DE 48 (Additional Data), subelement 77 (Funding/Payment Transaction Type Indicator), value C67 (Mastercard Merchant Presented QR)

### Validate Merchant Code

WHEN...	THEN the Authorization Platform...
DE 18 (Merchant Code) contains any one of the following MCCs in an Authorization Request/0100 message for a Mastercard Merchant Presented QR Payment Transaction, Mastercard Merchant Presented QR Refund Payment Transaction, or for a Mastercard Merchant Presented QR Funding Transaction: <ul style="list-style-type: none"><li>• 4829 = Money Transfer</li><li>• 6010 = Manual Cash</li><li>• 6011 = ATM</li><li>• 6532 = Payment Transaction—Customer Financial Institution</li><li>• 6533 = Payment Transaction—Merchant</li><li>• 6538 = MoneySend Funding</li><li>• 6540 = Funding (exclusive of MoneySend)</li><li>• 6555 = MA Initiated Rewards/Rebate</li><li>• 6050 = Quasi Cash</li><li>• 6051 = Quasi Cash—merchant</li></ul>	Will reject the transaction and forward the OI an Authorization Request Response/0110 with: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format error)</li><li>• DE 44 (Additional Response Data) = 018 (indicating the data element in error)</li></ul>

---

### Validate Presence of Mandatory Data

WHEN...	THEN the Authorization Platform...
DE 108 (MoneySend Reference Data), subelement 02 (Sender Data), subfield 11 (Sender Account Number) is not present, not numeric, contains all zeros, or exceeds 20 characters	Will reject the transaction and forward the OI an Authorization Request Response/0110 with <ul style="list-style-type: none"><li>• DE 39 = 30 (format error)</li><li>• DE 44 (Additional Response Data) = 108002 (indicating the data element in error)</li></ul>

### Validate Presence of Mandatory Data

WHEN...	THEN the Authorization Platform...
DE 108 (MoneySend Reference Data), subelement 02 (MoneySend Transaction Data), subfield 3 (Funding Source) is not present or does not contain one of the following values: 01 (Credit), 02 (Debit), 03 (Prepaid), 04 (Deposit Account), 05 (Mobile Money Account), 06 (Cash), or 07 (Reserved)	Will reject the transaction and forward the OI an Authorization Request Response/0110 with <ul style="list-style-type: none"><li>• DE 39 = 30 (format error)</li><li>• DE 44 (Additional Response Data) = 108002 (indicating the data element in error)</li></ul>

---

### Validate Transaction Amount Limit

WHEN...	THEN the Authorization Platform...
The transaction amount limit is exceeded	<p>Will reject the transaction and forward the OI an Authorization Request Response/0110 with</p> <ul style="list-style-type: none"><li>• DE 39 = 05 (Do not honor)</li></ul> <p>An Authorization Advice/0120 message will be sent to the RI with</p> <ul style="list-style-type: none"><li>• DE 60 (Advice Reason Code), subfield 1 (Values, in Authorization Advice/0120), value 151 (Blocking Processing Advice to Issuer [Mastercard Merchant Presented QR]).</li><li>• DE 60, subfield 2 (Values, in Mastercard In Control Service), code 0064 (Reject: Transaction Limit Check).</li><li>• DE 48 (Additional Data—Private Use), subelement 71 (Valid Subfield 1 and Subfield 2 Value Combinations), value 37D (Mastercard Merchant Presented QR Blocking—Transaction Amount Limit Exceeded).</li></ul>

### Validate Cumulative Transaction Amount Limit

WHEN...	THEN the Authorization Platform...
The cumulative transaction amount limit is exceeded	<p>Will reject the transaction and forward the OI an Authorization Request Response/0110 with</p> <ul style="list-style-type: none"><li>• DE 39 = 05 (Do not honor)</li></ul> <p>An Authorization Advice/0120 message will be sent to the RI with</p> <ul style="list-style-type: none"><li>• DE 60 (Advice Reason Code), subfield 1 (Values, in Authorization Advice/0120), value 151 (Blocking Processing Advice to Issuer [Mastercard Merchant Presented QR]).</li><li>• DE 60, subfield 2 (Values, in Mastercard In Control Service), code 0065 (Reject: Cumulative Limit Check).</li><li>• DE 48 (Additional Data—Private Use), subelement 71 (Valid Subfield 1 and Subfield 2 Value Combinations), value 37E (Mastercard Merchant Presented QR Blocking—Cumulative Transaction Amount Limit Exceeded).</li></ul>

### Validate the Originating Institution

WHEN...	THEN the Authorization Platform...
The Originating Institution, not registered for participation in the Mastercard Merchant Presented QR service, submits a transaction containing DE 48 (Additional Data), subelement 77 (Funding/Payment Transaction Type Indicator), value C67	<p>Will reject the transaction and forward the OI an Authorization Request Response/0110 with</p> <ul style="list-style-type: none"><li>• DE 39 = 58 (Transaction not permitted to acquirer/terminal)</li></ul>

## Domestic Activity

WHEN...	THEN the Authorization Platform...
If the Mastercard Merchant Presented QR RI has chosen to limit Mastercard Merchant Presented QR to domestic activity, then if the PAN country code does not equal the country code value in DE 32 (Acquiring Institution Identification Code)	<p>Will reject the transaction and forward the OI an Authorization Request Response/0110 with</p> <ul style="list-style-type: none"><li>• DE 39 = 05 (Do not honor)</li></ul> <p>An Authorization Advice/0120 message is sent to the RI with</p> <ul style="list-style-type: none"><li>• DE 60 (Advice Reason Code), subfield 1 (Values, in Authorization Advice/0120), code 151 (In Control Processing Advice to Issuer [Mastercard Merchant Presented QR]).</li><li>• DE 60, subfield 2 (Values, in Mastercard In Control Service) code 0072 (Reject: Geographic Restriction).</li><li>• DE 48 (Additional Data—Private Use), subelement 71 (Valid Subfield 1 and Subfield 2 Value Combinations), value 37F (Mastercard Merchant Presented QR Blocking—Domestic Activity Only).</li></ul>

## Valid Authorization Messages

WHEN...	THEN the Authorization Platform...
The Originating Institution submits an Authorization Request/0100 message for a valid Mastercard Merchant Presented QR transaction	<p>Will forward the Authorization Request/0100 message to the RI with</p> <ul style="list-style-type: none"><li>• DE 48, subelement 71, subfield 1, subfield 2, containing value 37V (Valid).</li></ul>
The Originating Institution submits an Authorization Request/0100 message for any other system issue that prevents successful Mastercard Merchant Presented QR service processing	<p>Will forward the Authorization Request/0100 message to the RI with</p> <ul style="list-style-type: none"><li>• DE 48, subelement 71, subfield 1, subfield 2, containing value 37U (Unable to process).</li></ul>

## Reject Reversal Messages

WHEN...	THEN the Authorization Platform...
The Originating Institution submits a Reversal Request/0400 message for a Mastercard Merchant Presented QR transaction	Will reject the transaction and forward the OI a Reversal Request Response/0410 with <ul style="list-style-type: none"><li>• DE 39 = 58 (Transaction not permitted to acquirer/terminal)</li></ul>

## Edits on Payment Transactions

**NOTE: The following edits become effective as of 12 June 2018.**

WHEN...	THEN the Authorization Platform...
DE 108 (MoneySend Reference Data), subelement 05 (Digital Account Information), subfield 01 (Digital Account Reference Number) in an Authorization Request/0100 message does not contain a valid PAN	Will reject the message and respond to the Originating Institution with an Authorization Request Response/0110 message that contains <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 12 (Invalid)</li></ul>
DE 108 (MoneySend Reference Data), subelement 05 (Digital Account Information), subfield 01 (Digital Account Reference Number) in an Authorization Request/0100 message is not properly formatted <ul style="list-style-type: none"><li>• DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 28 (Payment Transaction)</li><li>• DE 48 (Additional Data), subelement 77 (Funding/Payment Transaction Type Indicator), value C67 (Mastercard Merchant Presented QR)</li></ul>	Will reject the message and respond to the Originating Institution with an Authorization Request Response/0110 message that contains <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format error)</li></ul>

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 108 (MoneySend Reference Data), subelement 05 (Digital Account Information), subfield 01 (Digital Account Reference Number) in an Authorization Request/0100 message contains a Digital Account Reference Number that is already assigned or is mapped to a different funding account	<p>Will reject the message and respond to the Originating Institution with an Authorization Request Response/0110 message that contains</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 12 (Invalid)</li> </ul>
DE 108 (MoneySend Reference Data), subelement 05 (Digital Account Information), subfield 01 (Digital Account Reference Number) is not contained in an Authorization Request/0100 message, and the value in DE 108 (MoneySend Reference Data), subelement 02 (Sender Data), subfield 11 (Sender Account Number) is a valid Mastercard PAN	<p>Will populate DE 108, subelement 05 (Digital Account Information), subfield 01 (Digital Account Reference Number) in the Authorization Request/0100 message and forward the message to the Receiving Institution/Merchant bank.</p>
DE 108 (MoneySend Reference Data), subelement 05 (Digital Account Information), subfield 01 (Digital Account Reference Number) is not contained in an Authorization Request/0100 message, the value in DE 108, subelement 02, subfield 11 is not a valid Mastercard PAN	<p>Will forward the message to the Receiving Institution without the PAN field populated. The merchant will handle the refund as a manual cash distribution.</p>
The Originating Institution submits a Reversal Request/0400 message for a Mastercard Merchant Presented QR Refund transaction	<p>Will reject the message and respond to the Originating Institution with a Reversal Request Response/0410 message that contains</p> <ul style="list-style-type: none"> <li>• DE 39 = 58 (Transaction not permitted to acquirer/terminal)</li> </ul>

---

### Edit on Funding Transactions

**NOTE: The following edit becomes effective as of 6 November 2018.**

WHEN...	THEN the Authorization Platform...
The Originating Institution is not registered for participation in the Mastercard Merchant Presented QR service and submits a funding transaction in an Authorization Request/0100 message containing DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 00 (Purchase) and DE 48 (Additional Data—Private Use), subelement 77 (Funding/Payment Transaction Type Indicator), value C67 (Mastercard Merchant Presented QR)	Will reject the message and respond to the Originating Institution with an Authorization Request Response/0110 message that contains: <ul style="list-style-type: none"><li>• DE 39 = 58 (Transaction not permitted to acquirer/terminal)</li></ul>

### Edit on Refund Payment Transactions

**NOTE: The following edit becomes effective as of 12 June 2018.**

WHEN...	THEN the Authorization Platform...
The Receiving Institution is not registered for participation in the Mastercard Merchant Presented QR service and submits a refund transaction in an Authorization Request/0100 message containing DE 48 (Additional Data—Private Use), subelement 77 (Funding/Payment Transaction Type Indicator), value C68 (Mastercard Merchant Presented QR Refund)	Will reject the message and respond to the Originating Institution with an Authorization Request Response/0110 message that contains <ul style="list-style-type: none"><li>• DE 39 = 58 (Transaction not permitted to acquirer/terminal)</li></ul>

### Mastercard Merchant Presented QR Payment Transaction

**NOTE: The following edit is already effective for Receiving Institutions and becomes effective as of 10 August 2018 for Originating Institutions.**

WHEN...	THEN the Authorization Platform...
The individual transaction limit or the cumulative transaction amount or count limit is exceeded in an Authorization Request/0100 message for a Mastercard Merchant Presented QR Payment Transaction	<p>Will reject the message and forward the Originating Institution an Authorization Request Response/0110 message with:</p> <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 05 (Do Not Honor)</li></ul> <p>Will reject the message and forward to the Receiving Institution an Authorization Advice/0120—System-Generated message with:</p> <ul style="list-style-type: none"><li>• DE 48 (Additional Data), subelement 71 (On-behalf Service [OBS]), subfield 1 (On-behalf Service Indicator), value 37 (Mastercard Merchant Presented QR Blocking Service)</li><li>• DE 48, subelement 71, subfield 2 (On-behalf Result 1), value E (Mastercard Merchant Presented QR Blocking—Cumulative Transaction Amount or Count Limit Exceeded)</li><li>• DE 60 (Advice Reason Code), in the table Subfield 1 Values, in Authorization Advice/0120, value 151 (In Control Processing Advice to Issuer [Mastercard Merchant Presented QR])</li><li>• DE 60, in the table Subfield 2 Values, in Mastercard Merchant Presented QR Service, value 0064 (Reject: Transaction Limit Check) when the individual transaction limit is exceeded</li></ul> <p>Or</p> <ul style="list-style-type: none"><li>• DE 60, in the table Subfield 2 Values, in Mastercard Merchant Presented QR Service, value 0065 (Reject: Cumulative Limit Check) when the cumulative counts or amounts limit is exceeded</li></ul>

## Mastercard Merchant Presented QR Funding Transaction

**NOTE: The following edits become effective as of 6 November 2018.**

WHEN...	THEN the Authorization Platform...
An Authorization Request/0100 message for a Mastercard Merchant Presented QR Funding Transaction does not contain DE 108 (MoneySend Reference Data), subelement 03 (MoneySend Transaction Data), subfield 01 (Unique Transaction Reference)	Will reject the transaction and forward the OI an Authorization Request Response/0110 with: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format error)</li><li>• DE 44 (Additional Response Data) = 108003 (indicating the data element)</li></ul>
An Authorization Request/0100 message for a Mastercard Merchant Presented QR Funding Transaction contains DE 108 (MoneySend Reference Data), subelement 05 (Digital Account Information), subfield 02 (Mastercard Merchant Presented QR Receiving Account Number): <ul style="list-style-type: none"><li>• That is not a valid length</li><li>• That is not alphanumeric special characters</li><li>• That contains leading spaces</li><li>• That contains all zeros</li></ul>	Will reject the transaction and forward the OI an Authorization Request Response/0110 with: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format error)</li><li>• DE 44 (Additional Response Data) = 108005 (indicating the data element in error)</li></ul>
An Authorization Request/0100 message for a Mastercard Merchant Presented QR Funding Transaction contains DE 108 (MoneySend Reference Data), subelement 06 (Dynamic QR Data): <ul style="list-style-type: none"><li>• That is not a valid length</li><li>• That is not alphanumeric special characters</li></ul>	Will reject the transaction and forward the OI an Authorization Request Response/0110 with: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format error)</li><li>• DE 44 (Additional Response Data) = 108006 (indicating the data element in error)</li></ul>

### Mastercard Merchant Presented QR Refund Transaction

**NOTE: The following edit becomes effective as of 10 August 2018 for both Receiving Institutions and Originating Institutions.**

WHEN...	THEN the Authorization Platform...
The individual transaction limit or the cumulative transaction amount or count limit is exceeded in an Authorization Request/0100 message for a Mastercard Merchant Presented QR Refund Transaction	<p>Will reject the message and forward to the Receiving Institution an Authorization Request Response/0110 message with:</p> <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 05 (Do Not Honor)</li></ul> <p>Will reject the message and forward to the Originating Institution an Authorization Advice/0120—System-Generated message with:</p> <ul style="list-style-type: none"><li>• DE 48 (Additional Data), subelement 71 (On-behalf Service [OBS]), subfield 1 (On-behalf Service Indicator), value 37 (Mastercard Merchant Presented QR Blocking Service)</li><li>• DE 48, subelement 71, subfield 2 (On-behalf Result 1), value E (Mastercard Merchant Presented QR Blocking—Cumulative Transaction Amount or Count Limit Exceeded)</li><li>• DE 60 (Advice Reason Code), in the table Subfield 1 Values, in Authorization Advice/0120, value 151 (In Control Processing Advice to Issuer [Mastercard Merchant Presented QR])</li><li>• DE 60, in the table Subfield 2 Values, in Mastercard Merchant Presented QR Service, value 0064 (Reject: Transaction Limit Check) when the individual transaction limit is exceeded</li></ul> <p>Or</p> <ul style="list-style-type: none"><li>• DE 60, in the table Subfield 2 Values, in Mastercard Merchant Presented QR Service, value 0065 (Reject: Cumulative Limit Check) when the cumulative counts or amounts limit is exceeded</li></ul>

## Mastercard Merchant Presented QR Refund Payment Processing

**NOTE: The following edit becomes effective as of 12 June 2018.**

WHEN...	THEN the Authorization Platform...
The Receiving Institution submits an Authorization Request/0100 message for a Mastercard Merchant Presented QR refund transaction it will contain the Digital Account Reference Number in DE 2 (Primary Account Number [PAN])	Will include this value in DE 2 of the Authorization Request/0100 message sent to the Originating Institution.  In addition, the following data will be provided in DE 108 (MoneySend Reference Data): <ul style="list-style-type: none"><li>• Subelement 02 (Sender Data), subfield 11 (Sender Account Number)</li><li>• Subelement 03 (MoneySend Transaction Data), subfield 03 (Funding Source)</li></ul>

## Alternate Processing

If the RI is unable to respond, Mastercard Merchant Presented QR transactions will be declined.

In the event that the Mastercard Merchant Presented QR Blocking Service is not available:

- The platform which called the service will receive notice that the service is not available and the following information is sent to the RI in the Authorization Request/0100 message for an authorization decision.
  - DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Service), subfield 1 (On-behalf Service Indicator), value 37 (Mastercard Merchant Presented QR Blocking Service)
  - DE 48, subelement 71, subfield 2 (On-behalf Result 1), value U (Unable to process)

For Stand-In processing guidelines, refer to the *Mastercard Merchant Presented QR Program Guide*.

## Alternate Processing for Refund Payment Transactions

**NOTE: Alternate processing for refund payment transactions becomes effective as of 12 June 2018.**

If the Consumer's bank is unable to respond to a payment or refund payment request, the Mastercard Merchant Presented QR refund transaction will be declined.

Stand-In limits will be set to zero.

Stand-In processing guidelines will be published in a future update of the *Mastercard Merchant Presented QR Program Guide*.

### X-Code Processing

Mastercard Merchant Presented QR transactions will be declined by the Dual Message System (Authorization) in X-Code processing responding to the originator with DE 39 (Response Code), value 91 (Authorization System or issuer system inoperative).

## Mastercard MoneySend

---

The Mastercard® MoneySend™ service enables person-to-person transfers, account-to-account transfers, agent cash out, credit card bill payment, business to consumer disbursement, government/non-government organization to consumer disbursement, and business 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.

### Authorization Request/0100—Mastercard MoneySend Funding Transactions

Originating Financial Institutions (OFI) that are registered for the 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 (MoneySend Funding)
DE 48 (Additional Data—Private Use), TCC	M	•	M	R = Face-to-face retail or T = Non-face-to-face retail

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48, subelement 77 (Payment Transaction Type Indicator)	M	•	M	C07 = MoneySend Person-to-Person C52 = MoneySend Account-to-Account Transfer C53 = MoneySend Agent Cash Out C54 = MoneySend Credit Card Bill Payment C55 = MoneySend Business Disbursement C56 = MoneySend Government/Non-profit Disbursement C57 = MoneySend Acquirer Merchant Settlement C67 = Inter Platform Person-to-Person
DE 108, MoneySend Reference Data	O	•	C	Optional for all MoneySend Funding Transactions and required for all MoneySend Payment Transactions.
DE 124 (MoneySend, Sender Identification Data)	O	X	C	Acquirers may optionally send DE 124, subfields 1–4 containing sender identification data when the Authorization Request/0100 message is a MoneySend Funding 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 MoneySend transaction.

---

### **Reversal Request/0400—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.

<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 = Funding Transaction
DE 18 (Merchant Type)	M	•	M	MCC 6538 (MoneySend Funding)

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48 (Additional Data—Private Use), TCC	M	•	M	R = Face-to-face retail or T = Non-face-to-face retail
DE 108 (MoneySend Reference Data)	O	•	C	Optional for all MoneySend Payment and Funding Transactions.
DE 124 (MoneySend, 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 MoneySend 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>

## 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.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>DE 3 (Processing Code), value 00 (Purchase Transaction) is present And DE 18 (Merchant Type), value 6538 (MoneySend Funding) 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 MoneySend platform</p>	<p>Rejects the transaction 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).</p>

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Funding Transaction where: <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 00</li> <li>• DE 18 contains MCC 6538</li> <li>• DE 48, subelement 77 does not contain value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 48 (Transaction Category Codes) contains R (Face-to-face retail) or T (Non-face-to-face retail)</li> </ul>	Sends the Originating Institution an Authorization Request Response/0110 to include the following: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 048077 (indicating the data element in error)</li> </ul>
The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Funding Transaction where: <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 00</li> <li>• DE 18 does not contain value 6538</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 48 (Transaction Category Codes) contains R (Face-to-face retail) or T (Non-face-to-face retail)</li> </ul>	Sends the Originating Institution an Authorization Request Response/0110 to include the following: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 018 (indicating the data element in error)</li> </ul>
The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Funding Transaction where: <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 00</li> <li>• DE 18 contains MCC 6538</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 48 (Transaction Category Codes) does not contain value R (Face-to-face retail) or T (Non-face-to-face retail)</li> </ul>	Sends the Originating Institution an Authorization Request Response/0110 to include the following: <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 0480nn (where nn is the subelement number)</li> </ul>

## Authorization Request/0100—MoneySend Payment Transactions

Originating Financial Institutions (OFI) that are registered for the 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.

<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 18 (Merchant Type)	M	•	M	Must be one of the following values: MCC 6536 (MoneySend Intracountry) MCC 6537 (MoneySend Intercountry)
DE 48 (Additional Data—Private Use), TCC	M	•	M	P = Payment Transaction
DE 48, subelement 77 (Funding/ Payment Transaction Type Indicator)	C	•	C	C07 = MoneySend Person-to-Person C52 = MoneySend Account-to-Account Transfer C53 = MoneySend Agent Cash Out C54 = MoneySend Credit Card Bill Payment C55 = MoneySend Business Disbursement C56 = MoneySend Government/Non-profit Disbursement C57 = MoneySend Acquirer Merchant Settlement C67 = Inter Platform Person-to-Person
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				At a bank branch      0 = Not a CAT transaction
At an ATM				At an ATM      1 = Authorized Level 1 CAT: Automated dispensing machine with PIN
At an unmanned kiosk				At an unmanned kiosk      2 = Authorized Level 2 CAT: Self-service terminal
On the Internet				On the Internet      6 = Authorized Level 6 CAT: Electronic commerce

Data Element	Org	Sys	Dst	Values/Comments
DE 108 (MoneySend Reference Data)	O	X	C	Optional for all MoneySend Funding Transactions and required for all MoneySend Payment Transactions.
DE 124 (MoneySend, Sender Identification Data)	M	•	M	<p>Acquirers must send DE 124, subfields 2 and 3 containing sender identification data when the Authorization Request/0100 message is a MoneySend Payment Transaction (subfields 1 and 4 are optional).</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 MoneySend transaction.</p>

### Reversal Request/0400—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	<p>Must be one of the following values:</p> <p>MCC 6536 (MoneySend Intracountry)</p> <p>MCC 6537 (MoneySend Intercountry)</p>
DE 48 (Additional Data—Private Use), TCC	M	•	M	P = Payment Transaction

Data Element	Org	Sys	Dst	Values/Comments
DE 48, subelement 77, (Funding/ Payment Transaction Type Indicator)	C	•	C	<p>C07 = MoneySend Person-to-Person</p> <p>C52 = MoneySend Account-to-Account Transfer</p> <p>C53 = MoneySend Agent Cash Out</p> <p>C54 = MoneySend Credit Card Bill Payment</p> <p>C55 = MoneySend Business Disbursement</p> <p>C56 = MoneySend Government/Non-profit Disbursement</p> <p>C57 = MoneySend Acquirer Merchant Settlement</p> <p>C67 = Inter Platform Person-to-Person</p>
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: C07, C52–C57, C67
				<b>IF... 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
				On the Internet      6 = Authorized Level 6 CAT: Electronic commerce
DE 108 (MoneySend Reference Data)	C	X	C	<p>Conditional for acquirers to send for all MoneySend Payment Transactions and optional for all MoneySend Funding Transactions.</p> <p>Issuers are required to send DE 108 in the response message; issuers must echo—<b>unedited</b>—the information sent by the originator/acquirer.</p>

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 124 (MoneySend, Sender Identification Data)	M	•	M	<p>Acquirers must send DE 124, subfields 2 and 3 containing sender identification data when the Authorization Request/0100 message is a MoneySend Payment Transaction (subfields 1 and 4 are optional).</p> <p>In DE 124 of the response message, issuers must echo—<b>unedited</b>—the information sent by the originator/acquirer.</p>

---

**NOTE: A MoneySend Payment Transaction may only be reversed by the acquirer for reason of a documented clerical error and upon agreement with the issuer. In such an event, the error must be reversed within 24 hours of the date the MoneySend Payment Transaction was authorized.**

### 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.

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
When an OFI identified by the ICA number provided in DE 32 (Acquiring Institution ID Code) attempts to submit a MoneySend Payment Transaction but has not registered for the MoneySend 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).

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the MoneySend service and is submitting a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 does not contain MCC 6536 or MCC 6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met <ul style="list-style-type: none"> <li>– 0 = Not a CAT transaction</li> <li>– 1 = Authorized Level 1 CAT: Automated dispensing machine with PIN</li> <li>– 2 = Authorized Level 2 CAT: Self-service terminal</li> <li>– 6 = Authorized Level 6 CAT: Electronic commerce</li> </ul> </li> <li>• DE 124 is present</li> </ul>	<p>Sends the OFI an Authorization Request Response/0110 or Reversal Response/0410 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 018 (Merchant Type)</li> </ul>
<p>The OFI is registered for the MoneySend service and is submitting a MoneySend 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, C52, C53, C54, C55, C56, C57, or C67</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 MoneySend service and is submitting a MoneySend 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, C52, C53, C54, C55, C56, C57, or C67</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 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>

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</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 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 MoneySend platform	Declines the request and sends the OFI an Authorization Request Response/0110 message where DE 39 = 58 (Transaction not permitted to acquirer/terminal)
An issuing country, RFI, or RFI's account range is not able to offer the MoneySend 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 MoneySend Payment Transactions do not require UCAF data (DE 48, subelement 43).**

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 124, subfield 3 Street Address or Country code is not present or contains all zeros or spaces.</li> </ul>	<p>Sends the OFI an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30 (Format Error)</li> <li>• DE 44 = 124 (Merchant-defined Data)</li> </ul>

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 124, subfield 3 Country code is present but not a valid ISO recognized alpha Country code (Refer to the <i>Quick Reference Booklet</i> for valid Alpha [3 Characters] Country code)</li> </ul>	<p>Sends the OFI an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 124 (Merchant-defined Data)</li> </ul>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 124, subfield 3 Country code is valid but blocked (part of the MoneySend Blocking Country List)</li> </ul>	<p>Sends the OFI an Authorization Request Response/0110 to include the following:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 12 (Invalid Transaction)</li> </ul> <p>and</p> <p>Sends the RFI an Authorization Advice Message/0120 where:</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1, value 33 (MoneySend Blocking Service)</li> <li>• DE 48, subelement 71, subfield 2, value W (MoneySend Mastercard Blocking—Country not allowed for the MoneySend Transaction)</li> <li>• DE 60, subfield 1, value 200 (In Control Processing Advice to Issuer)</li> <li>• DE 60, subfield 2, value 0072 (Reject: Geographic Restriction)</li> </ul>

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC value 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 124, subfield 3 country code is USA or CAN</li> <li>• DE 124, subfield 3 State code is not present or contains all zeros or spaces or invalid code for USA and CAN</li> </ul>	<p>Sends the OFI an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 124 (Merchant-defined Data)</li> </ul>

#### **DE 108, Subelement 01, Subfield 01 (Receiver/Recipient First Name) and Subfield 03 (Receiver/Recipient Last Name)—Edit Check**

The Authorization Platform will perform the following system edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a cross-border MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 subfield is present and criteria is met</li> <li>• DE 108, subelement 01, subfield 01 (Receiver First Name) and DE 108, subelement 01, subfield 03 (Receiver Last Name) are present and contain all spaces or all numeric values</li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li> </ul>

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a cross-border MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met for MoneySend: <ul style="list-style-type: none"> <li>– 0 = Not a CAT transaction</li> <li>– 1 = Authorized Level 1 CAT: Automated dispensing machine with PIN</li> <li>– 2 = Authorized Level 2 CAT: Self-service terminal</li> <li>– 6 = Authorized Level 6 CAT: Electronic commerce</li> </ul> </li> <li>• DE 124 subfield is present and criteria are met</li> <li>• DE 108 is present and all criteria are met except: <ul style="list-style-type: none"> <li>– Subelement 01 (Receiver/Recipient Data) is present and subfield 01 (Receiver First Name), OR subfield 03 (Receiver Last Name) is absent</li> </ul> </li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li> </ul>

---

#### **DE 108, Subelement 01, Subfield 06 (Receiver/Recipient State/Province Code)—Edit Check**

The Authorization Platform will perform the following system edits.

<sup>37</sup> DE 124 (Member-defined Data) criteria includes:

- Subfield 2 (Sender/Payer Name/User ID) contains the sender name.
- Subfield 3 (Sender/Payer Address) contains sender address with applicable state and country code.

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 subfield is present and criteria is met</li> <li>• DE 108, subelement 01, subfield 07 (Receiver/Recipient Country) is U.S. or Canada.</li> <li>• DE 108, subelement 01, subfield 06 (Receiver State Code) is present and contains all zeros or spaces or invalid state code for U.S. or invalid province code for Canada.</li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li> </ul>

---

#### **DE 108, Subelement 01, Subfield 07 (Receiver/Recipient Country Code)—Edit Check**

The Authorization Platform will perform the following system edits.

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 subfield is present and criteria is met</li> <li>• DE 108, subelement 01, subfield 07 (Receiver/Recipient Country) is present and contains all spaces</li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li> </ul>

---

WHEN...	THEN the Authorization Platform...
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537/6538</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 subfield is present and criteria is met</li> <li>• DE 108, subelement 01, subfield 07 (Receiver/Recipient Country) is present but is an invalid country code (not per ISO standard)</li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li> </ul>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 subfield is present and criteria is met</li> <li>• DE 108, subelement 01, subfield 07 (Receiver/Recipient Country) is present and is a valid country code but is blocked (Part of the MoneySend Blocking Country List)</li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 12 (Invalid Transaction)</li> </ul> <p>and</p> <p>Sends an Authorization Advice Message/0120 to the issuer where:</p> <ul style="list-style-type: none"> <li>• DE 48, subelement 71, subfield 1, value 33 (MoneySend Blocking Service)</li> <li>• DE 48, subelement 71, subfield 2, value W (MoneySend Mastercard Blocking—Country not allowed for the MoneySend Transaction—Sender/Receiver Data)</li> <li>• DE 60, subfield 1, value 200 (In Control Processing Advice to Issuer)</li> <li>• DE 60, subfield 2, value 0072 (Reject: Geographical Restrictions)</li> </ul>

**NOTE: Transaction will be declined if the sender Country is subject to comprehensive geographic sanctions published by the Office of Foreign Assets Control (OFAC), <http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx>. The current list of countries subject to such sanctions is Cuba, Iran, North Korea, Sudan, and Syria; however, this list is subject to change.**

---

### **DE 108, Subelement 01, Subfield 12 (Receiver Identification Type)—Edit Check**

The Authorization Platform will perform the following system edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"><li>• DE 3, subfield 1 contains value 28</li><li>• DE 18 contains MCC values 6536/6537</li><li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li><li>• DE 61, subfield 10 criteria is met</li><li>• DE 124 subfield is present and criteria are met</li><li>• DE 108 subelement 01, subfield 12 (Receiver Identification Type) is present and does not contain one of the values 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 10</li></ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format error)</li><li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li></ul>

### **DE 108, Subelement 02, Subfield 01 (Sender First Name), and Subfield 03 (Sender Last Name)—Edit Check**

The Authorization Platform will perform the following system edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"><li>• DE 3, subfield 1 contains value 28</li><li>• DE 18 contains MCC values 6536/6537</li><li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li><li>• DE 61, subfield 10 criteria is met</li><li>• DE 124 is present and valid</li><li>• DE 108, subelement 02, subfield 01 (Sender First Name) and DE 108, subelement 02, subfield 03 (Sender Last Name) are present and contain all spaces or all numeric values</li></ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"><li>• DE 39 = 30</li><li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li></ul>

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 is present and valid</li> <li>• DE 108, subelement 02 (Sender Data) is present and DE 108, subelement 02, subfield 01 (Sender First Name) OR subfield 03 (Sender Last Name) is absent</li> </ul>	<p>Sends an Authorization Request Response/ 0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li> </ul>

---

#### **DE 108, Subelement 02, Subfield 11 (Sender Account Number)—Edit Check**

The Authorization Platform will perform the following system edits.

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 is present and valid</li> <li>• DE 108, subelement 02, subfield 11 (Sender Account Number) is present and contains all spaces or special characters</li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li> </ul>

---

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 is present and valid</li> <li>• DE108, subelement 02, subfield 11 (Sender Account Number) is absent</li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li> </ul>

---

#### **DE 108, Subelement 02, Subfield 12 (Sender Identification Type)—Edit Check**

The Authorization Platform will perform the following system edits.

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a cross-border MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 subfield is present and criteria are met</li> <li>• DE 108 subelement 02, subfield 12 (Sender Identification Type) is present and does not contain one of the values 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 10</li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 1080nn (where nn is the subelement number)</li> </ul>

---

#### **DE 108, Subelement 03, Subfield 03 (Funding Source)—Edit Check**

The Authorization Platform will perform the following system edits.

WHEN...	THEN the Authorization Platform...
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"><li>• DE 3, subfield 1 contains value 28</li><li>• DE 18 contains MCC values 6536/6537</li><li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li><li>• DE 61, subfield 10 criteria is met</li><li>• DE 124 is present and valid</li><li>• DE 108, subelement 03, subfield 03 (Funding Source) is present and does not contain one of the values 01, 02, 03, 04, 05, 06, 07</li></ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format error)</li><li>• DE 44 (Additional Response Data) = 108003 (indicating the data element in error)</li></ul>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"><li>• DE 3, subfield 1 contains value 28</li><li>• DE 18 contains MCC values 6536/6537</li><li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li><li>• DE 61, subfield 10 criteria is met</li><li>• DE 124 is present and valid</li><li>• DE 108, subelement 03, subfield 03 (Funding Source) is absent</li></ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format error)</li><li>• DE 44 (Additional Response Data) = 108003</li></ul>

### **DE 108, Subelement 03, Subfield 05 (Transaction Purpose)—Edit Check**

The Authorization Platform will perform the following system edits.

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07, C52, C53, C54, C55, C56, C57, or C67</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 is present and valid</li> <li>• DE 108, subelement 03, subfield 05 (Transaction Purpose) is present and does not contain one of the values 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, 13, 14, 15</li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 108003 (indicating the data element in error)</li> </ul>

---

### Other Edits

The Authorization Platform will perform the following system edits.

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The OFI is registered for the Mastercard MoneySend service and is submitting an Authorization Request/0100 message for a MoneySend Payment Transaction to a credit card (MCC) that is issued in country U.S. (840) where:</p> <ul style="list-style-type: none"> <li>• DE 3, subfield 1 contains value 28</li> <li>• DE 18 contains MCC values 6536/6537</li> <li>• DE 48, subelement 77 contains value C07</li> <li>• DE 61, subfield 10 criteria is met</li> <li>• DE 124 is present and valid</li> </ul>	<p>Sends an Authorization Request Response/0110 message to the acquirer where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 12 (Invalid Transactions)</li> </ul>

---

### Mastercard MoneySend Issuer Transaction Controls

The Mastercard® MoneySend™ Issuer Transaction Controls is an On-behalf Service that Receiving Institutions can use to manage their risk. Monitoring and blocking options include velocity by number of transactions and cumulative dollar amount, and sanction score.

### Network Blocking

Mastercard sets single transaction amount and 30 day accumulative amount limits to receiving accounts for MoneySend Payment Transactions. The maximum amount limit for single

transactions and 30 day accumulative amount limits vary by program type. Mastercard will decline transactions over the set limits with DE 39, value 05 (Do not honor).

## **Sanction Screening**

Mastercard provides a Sanction Screening service to assist with meeting Anti-Money Laundering (AML) obligations. The Sanction Screening score is provided to acquirers and issuers and will be available for all cross-border MoneySend Payment transactions and domestic MoneySend Payment transactions in Egypt, Canada, across Europe and the U.S. This service provides a score based on screening the individual sender name (consumer, business, government, and non-government) in the authorization message to support real-time decision making.

## **For More Information About Implementing the MoneySend Program**

For more information about implementing the MoneySend program, refer to the Mastercard *MoneySend Program Guide* or contact the Global Customer Service team.

## **Mastercard Safety Net**

---

This section provides a brief overview of the Mastercard Safety Net service, part of the Mastercard Global Safety and Security Standards suite of services.

### **Summary and Background**

Mastercard Safety Net provides issuers with a second line of defense to limit the impact of a large-scale fraud attack on one or more of their payment channels (for example, in ATM or e-commerce) when their payment systems are breached. The service also identifies when large-scale fraud attacks are occurring, utilizing insights from the Mastercard Network, so that appropriate action can be taken by the issuer. It does not replace an issuer's primary fraud prevention system. Issuers may alternatively enroll in the Safety Net Alert Only feature.

In November 2015, all issuers were automatically enrolled in Mastercard Safety Net. Previously issuers were required to submit a request if they wanted to opt out of the service.

Effective 21 April 2017 for all issuers except Ukraine, and effective July 2017 for Ukraine issuers, issuers must participate in the Mastercard Safety Net service except when processing Russian domestic transactions.

As applicable, Mastercard requires issuers to participate in Mastercard Safety Net across their entire consumer and commercial credit and debit portfolios, without the availability of an opt-out.

Issuers may enroll in the Mastercard Safety Net Alert Only option if desired through "Manage My Accounts" in Mastercard Connect™.

### **Data Requirements**

If a transaction is declined by the Safety Net service, issuers will receive an Authorization Advice/0120 message with the following values:

- DE 48, subelement 71, subfield 1 = 18 (Fraud Scoring Service)
- DE 48, subelement 71, subfield 2 = C (Fraud Scoring Service was performed successfully)
- DE 48, subelement 75, subfield 1 = 998 or 000
- DE 48, subelement 75, subfield 2 = NM (Network Monitor)
- DE 60, subfield 1 = 120 (Transaction Blocking)
- DE 121 = 000003 (Decline occurred due to an on-behalf service)

For more information about these data elements and values, refer to the Data Element Definitions chapter of this manual.

### **Mastercard Global Safety and Security Standards Roadmap**

Mastercard Safety Net is part of the Mastercard Global Safety and Security Standards Roadmap introduced to help participants in the Mastercard Network continue to benefit from the industry-leading safety and security practices and solutions provided by Mastercard.

The Mastercard Global Safety and Security Roadmap accommodates new innovations, such as support for next-generation solutions and new fraud tools that address increasingly digital environments.

The roadmap encompasses a series of rules and processing requirements for acquirers and issuers to help ensure the continued safety and security of the Mastercard Network and to protect the Mastercard brand. The requirements include participation in:

- Transaction alerts
- Mastercard Automatic Billing Updater (ABU)
- Mastercard Safety Net
- Security-related fields in the Dual Message System (Authorization)
- Authorization Accountholder Authentication Value (AAV) Validation Service

The ability to support these requirements will ensure that issuers have access to important safety and security services available on the Mastercard Network if needed to support their fraud and authorization strategy. Coding for the fields associated with these services, including the Mastercard Safety Net fields described previously, will allow issuers to benefit from advanced solutions that will address new threats as they emerge.

### **For More Information**

For more information or questions on Mastercard Safety Net or the Mastercard Global Safety and Security Standards Roadmap, contact the Global Customer Service team.

---

## **Masterpass Transactions**

---

This section provides a brief overview of the Masterpass™ by Mastercard® service.

Masterpass is a secure and convenient method for consumers to conduct e-commerce wallet transactions or transactions originated from other wallets. Masterpass enables e-commerce

merchants to convert browsing customers into buyers by providing a fast, convenient, and secure checkout experience.

## How It Works

The following information provides a high-level overview of the Masterpass wallet transaction process:

1. The consumer clicks the **Masterpass** button (or the **BUY WITH Masterpass** button) on a merchant's website to go the Masterpass sign-in page.
2. The consumer chooses the integrated Masterpass digital wallet that he or she wants to use, and then successfully completes authentication.
3. The consumer selects the preferred payment card and shipping address.
4. Masterpass securely transfers the consumer's payment and shipping information to the merchant's website confirmation page, where the merchant completes the checkout process.
5. The consumer's payment information is submitted to the merchant's acquirer for processing.

## Authorization Processing

Masterpass transactions submitted to the Masterpass platform for processing are identified by DE 48 (Additional Data—Private Use), subelement 26 (Wallet Program Data), subfield 1 (Wallet Identifier) containing a three-digit value.

Masterpass transactions are identified in the following messages:

- Authorization Request/0100
- Authorization Advice/0120—Acquirer-generated
- Authorization Advice/0120—System-generated

**NOTE: Acquirers in the Europe region must support the Masterpass identifiers in these authorization messages.**

The data values are generated by the Masterpass platform and passed to the merchant along with the consumer's checkout information (for example, card credentials, shipping address, and email address).

There will not be an edit to determine if these values are present; however, if a value exists, it will be validated and rejected if it consists of special characters, all zeros, or spaces.

## For More Information

More information on Masterpass can be found at [www.masterpass.com](http://www.masterpass.com).

## Authorization Request/0100—Masterpass Online Wallet

Following is a list of the data elements and values applicable to this message type. All mandatory Authorization Request/0100 data elements apply and all other transaction

conditions that identify specific transactions must be provided. For e-commerce transactions, the transaction details and values must be provided.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48 Additional Data—Private Use	M	X	M	Contains applicable subelement data.
DE 48 Additional Data—Private Use, subelement 26 (Wallet Program Data)		•	C	Contains the subfield representing the wallet information. Conditional for Masterpass Online transactions.

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

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 48 Additional Data—Private Use	M	X	M	Contains applicable subelement data.
DE 48 Additional Data—Private Use, subelement 26 (Wallet Program Data)		•	C	Contains the subfield representing the wallet information. Conditional for Masterpass Online transactions.

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

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 48 Additional Data—Private Use	•	M	M	Contains applicable subelement data.
DE 48 Additional Data—Private Use, subelement 26 (Wallet Program Data)	•	C	C	Contains the subfield representing the wallet information. Conditional for Masterpass Online transactions.

### **Authorization Platform Edits**

The Authorization Platform performs the following edits on Masterpass Transactions.

WHEN the message contains...	THEN the Authorization Platform...
<p>The Authorization Request/0100 or Authorization Advice/0120 message includes DE 48 (Additional Data—Private Use), subelement 26 (Wallet Program Data), subfield 1 (Wallet Identifier) with a value other than the following:</p> <ul style="list-style-type: none"><li>• 0–9</li><li>• A–Z or a–z</li></ul> <p>Subelement 26 cannot contain all zeros. If all zeros is present, transaction will be rejected.</p>	<p>Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130—System-generated where:</p> <p>DE 39 (Response Code) = 30 (Format error)</p> <p>DE 44 (Additional Response Data) = 048026 (indicating the data element in error)</p>

## 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
04	Token requirements not fulfilled for this token type
21	Payment Cancellation

### **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.

<b>Value</b>	<b>Description</b>
00	Approved
05	Do not honor
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.

<b>DE 39</b>	<b>DE 48, subelement 84</b>	<b>Merchant Advice Description</b>	<b>Examples of Reason for Decline</b>	<b>Suggested Merchant Action</b>
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	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	Payment Cancellation	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

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)
- 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.</p> <p>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 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.</p> <p><b>NOTE: Subelement 72 should not be returned in the Authorization Request Response/0110.</b></p> <p>The Authorization Platform returns subelement 72 in the Authorization Request Response/0110 message when subelement 72 is present in the Authorization Request/0100 message.</p> <p>The acquiring MIP removes subelement 72 before sending the Authorization Request Response/0110 message to the acquirer host.</p>

<b>DE 48 Subelement:</b>	<b>Description</b>
Subelement 74 (Additional Processing Information)	<p>For M/Chip Processing services, subelement 74 notifies the acquirer that there was an issue with the cryptogram validation.</p> <p>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.</p> <p>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.</p>
Subelement 79 (Chip CVR/TVR Bit Error Results)	<p>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).</p> <p>Subelement 79 should not be returned in the Authorization Request Response/0110.</p>

## 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.

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])
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])

<b>IF the transaction is Full-Grade and...</b>	<b>THEN the Authorization Platform will...</b>
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>

<b>IF the transaction is Partial-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</p> <p>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</p> <p>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</p> <p>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 DE 55 is present and...</b>	<b>THEN the Authorization Platform will...</b>
DE 22 is not 05, 07, 79, or 80	<p>Reject the transaction for a format error:</p> <p>DE 39 = 30</p> <p>DE 44 = 055</p>

### **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.

**Subelement 71 (On-behalf Services)... Contains...**

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
  - 09 = PAN entry via electronic commerce, including remote chip

The Authorization Platform performs the following edits:

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 = 0480nn (where nn is the subelement number)

### Decline Option for Issuers

Mastercard has enhanced the M/Chip Cryptogram Pre-validation service with a decline option indicator to decline transactions on-behalf of participating issuers when the Application Request Cryptogram or the chip data validation for the transaction is not successful.

For the decline option indicator, Mastercard will forward the transaction to the issuer or decline the transaction on-behalf of the issuer on the basis of the information included in the decision matrix. For each value of the On-behalf Service (OBS) results, the decision matrix includes which action to take (forward or decline the transaction).

Mastercard supports the following four options for issuers registering to the OBS 02 service.

- Option 1: Do not use the decline option for neither contact nor contactless transactions.
- Option 2: Use the decline option for contact and contactless transactions.
- Option 3: Use the decline option for contact transactions and do not use the decline option for contactless transactions.
- Option 4: Use the decline option for contactless transactions and do not use the decline option for contact transactions.

### 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.

<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
The Application Cryptogram is invalid	I
The cryptogram in the Application Cryptogram is valid but the AC is not an ARQC nor a TC	G
The Application Cryptogram was a valid ARQC but the TVR/CVR was invalid	T
There is no matching key file for this PAN, PAN expiry date and KDI combination	K
The security platform has timed out	X
The security platform has experienced a processing error	Z
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 ARQC 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).

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	0059	=	Format Error
G	0039	=	Application Cryptogram is valid but not an ARQC nor a TC; Status of TVR/CVR unknown
I	0034	=	Invalid Chip Cryptogram
K	0037	=	No matching key file for this PAN, PAN expiry date and KDI combination—Validation of ARQC and CVR/TVR not performed, status unknown

---

<b>IF subfield 2 (OB Result 1) contains...</b>	<b>THEN DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code) contains...</b>		
T	0035	=	TVR/CVR validation failed
U	0032	=	Reject: Chip Data Processing Error
		-Or-	
			Another valid advice reason code
V	0000	=	Accept
		-Or-	
			Another valid advice reason code
X	0038	=	Security platform time out
Z	0040	=	Security platform processing error

---

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 mandated. 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.

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.

Registration forms Chip Project Request Workbook (CPRW) and Parameter Worksheet will be updated to include new options for M/Chip Cryptogram Pre-Validation Service processing.

Issuers opting for the M/Chip Cryptogram Pre-Validation Service with the decline option indicator should work with their business and Customer Implementation Services representatives to enable the M/Chip Cryptogram Pre-Validation Service with the decline option indicator by specifying which existing or new account ranges they want to support using the CPRW or *Parameter Worksheet* if issuers are in the Europe region.

### **Alternate Processing**

If a transaction is routed to the Stand-In System, the Stand-In System will respond to the acquirer based on the service results and on the instructions established by the issuer.

The issuer will receive the appropriate values 0037, 0038, and 0040 in DE 60, subfield 2 in the Authorization Advice/0120 message for the M/Chip Cryptogram Pre-Validation Service with the decline option indicator and M/Chip Cryptogram Validation in Stand-In Processing Service, with new values K, X, and Z in DE 48, subelement 71, subfield 2.

### **Authorization Platform Edits**

The Authorization Platform will perform the following system edits.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
EMV tag values other than 91, 71, and 72 are present and sent in the Authorization Request Response/0110 message or if the tag-length-value (TLV) structure of DE 55 (Integrated Circuit Card System Related Data) is incorrect	Sends an Authorization Negative Acknowledgement/0190 message to the issuer as a format edit error where: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format Error)</li><li>• DE 44 (Additional Response Data) = 055 (indicating the data element in error)</li></ul>

### **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.

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
  - 09 = PAN entry via electronic commerce, including remote 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 = 0480nn (where nn is the subelement number)

### **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 nor a TC	G
The Application Cryptogram was a valid ARQC but the TVR/CVR was invalid	T
There is no matching key file for this PAN, PAN expiry date and KDI combination	K
The security platform has timed out	X
The security platform has experienced a processing error	Z
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 the acquirer 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.

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	0059 = Format Error
G	0039 = Application Cryptogram is valid but not an ARQC nor a TC; Status of TVR/CVR unknown
I	0034 = Invalid Chip Cryptogram
K	0037 = No matching key file for this PAN, PAN expiry date and KDI combination—Validation of ARQC and CVR/TVR not performed, status unknown
T	0035 = TVR/CVR validation failed
U	0032 = Reject: Chip Data Processing Error -Or- Another valid advice reason code
V	0000 = Accept

---

**IF subfield 2 (OB Result 1) contains... THEN DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code) contains...**

---

-Or-

Another valid advice reason code

X	0038	=	Security platform time out
Z	0040	=	Security platform processing error

---

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 mandated.

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.

### **Alternate Processing**

If a transaction is routed to the Stand-In System, the Stand-In System will respond to the acquirer based on the service results and on the instructions established by the issuer.

The issuer will receive the appropriate values 0037, 0038, and 0040 in DE 60, subfield 2 in the Authorization Advice/0120 message for the M/Chip Cryptogram Pre-Validation Service with the decline option indicator and M/Chip Cryptogram Validation in Stand-In Processing Service, with new values K, X, and Z in DE 48, subelement 71, subfield 2.

### **Authorization Platform Edits**

The Authorization Platform will perform the following system edits.

WHEN...	THEN the Authorization Platform...
EMV tag values other than 91, 71, and 72 are present and sent in the Authorization Request Response/0110 message or if the tag-length-value (TLV) structure of DE 55 (Integrated Circuit Card System Related Data) is incorrect	Sends an Authorization Negative Acknowledgement/0190 message to the issuer as a format edit error where: <ul style="list-style-type: none"><li>• DE 39 (Response Code) = 30 (Format Error)</li><li>• DE 44 (Additional Response Data) = 055 (indicating the data element in error)</li></ul>

## MIP Transaction Blocking

---

MIP Transaction Blocking provides issuers with easy-to-manage, flexible controls that supplement their authorization strategy.

MIP Transaction Blocking extends an issuer's authorization capabilities, augmenting their defenses to protect portfolios from fraud attacks, as well as manage specialized payment programs with ease. An issuer's participation in the MIP Transaction Blocking Service is optional.

This service may not have the effect of causing the acquirer to be in noncompliance with any Mastercard Standard, including Rule 6.4, Selective Authorization.

Issuers may want to apply MIP Transaction Blocking to:

- Prevent the authorization of fraudulent transactions for compromised account ranges
- Prevent the authorization of transactions due to operational emergencies (for example, the issuer encounters problems supporting certain processing codes or POS PAN entry modes)
- Decline authorizations for an account range in combination with the point-of-interaction (POI) country in the event of local issues that necessitate preventing transactions from being authorized until those issues are resolved
- Protect assigned BIN ranges before they go into production or account ranges in production that are not actively used

MIP Transaction Blocking provides issuers the ability to decline authorizations in the Dual Message System based upon the issuing ICA number or account range, and one or more of the following transaction parameters:

- 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 32 (Acquiring Institution ID Code)
- 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 [or Sub-Merchant Information, if applicable])

MIP Transaction Blocking can also provide Full BIN Blocking on authorization requests for an entire BIN range or a segment of a BIN range, defined up to 11 digits, and is available globally on both the Dual and Single Message Systems.

## **MIP Transaction Block Setup**

Issuers must provide the following information for each transaction block setup.

The following information is required for each transaction block setup:

- ICA or Routing and Transit Number and account range
- The data elements identifying the type of transaction to be blocked
- Effective date
- The response code that will be returned in the Authorization Request Response/0110 message to the acquirer when the transaction matches the blocking criteria. Issuers may choose a response code from the following list:
  - 03 (Invalid merchant)
  - 04 (Capture card)
  - 05 (Do not honor)
  - 12 (Invalid transaction)
  - 57 (Transaction not permitted to issuer/cardholder)
  - 58 (Transaction not permitted to acquirer/terminal)

**NOTE: If issuers do not specify a decline response code, the default response code is 05 (Do not honor).**

- Registration for the optional MIP Transaction Blocking ICA Level Block Summary (SI738010-AA) and delivery endpoint.

## **MIP Transaction Blocking ICA Level Block Summary (SI738010-AA)**

The MIP Transaction Blocking ICA Level Block Summary (SI738010-AA) is an optional report showing each ICA level block for the issuer and the account ranges associated to that block. The ICA Blocking Summary report will assist issuers in determining the account ranges that are blocked via ICA level MIP Transaction Blocking records.

## **To Participate**

Issuers may choose to participate in and customize their MIP Transaction Blocking settings by completing the *MIP Transaction Blocking Service Request Form* (Form 810) and submitting the form to the Global Customer Service team.

For questions about participating in MIP Transaction Blocking, contact the Global Customer Service team.

## **Authorization Platform Edits**

The Authorization Platform performs the following edits on Authorization Request/0100—MIP Transaction Blocking transactions.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
The acquirer sends an Authorization Request/0100 message and the transaction matches a MIP transaction block record	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <p>DE 39 = The response code identified in the MIP transaction block setup</p> <p>and</p> <p>May send the issuer an Authorization Advice/0120 message where</p> <ul style="list-style-type: none"> <li>• DE 39 = The response code sent in the Authorization Request Response/0110</li> <li>• DE 60 (Advice Reason Code), Subfield 1 (Advice Detail Code) will contain 120</li> <li>• DE 121 (Authorizing Agent ID Code) will contain 000003 (Decline occurred due to an on-behalf service)</li> </ul>
The transaction does not match any MIP transaction block	Forwards the Authorization Request/0100 message to the issuer or to the Stand-In System if the issuer is unavailable.

## Full BIN Block

The Full BIN Block service blocks authorization requests for an entire BIN range or a segment of a BIN range, defined up to 11 digits.

Through this service, issuers can protect assigned BIN ranges before they go into production. Issuers also can protect account ranges in production that are not actively used. The Full BIN Block service will decline any authorization request in the identified account range with response code 14 (Invalid card number).

The Full BIN Block service is available globally on both the Dual and Single Message Systems. This service is recommended when a BIN has been assigned by Mastercard for use by the issuer, but that is not yet supported by the issuer's authorization system.

Participation in the Full BIN Block service is optional.

## Benefits

Issuers may want to apply authorization blocking for inactive BINs to:

- Block an entire BIN range or a segment of a BIN range.
- Combat fraud attacks on inactive BIN ranges, defined as "live" on Mastercard systems but not in production on the issuer host system.

## To Participate

To sign up for the Full BIN Block service, issuers must complete the *MIP Transaction Blocking Service Request Form* (Form 810).

## Authorization Platform Edits

The Authorization Platform performs the following edits on Authorization Request/0100—Full BIN Block transactions.

WHEN...	THEN the Authorization Platform...
The acquirer sends an Authorization Request/0100 message and the transaction falls within a Full BIN Block	Sends the acquirer an Authorization Request Response/0110 message where:  DE 39 = 14 (Invalid card number. The transaction is declined.)

## 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 can 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 can be filled by an acquirer or by a third-party registered with Mastercard by the acquirer as its Service Provider. 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.
- Issuer Domain—In the issuer domain, the Service Manager acts on behalf of issuers. The role of Service Manager can be filled by a third-party registered with Mastercard by the

issuer as its Service Provider. 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 can use a service manager to provide the Mobile Remote Payments program services.
- Acquirers can 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, refer to the *Mobile Remote Payments Program Guide*.
- Supporting data requirements, refer to 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.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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) = 048048 (indicating the data element in error)</li></ul>

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>The Authorization Request/0100 or Authorization Request Response/0120—Acquirer-generated message contains:</p> <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>	<p>Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where</p> <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).

The United Kingdom must support partial approvals for debit/prepaid cards and balance responses for prepaid cards. For MCC 5542 only partial approval support is required.

### 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.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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

### 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.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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	<p>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.</p> <p>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)</p>
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 1 (Account Type)	•	X	M	00 = Default Account (not specified or not applicable)
DE 54 (Additional Amounts), subfield 2 (Amount Type)	•	X	M	57 = Original Amount
DE 54 (Additional Amounts), subfield 3 (Currency Code)	•	X	M	Refer to the <i>Quick Reference Booklet</i>
DE 54, subfield 4 (Amount)	•	X	M	C 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
- 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—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.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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 = 048061

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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 = 048061
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.

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 48, subelement 61 is not present or DE 48, subelement 61, subfield 1 does not contain value 1 or DE 3, subfield 1 is 09 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

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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 of this manual for more information.

Issuers must be able to receive and support Payment Transactions unless they have regulatory restrictions that would prevent their participation in Payment Transactions.

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.
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	P = Payment Transaction

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48, subelement 77 (Funding/ 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 = Mastercard Rebate</li> <li>• C03 = rePower 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 = MoneySend Person-to-Person</li> <li>• C09 = Card Activation (Currently only applicable for Private Label Prepaid Cards issued in Europe)</li> <li>• C52 = MoneySend Account-to-Account Transfer</li> <li>• C53 = MoneySend Agent Cash Out</li> <li>• C54 = MoneySend Credit Card Bill Payment</li> <li>• C55 = MoneySend Business Disbursement</li> <li>• C56 = MoneySend Government/Non-profit Disbursement</li> <li>• C57 = MoneySend Acquirer Merchant Settlement</li> <li>• C67 = Inter Platform Person-to-Person</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.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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 = 048000
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 = 048077
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) contains value 28 (Payment Transaction), and DE 48 (Additional Data—Private Use), subelement 77 (Funding/ 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

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) contains value 28 (Payment Transaction), and DE 48 (Additional Data—Private Use), subelement 77 (Funding/ 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:	The Authorization Platform declines the request with a format error response where:  DE 39 (Response Code) = 30 DE 44 (Response Data) = 022
<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>	

---

**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.**

## PIN Management Service

Mastercard supports chip and magnetic stripe PIN management services.

### 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 unlock—Allows cardholders to unlock 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 or PIN Unblock (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	91 = PIN Unblock or 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 Disbursements

<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	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	•	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 or PIN Unblock (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	<p>70 = Contact Card Issuer</p> <p>71 = PIN Not Changed</p> <p>85 = Not Declined (Successful PIN Change or PIN unblock) (recommended for chip cards)</p> <p>89 = Unacceptable PIN—Transaction Declined—Retry</p>
DE 55 (Integrated Circuit Card [ICC] System-Related Data)	C	•	C	<p>Contains system-generated Authorization Response Cryptogram (APRC).</p> <p>Depending on the card application, DE 55 may contain an issuer script. The issuer script message contains instructions to the chip card:</p> <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.

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

<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 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 Disbursements
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.

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.

<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 Disbursements
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
DE 52 (Personal ID Number [PIN] Data)	C	X	C	Required for ATM transactions.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 125 (New PIN Data)	C	X	C	<p>Must be present for all online chip card PIN change transactions; otherwise not present.</p> <p>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.</p>

**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.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 39 (Response Code)	M	•	M	<p>00 = Approved or completed successfully (Successful PIN Change)</p> <p>70 = Contact Card Issuer</p> <p>71 = PIN Not Changed</p> <p>85 = Not Declined (Successful PIN Change) (recommended for chip cards)</p> <p>89 = Unacceptable PIN—Transaction Declined—Retry</p>

#### **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.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 3 (Processing Code), subfield 1	M	•	M	92 = PIN Change

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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 Disbursements
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.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 3, subfield 1 contains value 91 (PIN Unblock) and	Sends the acquirer an Authorization Request Response/0110 message where:
DE 22, subfield 1 does not contain value 05 (PAN auto-entry via chip)	DE 39 (Response Code) = 57 (Transaction not permitted to issuer/cardholder)

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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)
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 = 048000

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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 System or issuer system inoperative)

#### **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: • 02 • 90	Sends the acquirer a Reversal Request Response/0410 message where:  DE 39 = 30  DE 44 = 022

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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 = 048000
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 Customers**

---

Mastercard supports PIN translation for acquirers and issuers and issuer PIN validation for Track 1 and Track 2 on the Mastercard 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 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 customers 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).

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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 Single Message System
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.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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)

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>

---

<b>WHEN the issuer subscribes to the...</b>	<b>THEN the issuer...</b>
Online PIN Pre-validation	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.

## PIN Validation Edits

The following edits apply to Authorization Request/0100 messages (for issuers only).

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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	<p>Fowards the Authorization Request/0100 message where:</p> <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	<p>Fowards the Authorization Request/0100 message where:</p> <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	<p>Fowards the Authorization Request/0100 message where:</p> <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	<p>Fowards the Authorization Request/0100 message where:</p> <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	<p>Fowards the Authorization Request/0100 message where:</p> <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>

<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>

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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 Network.

## **PIN Verification Value/PIN Offset on File Service**

The PIN Verification Value (PVV)/PIN Offset used in PIN validation is usually located on Track 1 or Track 2 of a card's 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 card's 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 can use Bulk ID RA85 or CONNECT:Direct to send the PVV/PIN Offset file to Mastercard.

#### **PVV/PIN Offset File Header Record**

<b>Field Name</b>	<b>Attribute</b>	<b>Length</b>	<b>Comments/Values</b>
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

#### **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)

<b>Field Name</b>	<b>Attribute</b>	<b>Length</b>	<b>Comments/Values</b>
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 Customers

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 Network, refer to the PIN Processing for Europe Region Customers 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 customers' 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:

PEK	Description
Static	<ul style="list-style-type: none"><li>• Customers and the Authorization Platform establish these keys offline.</li><li>• Customers and the Authorization Platform must establish a single PEK. This PEK must be associated with the acquirer's customer ID.</li></ul>

PEK	Description
Dynamic	<ul style="list-style-type: none"> <li>Customers and the Authorization Platform exchange these keys automatically online every 24 hours or every 2,500 transactions, whichever occurs first.</li> <li>Customers 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.

Data Element	Org	Sys	Dst	Values/Comments
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.
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

Data Element	Org	Sys	Dst	Values/Comments
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.

Data Element	Org	Sys	Dst	Values/Comments
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 the following table that identifies possible responses based on PIN processing conditions.
DE 48 (Additional Data—Private Use), TCC	C	•	C	Must contain the appropriate TCC code.

Data Element	Org	Sys	Dst	Values/Comments
DE 48, subelement 80 (PIN Service Code)	C	•	C	<p>Identifies whether the Authorization Platform attempted to verify or translate the PIN. Valid values:</p> <ul style="list-style-type: none"> <li>• PV = The Authorization Platform verified the PIN</li> <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 = 52 DE 48, subelement 80 = TI
PIN processing was successful (verification or translation).	DE 39 = any valid code DE 48, subelement 80 = TV or PV

IF...	THEN...
The Authorization Platform was unable to decrypt the PIN for the issuer.	DE 39 = 91 (Authorization System 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 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 Single Message System 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 Single Message System 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 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* (Form 536).

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>

Data Element	Org	Sys	Dst	Values/Comments
DE 52 (Personal ID Number (PIN) Data)	C	X	C	<p>Will be present if the Authorization Platform does not perform PIN verification. The issuer verifies the PIN data in DE 52.</p> <p>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.</p>

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)				<p>This subelement contains the results of PIN processing as follows:</p> <table> <tr> <td>IF the issuer chooses to...</td> <td>THEN the Authorization Platform...</td> </tr> </table>	IF the issuer chooses to...	THEN the Authorization Platform...
IF the issuer chooses to...	THEN the Authorization Platform...					

Data Element	Org	Sys	Dst	Values/Comments
				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.

The Reversal Advice/0420 message identifies the corresponding Authorization Request Response/0110 message being reversed that contained PIN data.

Data Element	Org	Sys	Dst	Values/Comments
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 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 customer ID as follows:

- As the 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 setup process 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 the Single Message System for PIN-processing services and elect to use the PIN Validation in Stand-In service, the Single Message System 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 the Single Message System to update cardholder PINs and must use Single Message System-managed security keys. A Customer Implementation Services specialist will assist issuers with setting up a file or adding new files for testing and production.

Participating issuers must send a PVV/PIN Offset file to the Single Message System 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 the Single Message System 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

Field Name	Attribute	Length	Comments and Values
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.

<b>Field Name</b>	<b>Attribute</b>	<b>Length</b>	<b>Comments and Values</b>
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
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

<b>Field Name</b>	<b>Attribute</b>	<b>Length</b>	<b>Comments and Values</b>
Record type ID	Alphanumeric	3	TRL = trailer record
Number of detail records	Numeric	11	Detail record count

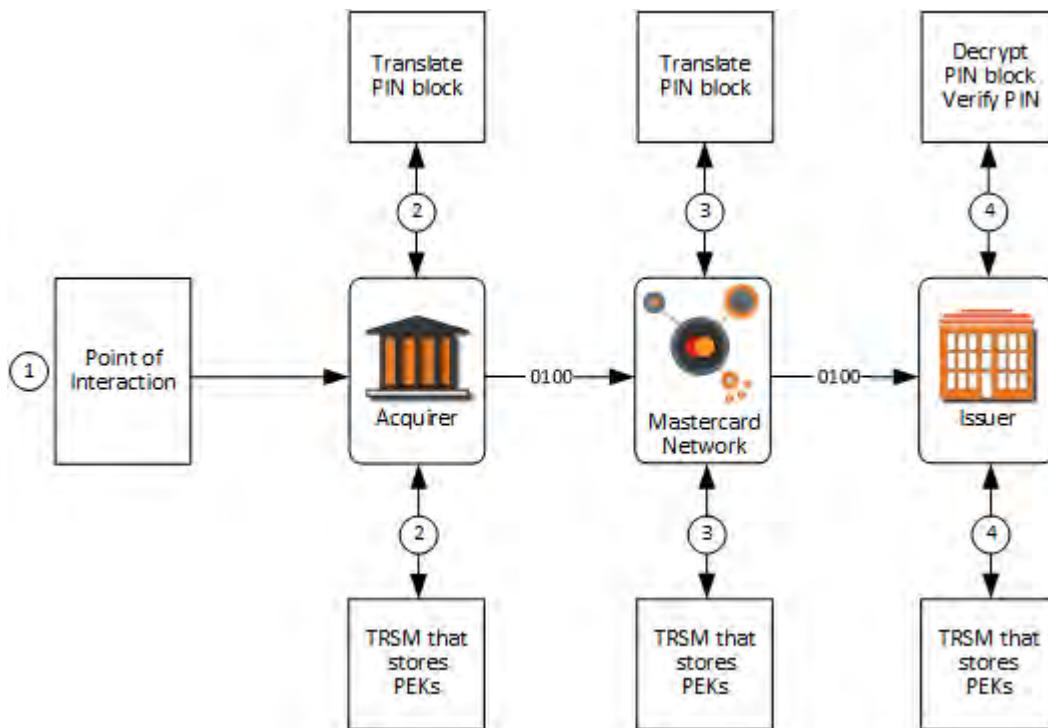
Field Name	Attribute	Length	Comments and Values
Filler	Alphanumeric	50	Spaces

### 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.

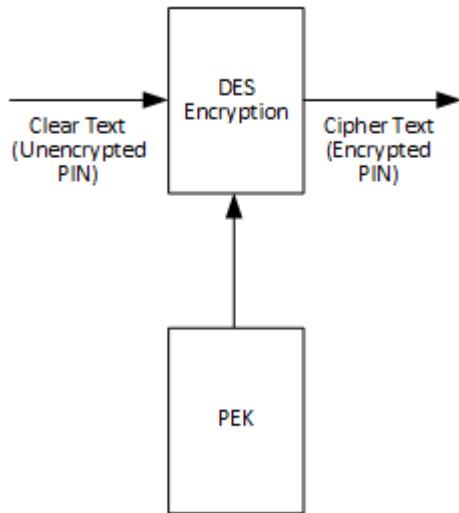
**Second Block—PAN Data:** The first four digits of the second block contain 0000, followed by the 12 right-most digits of the PAN, excluding the check digit. The acquirer then pads zeros to the left to complete the 16-digit data element.

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

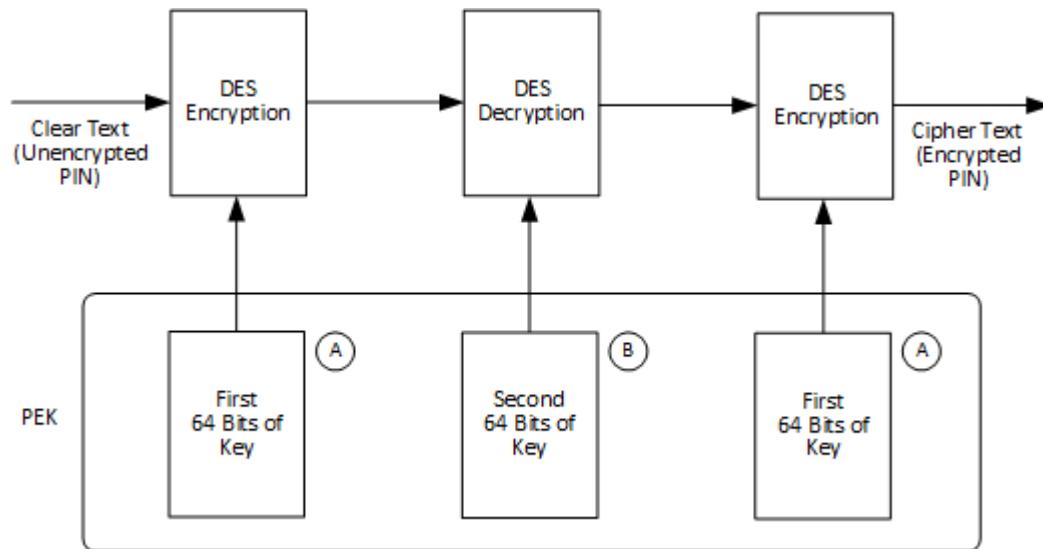
Encrypt PIN information using a single DES key algorithm with single-length PEKs as follows:



- b. Triple DES algorithm with double length PEKs<sup>38</sup>

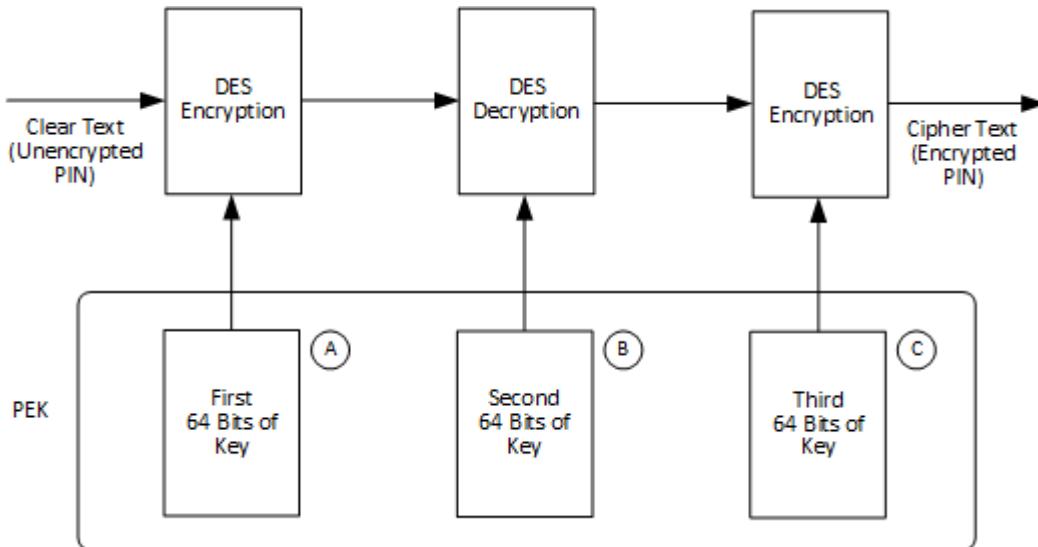
Encrypt PIN information using a triple DES key algorithm with double-length PEKs as follows:

<sup>38</sup> When a customer chooses to support triple DES, the customer must support both sending and receiving double-length (16-byte) PEKs.



c. Triple DES algorithm with triple length PEKs<sup>38</sup>

Encrypt PIN information using a triple DES key algorithm with triple-length PEKs as follows:



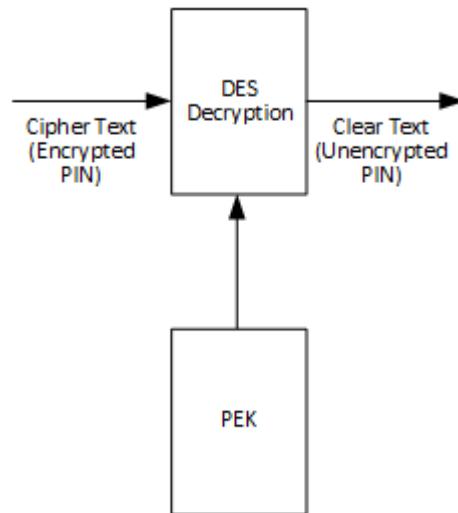
3. The acquirer sends the translated PIN block to the Authorization Platform. The Authorization Platform translates it from the acquirer PEK to the issuer PEK using the procedures described in step 2. The Authorization Platform then sends the translated PIN block to the issuer for verification.<sup>39</sup>

<sup>39</sup> 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.

4. The issuer then translates the PIN block and verifies the PIN using:

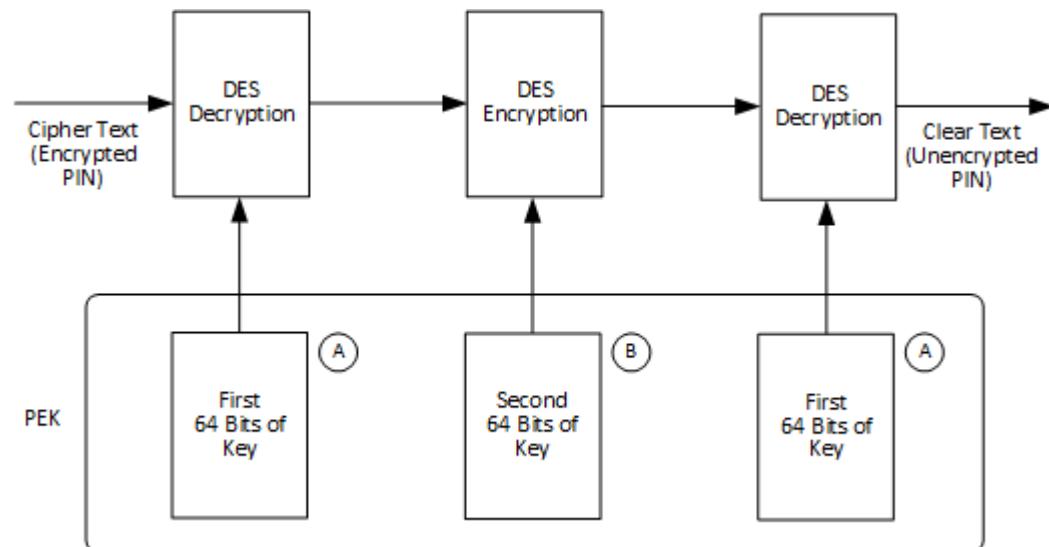
- a. Single DES algorithm

Decrypt PIN information using a single DES key algorithm with single-length PEKs as follows:



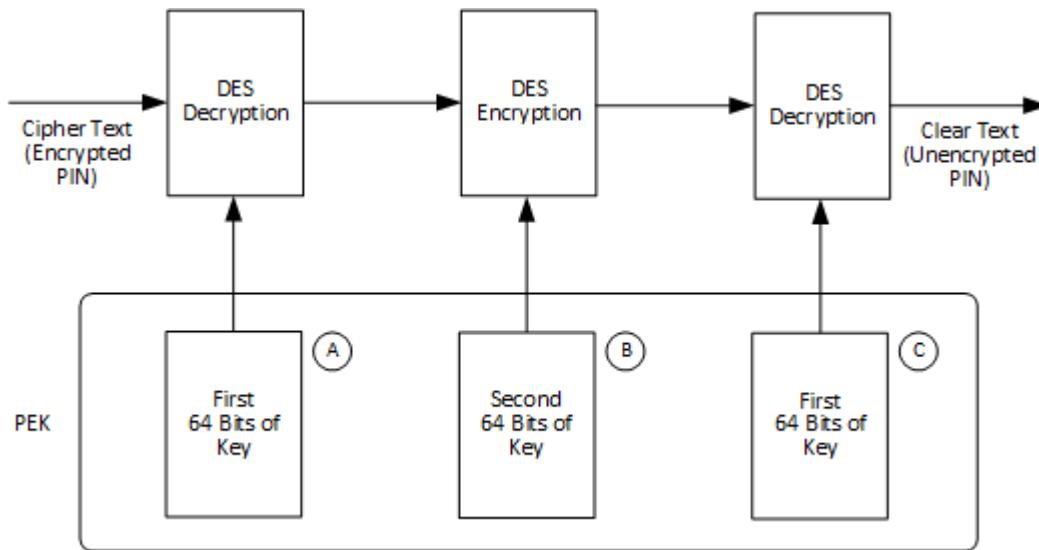
- b. Triple DES algorithm with double length PEKs

Decrypt PIN information using a triple DES key algorithm with double- or triple-length PEKs as follows:



- c. Triple DES algorithm with triple length PEKs

Decrypt PIN information using a triple DES key algorithm with triple-length PEKs as follows:



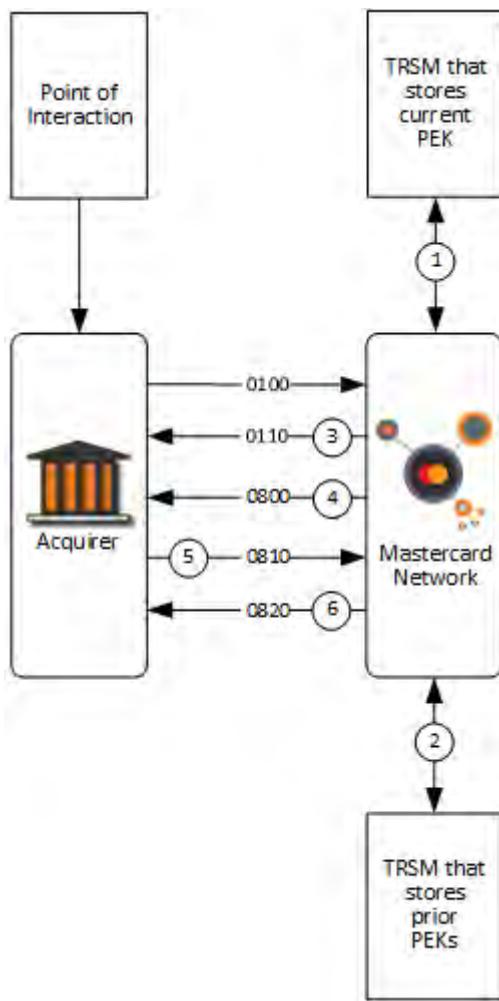
### **Detection of PEK Corruption Using Sanity Checks**

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.

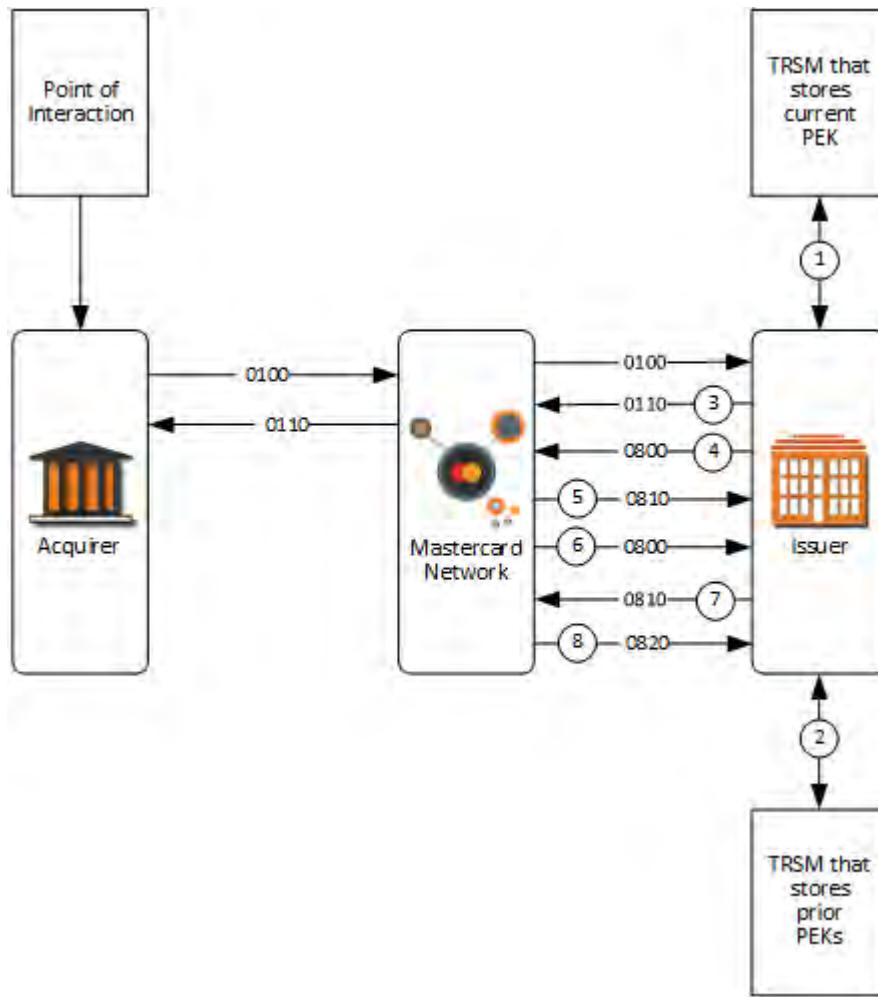


1. The Authorization Platform's Sanity Check reveals an out-of-synchronization condition with the PEK that it shares with the acquirer.
2. If five consecutive transactions fail the Sanity Check, and the Authorization Platform has performed steps 1–3 with each of the previous five transactions from the 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).

Mastercard Private Label card programs will use Mastercard or Maestro BIN ranges.

In addition to the following information, refer to the *Private Label Rules* manual for more details.

### 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.

## 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.

### 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 Disbursements) or 6011 (Member Financial Institution—Automated Cash Disbursements)

---

<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>• 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>
DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	M	•	M	Must contain value P
DE 48 (Additional Data—Private Use), subelement 77 (Funding/ 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)

---

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
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 System 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.

### **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>
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) contains value 28 (Payment Transaction), and DE 48 (Additional Data—Private Use), subelement 77 (Funding/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

WHEN...	THEN the Authorization Platform...
<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 (Funding/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><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>	<p>The Authorization Platform declines the request with a format error response where: DE 39 (Response Code) = 30 DE 44 (Response Data) = 022</p>

### 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), subelement 77 (Funding/Payment Transaction Type Indicator), value C09 (Card Activation).
- 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 (Funding/Payment Transaction Type Indicator), value C09 (Card Activation).
- 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 an acquirer to send a product inquiry authorization request message to Mastercard.

#### **NOTE: Applies only to the U.S. region.**

As part of the authorization response to an acquirer, Mastercard will provide an acquirer with the product code associated with the particular Mastercard card number. Additionally, because product codes for Mastercard® Standard Card, Gold Mastercard® Card, Platinum Mastercard® Card, or World Mastercard® Card programs potentially fall under different interchange rate structures, Mastercard will also 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, along 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. The issuer Authorization Request Response/0110—Product Inquiry Service message follows the same requirements as the Account Status Inquiry Service.

### **Acquirers**

Acquirers that choose to support Product Inquiry Service transactions must send Authorization Request/0100 messages containing DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI]) and DE 4 (Amount, Transaction) with a transaction amount of zero when submitting Product Inquiry Service transaction requests.

**NOTE: Product Inquiry Service messages that include address verification and/or CVC 2 validation requests will be deemed to be an attempt to mitigate fraud. As such, they will be designated as an Account Status Inquiry Service transaction and billed accordingly.**

### **Issuers**

Issuers will receive Authorization Request/0100 messages containing DE 61, subfield 7, value 8, and DE 4 with a transaction amount of zero. Issuers must respond to these transactions with value 00 (Approved or completed successfully), 85 (Not Declined), 05 (Do Not Honor) or other valid business decline responses in DE 39 (Response Code). Invalid business declines include values 03 (Invalid merchant), 12 (Invalid transaction), 13 (Invalid amount), 30 (Format error), 51 (Insufficient funds/over credit limit), 57 (Transaction not permitted to issuer/cardholder), and 58 (Transaction not permitted to acquirer/terminal).

### **For More Information**

For more information about the Product Inquiry Service, contact the Global Customer Service team.

### **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.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Comments</b>
4 Amount, Transaction	M	•	M	Transaction amount of zero, in the acquirer's currency, at the point of interaction.

<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, subfield 7 (POS Transaction Status), value 8 (Account Status Inquiry Service [ASI])	M	•	M	

## Proximity Payments

The Mastercard Proximity Payments solution, which includes Mastercard contactless magnetic stripe and Mastercard contactless 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 environments (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.

## 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.

<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	
DE 48, subelement 61 (POS Data, Extended Condition Codes), subfield 2 (Purchase Amount Only Terminal Support Indicator)	C	•	C	1 = Merchant terminal supports receipt of purchase only approvals

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 54 (Additional Amounts), subfield 1 (Account Type)	M	X	M	<p>The Authorization Platform provides a second occurrence of DE 54 to the issuer if billing currency is different than transaction currency.</p> <p>Must contain one of the following values:</p> <p>00 = Default account (not specified or not applicable)</p> <p>10 = Savings Account</p> <p>20 = Checking Account</p>
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.

<b>The Issuer must provide...</b>	<b>The Acquirer will receive...</b>
<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 (Additional Amounts) cash back amount and, if applicable, the DE 28 (Amount, Transaction Fee) 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:

- 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.

## Authorization Platform Edits

The Authorization Platform will perform the following edits on Purchase of Goods or Services with Cash Back transactions.

### Authorization Request/0100

WHEN...	THEN the Authorization Platform...
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 the amount in DE 4 (Amount, Transaction)	DE 39 = 30 DE 44 = 054

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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 = 048061
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 or DE 3, subfield 1 is not 09 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
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 Request Form* and providing the form to their Global Customer Service 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, subelement 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 (value 10), 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.

DE 54, 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.

Mastercard also supports DE 54, subfield 2, value 12 (Vision Rx Eligibility Amount), which allows the acquirer to indicate the portion of the amount spent on vision Rx or vision products/services. When a prescription is issued and dispensed by a licensed vision center for vision products/services (for example, tests/exams, lenses, glass frames, and so on), the patient portion of the cost is considered an eligible item under IRS regulations for processing as per the Special Interest Group for IIAS Standards (SIGIS). Acquirers may provide DE 54, subfield 2, value 12 by itself in the Authorization Request/0100 or the Authorization Advice/0120 messages or in combination with value 10 or values 10 and 11.

Values 10, 11, or 12 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.

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><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: Entire Vision Prescription Amount

This example illustrates that the issuer approved the entire Vision Prescription 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.

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>
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 12 = USD 40</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 (Original Amount) = USD 100</li> <li>• DE 39 = 10</li> </ul>

### **Example 3—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.

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>
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> <li>• DE 4 = USD 20</li> <li>• DE 54, subfield 2, value 57 = USD 100</li> <li>• DE 39 = 10</li> </ul>

### **Example 4—Partial Approval: Partial Vision Prescription Amount**

This example illustrates that the issuer approved only a portion of the Vision Prescription 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.

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>
From Issuer	To Acquirer

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>
<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 12 = USD 40</li> </ul>	<ul style="list-style-type: none"> <li>• DE 6 = USD 20</li> <li>• DE 39 = 10</li> </ul> <p style="text-align: center;">S</p> <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 5—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.

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>				
	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 50%;">From Issuer</th> <th style="text-align: left; width: 50%;">To Acquirer</th> </tr> </thead> <tbody> <tr> <td> <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> </td><td> <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 responded with DE 39 = 00</li> </ul> </td></tr> </tbody> </table>	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> <li>• No DE 54, subfield 2, value 57 (Original Amount) is provided in this scenario because the issuer responded with DE 39 = 00</li> </ul>
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> <li>• No DE 54, subfield 2, value 57 (Original Amount) is provided in this scenario because the issuer responded with DE 39 = 00</li> </ul>				

### **Example 6—Full Approval: Entire Vision Prescription 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 Vision Prescription Amount.

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>		
	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 50%;">From Issuer</th> <th style="text-align: left; width: 50%;">To Acquirer</th> </tr> </thead> </table>	From Issuer	To Acquirer
From Issuer	To Acquirer		

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>
<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 12 = USD 100</li> </ul>	<ul style="list-style-type: none"> <li>• DE 4 = USD 100</li> <li>• DE 39 = 10</li> <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>

### **Example 7—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 to use another form of payment for the remaining USD 80 or remove some items from the purchase.

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>				
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">From Issuer</td> <td style="width: 50%;">To Acquirer</td> </tr> </table>	From Issuer	To Acquirer	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">From Issuer</td> <td style="width: 50%;">To Acquirer</td> </tr> </table>	From Issuer	To Acquirer
From Issuer	To Acquirer				
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> </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 8—Partial Approval: Partial Healthcare Eligibility Amount and Vision Prescription Amount , including Prescriptions and Vision Prescriptions**

This example illustrates that the issuer approved only a portion of the Healthcare, Prescription Eligibility, and Vision Prescription amounts. 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.

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>				
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">From Issuer</td> <td style="width: 50%;">To Acquirer</td> </tr> </table>	From Issuer	To Acquirer	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">From Issuer</td> <td style="width: 50%;">To Acquirer</td> </tr> </table>	From Issuer	To Acquirer
From Issuer	To Acquirer				
From Issuer	To Acquirer				

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>
<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 20</li> <li>• DE 54, subfield 2, value 11 = USD 10</li> <li>• DE 54, subfield 2, value 12 = USD 10</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>

#### **Example 9—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.

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>
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>
---	--

#### **Example 10—Full Approval: Entire Healthcare Eligibility Amount and Vision Prescription Amount, including Prescriptions and Vision 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 and Entire Vision Prescription Amount.

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>
From Issuer	To Acquirer

<b>Authorization Request/0100</b>	<b>Authorization Request Response/0110</b>
<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 60</li> <li>• DE 54, subfield 2, value 11 = USD 10</li> <li>• DE 54, subfield 2, value 12 = USD 40</li> </ul>	<ul style="list-style-type: none"> <li>• DE 4 = USD 100</li> <li>• DE 39 = 10</li> <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

**NOTE: DE 54 (Additional Amounts), subfield 2 (Amount Type), value 12 (Vision Rx Eligibility Amount) is an independent field and can be used without value 10 (Healthcare Eligibility Amount).**

**NOTE: When DE 54 contains multiple occurrences, the DE 54, subfield 2, value 10 (Healthcare Eligibility Amount) can co-exist with amount types other than the value 11 (Prescription Eligibility Amount).**

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
<p>DE 54, subfield 2, values 10, 11, or 12 are present and</p> <p>DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) is not 00 (Purchase of goods or services)</p>	<p>Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30 (Format error)</li> <li>• DE 44 = 054</li> </ul>
<p>DE 54 (Additional Amounts), subfield 2 (Amount Type) is greater than transaction amount in DE 4 (Amount, Transaction) and the healthcare amount types (10 or 12) are populated separately</p> <p>or</p> <p>The sum of healthcare and vision amount types (10 or 12) are populated together and is greater than request amount in DE 4</p>	<p>Sends the acquirer an Authorization Request Response/0110 or Authorization Advice Response/0130 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 (Response Code) = 30 (Format error)</li> <li>• DE 44 (Additional Response Data) = 054</li> </ul>

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 54 subfield 2, values 10, 11, or 12 are 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.
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, values 10, 11, or 12	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 = 048032</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.

---

<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	<p>Updates the value in DE 48, subelement 61, subfield 3 as follows:</p> <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	<p>Sends the acquirer an Authorization Request Response/0110 message where:</p> <ul style="list-style-type: none"> <li>• DE 39 = 30</li> <li>• DE 44 = 048061</li> </ul>

---

## Reversal Request/0400

---

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
DE 54, subfield 2, values 10, 11, or 12 are present in the Reversal Request/0400 message	Removes DE 54, subfield 2, values 10, 11, and 12 from the Reversal Request/0400 message to the issuer.

---

## Reversal Processing

Mastercard supports the reversal of a full transaction amount or a partial transaction amount using reversal processing.

### Best Practices for Authorization Reversal Processing

Mastercard provides the following update to its best practices for the management of authorization reversals. These best practices are intended to guide dual message acquirers, issuers, and processors in the usage of these transactions.

**NOTE: These best practices are in effect for current processing or 14 October 2016, as noted.**

## Background

Merchant-initiated authorization reversal messages are intended to assist issuers in managing "open-to-buy." This processing function is especially critical to debit and prepaid card issuers. Merchants and acquirers submit authorization reversal messages when:

- The final transaction amount was less than the authorized amount
- The cardholder cancels or chooses not to complete all or part of the transaction
- All or a portion of the goods or services could not be provided (for example, out-of-stock items)
- The authorization was submitted in error (for example, duplicate request or technical failures)

## Guiding Principles

The following is provided as guidance for reversal processing. Note that unless otherwise specified, these are best practices and are not mandatory:

- Authorization reversal messages are intended to fully or partially release a hold of funds prior to clearing the transaction.
- Purchase returns (or refunds) are managed offline after the first presentment has been processed, and are presented to clearing as a credit.
- Mastercard recommends that merchants submit reversals as soon as an adjustment to the original authorization amount is known. Only approved authorization requests or transactions that have timed out are required to be reversed.
  - Merchants and acquirers must submit a full or partial reversal (as applicable) within seven calendar days of an original undefined authorization or final authorization request and within 30 calendar days of an original preauthorization request.
  - Merchants and acquirers must submit a full or partial reversal within 24 hours of transaction cancellation or of the transaction completing for an amount different from the authorized amount.

**NOTE: Refer to the Incremental Preauthorization Standards section in this chapter of this manual for more information about revised Standards for authorizations and preauthorizations.**

- Reversals must contain the mandatory matching data elements from the original authorization in order for an issuer to release the appropriate funds, subject to the issuer's risk or fraud control policies.

## Specific Scenarios

Specific Scenarios are described as follows:

- If an incremental authorization has been submitted, a reversal should reference original transaction data, including the original Trace ID, and data element (DE) 4 (Amount, Transaction) should be the sum of the original authorized amount plus any incremental amounts.

- Issuers will release any hold of funds once a clearing presentment has been matched (using the Trace ID in addition to other data elements) to the original authorization. Accordingly, a merchant is not required to submit a partial reversal if the lower amount is processed by Mastercard clearing within 24 hours of finalization of the transaction—assuming multi-clearing processing is not utilized.
- Partial reversals must be used when multi-clearing processing is utilized, since issuers will maintain a hold of funds for subsequent presentments.

### **Reversal Message Data Element Details**

As follows are details about reversal messaging data elements:

- Mandatory Reversal Request/0400 data elements used for issuer matching, which must contain the same value from the original Authorization 0100/0110 message:
  - DE 2 (Primary Account Number [PAN])
  - DE 3 (Processing Code)
  - DE 4 (Amount, Transaction)
  - DE 38 (Authorization ID Response)
  - DE 48, subelement 63 (Trace ID) (from original DE 15 [Date, Settlement] and DE 63 [Network Data])
  - DE 49 (Currency Code, Transaction)
  - DE 90 (Original Data Elements) (from original DE 7 [Transmission Date and Time], DE 11 [System Trace Audit Number (STAN)], and DE 32 [Acquiring Institution ID Code] and DE 33 [Forwarding Institution ID Code])

**NOTE:**

**Reversals submitted for technical failures (DE 39 reversal reason code 06—Error) will not contain DE 38 (Authorization ID) or DE 48, subelement 63 (Trace ID), because no Authorization Request Response/0110 message was received. If Trace ID data from the original authorization is not available due to technical failures, DE 48, subelement 63 in the reversal must contain zeros.**

**DE 90, subfield 1 must contain the Message Type Identifier (MTI) of the original authorization message. The remaining subfields may contain valid matching values from the original authorization or may be zero-filled if they are not available.**

- Mandatory Reversal Request/0400 message data elements that may use default values consistent with the merchant initiating the reversal, unless supplied directly from the merchant point-of-interaction (POI) (for example, merchants with multiple card acceptor business codes [MCCs]):
  - DE 18 (Merchant Type)
  - DE 22 (Point-of-Service [POS] Entry Mode)
  - DE 32 (Acquiring Institution ID Code) and DE 33 (Forwarding Institution ID Code) by using default values consistent with the merchant, DE 32 and DE 33 will be the same values as in the original 0100 message

- DE 39 (Response Code)
- DE 41 (Card Acceptor Terminal ID)
- DE 42 (Card Acceptor ID Code)
- DE 43 (Card Acceptor Name/Location for All Transactions)
- DE 61 (Point-of-Service [POS] Data)

Mastercard recommends that DE 39 (Response Code) be populated with one of the following Reversal Request/0400 reason codes:

- 06—Error
- 17—Customer Cancellation
- 32—Partial Reversal
- 34—Suspect Fraud
- 68—Response Received Late
- Minimum list of original Authorization 0100/0110 data elements to be saved for submitting a Reversal Request/0400 message:
  - DE 2 (Primary Account Number [PAN])
  - DE 3 (Processing Code)
  - DE 4 (Amount, Transaction)
  - DE 7 (Transmission Date and Time)
  - DE 11 (System Trace Audit Number [STAN])
  - DE 15 (Date, Settlement)
  - DE 38 (Authorization ID Response)
  - DE 49 (Currency Code, Transaction)
  - DE 63 (Network Data)

**NOTE:**

**DE 15, DE 38, and DE 63 will only be available if an approved authorization response was received.**

**If DE 7 and DE 11 from the original authorization cannot be saved, DE 90, subelements 2 and 3 may be zero-filled within the Reversal Request/0400 message.**

- Optional/Conditional data elements that must contain the same value from the original Authorization 0100 if included in the Reversal Request/0400 message:
  - DE 12 (Time, Local Transaction)
  - DE 13 (Date, Local Transaction)
  - DE 14 (Date, Expiration)
  - DE 23 (Card Sequence Number)
  - DE 28 (Amount, Transaction Fee)
  - DE 37 (Retrieval Reference Number)
  - DE 54 (Additional Amounts)

## 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 message 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).

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 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 = Issuer Time-out</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.

**NOTE: Customers 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.

<b>WHEN...</b>	<b>THEN the Authorization Platform...</b>
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.

<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

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

## Visa Transaction Processing

Mastercard supports Visa transaction processing as described in this section.

### 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 through X-code and will decline the Visa transaction.

**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.

<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	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.

---

<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 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.
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. Refer to Visa Base I Technical Specifications manual for a list of all CPS request values in Visa field 62.1.
DE 48, subelement 91 (Visa Custom Payment Service Request/ Transaction ID, [Visa field 62.2 and 62.3])	C	•	C	Must be present for incremental authorization and reversal transactions and contain the Transaction ID and/or the CPS validation code of the original transaction.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48, subelement 96 (Visa Market-Specific Data [Visa field 62.4])	C	•	C	<p>Must be present for hotel or automobile transactions and contain one of the following values:</p> <p>A = Automobile rental</p> <p>B = Bill payment transaction</p> <p>E = Electronic commerce transaction aggregation</p> <p>H = Hotel rental</p> <p>J = B2B invoice payments</p> <p>M = Healthcare—Medical</p> <p>N = Failed market-specific data edit</p> <p>T = Transit (in healthcare transactions only)</p>
DE 48, subelement 97 (Visa Prestigious Property Indicator [Visa field 62.6])	C	•	C	<p>May be present for participants in the Visa Prestigious Lodging program and contains one of the following values:</p> <p>D = Visa established limits</p> <p>B = Visa established limits</p> <p>S = Visa established limits</p>
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.

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48, subelement 85 (Account Status [Visa Only])	C	•	C	<p>Identifies the account range as regulated or non-regulated interchange. Must be one of the following values:</p> <p>R = Account is regulated</p> <p>N = Account is non-regulated</p>

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48, subelement 90 (Custom Payment Service Request [Visa field 62.1])	M	•	M	If the request qualifies for Visa CPS and is approved, refer to the Visa Base I Technical Specifications manual for a complete list of CPS-qualified codes in Visa field 62.1.  If the original request does not qualify for CPS, Visa returns an "N" or "T" in the response.
DE 48, subelement 91 (Visa Custom Payment Service Request/Transaction ID)	C	•	C	Must be present if DE 48 subelement 90 is present. Contains one of the following response lengths:  When length field is 04: Subelement 91 contains the Visa CPS validation code (Visa field 62.3, four bytes alphanumeric). Refer to the Visa Base I Technical Specifications manual for more information on Visa CPS validation codes.  When length field is 15: Subelement 91 contains the transaction ID (Visa field 62.2, 15 bytes numeric).  When length field is 19: Subelement 91 contains the transaction ID (Visa field 62.2, 15 byte numeric) and CPS validation code (Visa field 62.3, four bytes alphanumeric).
DE 48, subelement 96 (Visa Market-Specific Data [Visa field 62.4])	C	•	C	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:  A = Automobile rental H = Hotel rental N = Failed market-specific data edit

---

### **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.

<b>LLL</b>	<b>"VAR"—999 maximum bytes (TCC + Subelement (SE) data)...</b>						
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		
<b>mandatory</b>		SE ID 90 Length	SE 90 Length	Authorization Characteristics Indicator	SE ID 91 Length	SE 91 Length Transaction ID and/or CPS Validation Code

**1002 maximum bytes (LLL +TCC + Subelement Data)...**

**...“VAR”—999 maximum bytes (TCC + Subelement (SE) data)**

2 bytes	2 bytes	1 byte	2 bytes	2 bytes	1 byte
<b>Third Subelement Data</b>			<b>Fourth Subelement Data</b>		
SE ID 96	SE 96 Length	Market-specific Data ID	SE ID 97	SE 97 Length	Prestigious Property Indicator

**...1002 maximum bytes (LLL +TCC + Subelement Data)**

## Visa Programs

Mastercard supports Visa transactions as described in this section.

### 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

<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.

<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	PAN begins with 4 indicating a Visa card.

Data Element	Org	Sys	Dst	Values/Comments
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.

Data Element	Org	Sys	Dst	Values/Comments
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

<b>Data Element</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
DE 48, subelement 94, subfield 2 (Merchant Request for Commercial Card Type)	C	•	C	<p>Contains one of the following values:</p> <p>0 = Decline or not a Commercial Card</p> <p>B = Business Card</p> <p>R = Corporate Card</p> <p>S = Purchase Card</p>

## **Visa Token Processing**

Mastercard has expanded the functionality of the Visa Gateway to support tokenization processing for partial shipments, recurring payments, and e-commerce mobile transactions for Visa-branded, dual-message authorization transactions submitted to the Mastercard Network.

These enhancements affect acquirers that use the Mastercard Network to submit Visa-branded dual-message authorization transactions.

### **Tokenized Recurring Payment Messages**

Acquirers must be prepared to identify tokenized recurring payment transactions in Authorization Request/0100 and Reversal Request/0400 messages.

- Existing value 4 (Standing order/recurring transactions) in DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence)
- Presence of DE 48 (Additional Data—Private Use), subelement 43 (Secure Electronic Commerce Verification Service) containing the partial shipment verbiage as follows: PARTIALbSHIPMENTbbbbbbbbbbbb or PARTIALSHIPMENT00000000000000 where b represents a space. This field contains 28 positions.
- Existing values 2 (Channel) in position 1 (Security Protocol), 1 (Cardholder certificate not used) in position 2 (Cardholder Authentication), and 0 (UCAF data collection is not supported by the merchant or a SecureCode merchant has chosen not to undertake SecureCode on this transaction) in position 3 (UCAF Collection Indicator) in DE 48 (Additional Data—Private Use), subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator)
- Existing value 81 (PAN manual entry via e-commerce) in DE 22 (Point-of-Service Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)

### **Tokenized Partial Shipment Messages**

Acquirers must be prepared to identify tokenized partial shipment transactions in Authorization Request/0100 and Reversal Request/0400 messages whose original transaction was token-based with a valid cryptogram. Cryptographic data from the original transaction must be resent in Authorization Request/0100 messages for partial shipments, but is not required in Reversal Request/0400 messages.

- DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence), value 5 (Electronic order [home PC, Internet, mobile phone, PDA])
- DE 48 (Additional Data—Private Use), subelement 43 containing the cryptographic data from the original transaction
- DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator):
  - Position 1 (Security Protocol), value 2 (Channel)
  - Position 2 (Cardholder Authentication), value 1 (Cardholder certificate not used)
  - Position 3 (UCAF Collection Indicator), value 2 (UCAF data collection is supported by the merchant, and UCAF data must be present [DE 48, subelement 43 must contain a fully authenticated AAV])
- DE 22 (Point-of-Service Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), values 10 (Credential on File) or 81 (PAN manual entry via e-commerce)

**NOTE: DE 48, subelement 43 is not required in Reversal Request/0400 messages for partial shipments.**

### **Tokenized E-Commerce with Mobile Device Messages**

Acquirers must be prepared to receive the tokenized e-commerce with mobile device transaction identifier in Authorization Request Response/0110 and Reversal Request Response/0410 messages.

- Value B (Tokenized e-commerce with mobile device) in DE 48, subelement 90 (Custom Payment Service Request Response [Visa Only])
- Value Y (Transaction is processed through Visa Checkout) in DE 48, subelement 78 (Payment Service Indicators [Visa Only]), subfield 4 (Visa Checkout Indicator)

### **Authorization Request/0100—Visa Token Request**

Following is a list of the data elements and values applicable to the Authorization Request/0100 message type for token requests for Visa primary account numbers. All mandatory Authorization Request/0100 data elements apply except where noted.

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
2 Primary Account Number	M	•	M	Cardholder's primary account number
3 Processing Code	M	•	M	00 = Purchase
4 Amount, Transaction)	M	•	M	Must be zero
14 Date, Expiration	M	•	M	Cardholder's primary account expiration date
48 Transaction Category Code	M	•	M	Contains the appropriate Transaction Category Code (TCC).

<b>Data Element ID and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>	
48 Additional Data—Private Use, subelement 33 (PAN Mapping File Information)	M	•	M	<p>This is a Tag-Length-Value field. The tags in the subelement will indicate which subfields are present. Only subfield 6 is required.</p> <p>Subfield 6 (Token Requestor ID) = The ID assigned by the Visa Token Vault to the Token Requestor.</p>	
48 Additional Data—Private Use, subelement 42 (Electronic Commerce Indicators)	C	•	C	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.	
48 Additional Data—Private Use, subelement 43—3-D Secure Electronic Commerce Verification Service	C	•	C	<p>Position 1 = 8 (Non-Mastercard 3-D Secure Electronic Commerce transaction [Visa, JCB, Diners Club, or American Express])</p> <p>Position 2-21 (3-D Secure Electronic Commerce Cardholder Authentication Verification Value [CAVV])</p>	
48 Additional Data—Private Use, subelement 82 (Address Verification Service Request)	M	•	M	52 = AVS and Authorization Request/0100	
48 Additional Data—Private Use, subelement 92 (CVV2 Data [Visa Only])	C	•	C	CVV2 value from the signature panel of the card when applicable.	
61 Point-of-Service [POS] Data, subfield 7 (POS Transaction Status)	M	•	M	8 = Account Status Inquiry	
120 Record Data		M	•	M	The cardholder's billing address

#### **Authorization Request Response/0110—Visa Token Request Response**

Following is a list of the data elements and values applicable to the Authorization Request Response/0110 message for responses to Visa token requests. All mandatory Authorization Request Response/0110 data elements apply except where noted.

<b>Data Element and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
2 Primary Account Number	ME	•	ME	Cardholder's primary account number.

<b>Data Element and Name</b>	<b>Org</b>	<b>Sys</b>	<b>Dst</b>	<b>Values/Comments</b>
3 Processing Code	ME	•	ME	00 = Purchase
4 Amount, Transaction	CE	X	M	Must be zero.
39 Response Code	M	•	M	Contains the applicable response code.
48 Additional Data—Private Use, subelement 33 (PAN Mapping File Information)	C	•	C	<p>This is a Tag-Length-Value field. The tags in the subelement will indicate which subfields are present.</p> <ul style="list-style-type: none"> <li>• Subfield 1 (Account Number Indicator) = C (Mastercard Digital Enablement Service Device Account Number)</li> <li>• Subfield 2 (Account Number) = Token</li> <li>• Subfield 5 (Token Assurance Level) = Value between 00 and 99 indicating the Token Assurance Level assigned by the Visa Token Vault.</li> <li>• Subfield 6 (Token Requestor ID)</li> </ul> <p><b>NOTE: The Visa token expiration date will be the same as the expiration date of the primary account number.</b></p>
48 Additional Data—Private Use, subelement 45—3-D Secure Electronic Commerce Transactions Response Code	C	•	C	The Visa Cardholder Authentication Verification Value (CAVV) results code.
48 Additional Data—Private Use, subelement 82 (Address Verification Service)	CE	•	CE	52 = AVS and Authorization Request/0100
48 (Additional Data—Private Use), subelement 83 (Address Verification Service Response)	C	•	C	The AVS verification response code.
48 Additional Data—Private Use, subelement 87 (CVV2 Response [Visa Only])	C	•	C	The CVV2 response.
120 Record Data, subfield 01 (AVS Service Indicator 1)	C	X	C	Must be the same value as in the original Authorization Request/0100 message, if present.

---

# Notices

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

## Proprietary Rights

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

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

## Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

## Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

## Translation

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

## Information Available Online

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