Authorization Manual

15 October 2019

AP

Summary of Changes, 15 October 2019

This summary reflects changes effective since the last update of this publication.

Description of Change	Where to Look
General	
Removed all references to Mastercard Electronic™.	Throughout
Added references to Digital Payment Data Field (DE 104).	Throughout
Updated Funding/Payment Transaction Type Indicator to Transaction Type Identifier.	Throughout
Replaced Mastercard SecureCode with Mastercard Identity Check.	Throughout
Chapter 2, Basic Authorization Concepts	
In X-Code Processing, Acquirer MIP X-Code Processing, MIP X-Code Limits subsection, added new product code MPE (Name for GCMS Product ID MPE) and MSP (Muse Mastercard).	MIP X-Code Limits
Chapter 7, Authorization Service Details	
In Account Balance Response, deleted the following language—NOTE: Issuers in the United Kingdom (U.K.) may provide a maximum of two account balances, the ledger balance in addition to the available balance, when responding to intracountry ATM transactions.	Account Balance Response
In Currency Conversion Processing, Currency Conversion Rates, replaced "The wholesale mid rates are obtained from the Member Profile 5—Currency Conversion Values, ISO code, ISO Rate, and Rate Exponent record in the daily Mastercard Parameter Extract (MPE) File (bulk ID T007)." with "The T057 Currency Conversion Rate File provides customers with Mastercard-Issued USD Rates and Mastercard-Issued Cross Rates, including wholesale mid rates."	Currency Conversion Rates
In Authorization and Preauthorization Processing Standards: • Removed text referring to requirements that went into effect 14 October 2016. • Added Middle East/Africa card acceptors to regions where initiated authorizations must clearly be distinguished as a final authorization or a preauthorization.	Authorization and Preauthorization Processing Standards
In Authorization and Preauthorization Processing Standards, Preauthorization, Final Authorization, and Undefined Authorization Transactions, removed text in Note—In addition, for CNP preauthorizations, the transaction amount must equal the approved authorization amount.	Preauthorization, Final Authorization, and Undefined Authorization Transactions

Description of Change	Where to Look
In Mastercard In Control Services, Mastercard Consumer Controls: • Added budget limits and travel to the listed features that issuers can offer available alerts and controls to their cardholders. • Removed static geolocation, MCCs, budgets, and filters from the listed features with alerts only.	Mastercard Consumer Controls
Added the new "Refund Transactions" section.	Refund Transactions
In the new Refunds Transactions section, added new subsection Refund Transaction Support Requirements.	Refund Transaction Support Requirements
In the Sweden Domestic Authorization Switching Service, replaced the information in the Refund Transactions section with a reference to the new Refund Transaction section in chapter 7.	Refund Transaction Processing
In Cardholder-Activated Terminals, updated reference citation from Mastercard Rules to Transaction Processing Rules.	Cardholder-Activated Terminals
In Cardholder-Activated Terminals, Automated Fuel Dispensers, updated text regarding Authorization Advice/0120 and Reversal Request/0400 messages.	Automated Fuel Dispensers
In Partial Approvals, replaced card-activated terminals (CATs) with transactions identified with MCC 5542 (Fuel Dispenser, Automated).	Partial Approvals
Added new option for Issuers to exchange a SPA1 key or to not enroll for the AAV validation service by completing Form 735. Added new section Digital Payment Data Field (DE 104). **NOTE: These changes in the manual are effective 5 November 2019.**	Universal Cardholder Authentication Field
Removed details regarding History Server due to it being retired. Added information regarding Smart Authentication service.	Mastercard Attempts and Smart Authentication AAV Service
Added Transaction Type Identifiers values C65, F07, F52, F53, F54, F61, and F64 to DE 48, subelement 77. **NOTE: These changes in the manual are effective 5 November 2019.**	Payment Transactions Payment Account Status Inquiry
Removed DE 124, subfields 1–4 from MoneySend Payment ASI Transaction Messages table.	Payment Account Status Inquiry
Chapter 8, Reports	
In Authorization Parameter Summary Report (SI737010-AA), Field Descriptions, Global Parameters, removed Refund Participant field that indicated an optional flag for the Europe region.	Global Parameters
Chapter 11, PSD2 Authentication Requirements	

Description of Change	Where to Look
Added new Chapter 11 PSD2 Authentication Requirements.	PSD2 Authentication Requirements
Appendix C: File Layouts	
In Appendix C: File Layouts, BIN Table Resource File: • File Layout: – Added new Anonymous Prepaid Indicator. • Detail Record: – Added new Anonymous Prepaid Indicator. – Reduced field name Filler attribute value from ans-19 to ans-18.	BIN Table Resource File

Contents

Chapter 1 System Overview

This section provides basic information about the Mastercard Authorization Platform: what it is, what it does, and whom it serves. The section highlights features of the Authorization Platform that contribute to its flexibility, usefulness, and adaptability to customer needs. It also directs you to additional sources of information regarding specific topics related to authorization.

About the Mastercard Authorization Platform

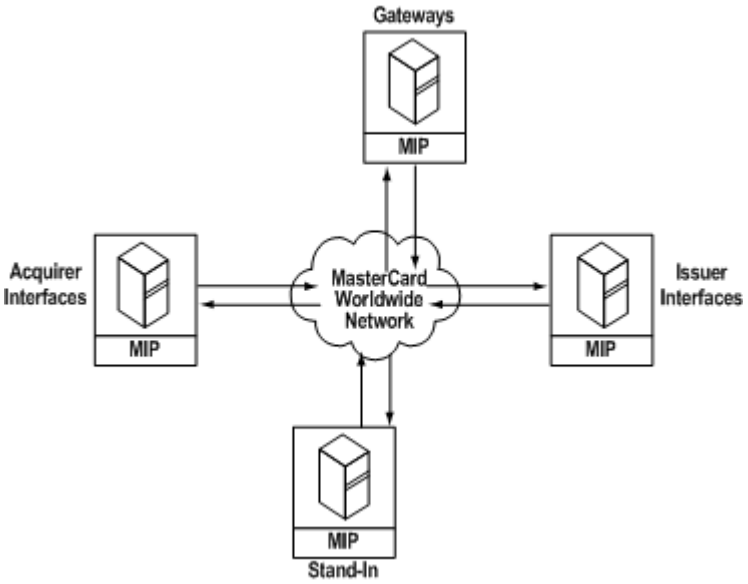
The Mastercard Authorization Platform is an international message processing system that serves all Mastercard principals, affiliates, and associations: large and small, automated and non-automated. The Authorization Platform transmits authorization validation data among issuers, acquirers, and points of interaction.

The Authorization Platform refers to both hardware (the physical communications lines of the Mastercard Network and Mastercard interface processors [MIPs]) and software (the Mastercard Network authorization application).

NOTE: Throughout this manual, functional references to online indicate an acquirer or issuer that is directly connected to a Mastercard MIP, and does not imply any web-based or Internet connotation.

Mastercard Network Components

This diagram illustrates the Mastercard Network components and interfaces.



NOTE: Mastercard reserves the right to record, store, and use all data transmitted via the Mastercard Authorization Platform in online electronic transactions, subject to Mastercard privacy and security compliance policies and applicable laws and regulations, without further notice.

MIP

The Mastercard interface processor (MIP) is a front-end communications processor placed on-site at a Mastercard customer's facility or at a processor or hub site. The MIP provides access to the Mastercard Network.

MIPs provide access to all Mastercard electronic funds transfer (EFT) products and to a wide variety of other EFT services via Mastercard gateways. MIP software supports issuing and acquiring functions, including routing Mastercard transactions to issuers, acquirers, and Stand-In System processing and switching non-Mastercard transactions to appropriate destinations via the gateways.

Mastercard is the sole and exclusive owner of the MIP and all MIP components, including all hardware, software, systems, and documentation placed by Mastercard at a customer's facility or other customer-designated location.

A customer may apply for use of a MIP by submitting a written request to Mastercard. If approved, effective as of the placement of the MIP at the facility identified by the customer, the customer is granted a non-exclusive, non-assignable license to use the MIP.

Mastercard Network

The Mastercard Network is the telecommunications and data transport mechanism that facilitates the routing and processing of financial transactions. The network links all Mastercard customers and data processing centers into a single online financial network.

Acquirer Interfaces

Most acquirers access the Mastercard Authorization Platform via the online method, through connectivity between the acquirer host and a MIP.

Mastercard offers other interfaces to acquirers that do not have online connectivity. Mastercard converts messages sent through these other interfaces into online messages.

Issuer Interfaces

Most issuers access the Mastercard Authorization Platform online, through connectivity between the issuer host and a MIP.

Stand-In System Processing

The Stand-In host contains the issuer information necessary to perform authorization processing for online issuers that are unavailable or that cannot be reached.

The Stand-In System also performs the following functions:

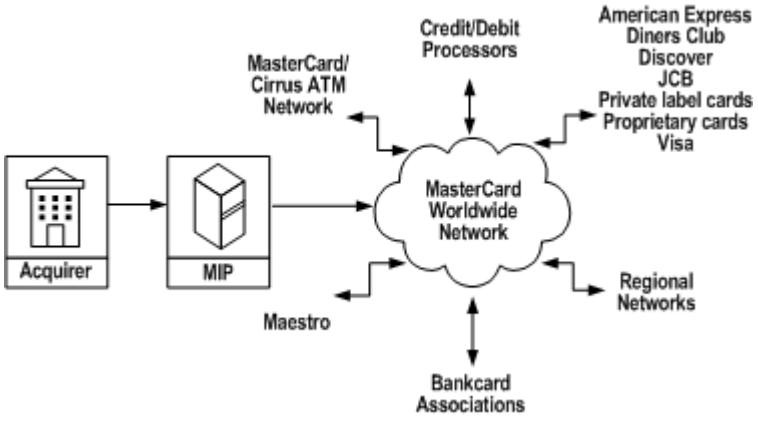
- Processes file maintenance to the Stand-In Account File, Electronic Warning Bulletin, or Local Stoplist.
- Processes network management messages for online customers.
- Generates Authorization Advice/0120 (store-and-forward) messages to advise online issuers of authorizations processed on their behalf.

Gateways

The Mastercard Network authorization application has interfaces called gateways that permit processing between the Mastercard Network and other networks.

Authorization Gateways

The following diagram illustrates Mastercard Network gateways.



Features of the Platform

To support customers, Mastercard developed and continues to enhance features of the Authorization Platform to meet customers' current and future needs.

The Authorization Platform provides the following features:

- Access to all customers 24 hours a day, 365 days a year
- Fast and cost-effective authorization processing
- Interfaces to support non–Mastercard card processing
- Backup to primary routing and authorizing paths
- Multiple currency conversion capability
- Support of security functions
- Reporting

Access to All Customers 24 Hours a Day, 365 Days a Year

The Mastercard Authorization Platform operates on a continuous basis, ensuring that cardholders can use a Mastercard card program anytime and that acquirers and issuers always have access to Mastercard authorization processing facilities.

Fast and Cost Effective Authorization Processing

The structure of the Mastercard Network enhances fast and cost-effective processing by allowing transactions to travel the shortest route to their destinations.

The network's design consists of redundant paths guaranteeing that there are always two or more paths to a given destination. If for some reason part of the network is down, this multiple routing structure of the Mastercard Network allows the transaction to continue to travel the next shortest route, eliminating congestion on the network.

Interfaces to Support Non-Mastercard Card Processing

The Authorization Platform supports Mastercard card products and non-Mastercard card products. Acquirers, therefore, can process a wide variety of card brands via their access to the Mastercard Network.

In addition to Mastercard products, the Authorization Platform supports processing of the following types of cards:

- American Express
- Diners Club
- Discover
- JCB
- Private label cards
- Proprietary cards
- Visa

Backup to Primary Routing and Authorizing Paths

At times, customers may experience internal communication problems, scheduled down times, or network problems. The Mastercard Authorization Platform provides backup authorization alternatives ensuring that an authorization response occurs for every authorization transaction.

Routing and authorizing alternatives include the following:

- The network routes transactions via multiple paths, decreasing the impact of trouble spots on the network.
- Stand-In processing uses issuer-established parameters to process authorization transactions at the St. Louis Operations Center on behalf of online issuers that are unavailable or cannot be reached.
- X-Code processing processes authorization transactions at the MIP or at the acquirer's host for transactions that cannot travel beyond that point.

Mastercard also provides routing and authorization alternatives that customers select ahead of time to enhance their productivity and the usefulness of the Authorization Platform to them. These alternatives include the following:

- Floor limit values allow the merchant to authorize certain transactions at the point-of-interaction without requesting authorization from the issuer. For a list of current floor limit values, refer to the *Quick Reference Booklet*.

- Special routing gives issuers the option of having authorization requests for cards within a particular bank identification number (BIN) range routed according to the parameters and endpoint established for some other BIN. For example, after acquiring a portfolio, an issuer can request special routing to ensure that authorization requests for the cards in the new portfolio are processed using the Stand-In limits and established endpoint for the issuer's other BINs.

Currency Conversion Processing

The Authorization Platform automatically provides a currency conversion service to acquirers and issuers to allow processing of online 01xx authorization and 04xx reversal transaction messages in the customer's preferred currency.

Support of Security Functions

In conjunction with authorization processing, Mastercard offers security services to minimize risk.

- Account Management System (AMS)
- Address Verification Service (AVS)
- Card Validation Code (CVC) verification
- Cardholder Authentication
- Digital Secure Remote Payment (DSRP)
- Expert Monitoring Solutions Hosted by Mastercard
- Global Automated Referral Service (GARS)
- M/Chip Cryptogram Pre-validation Service
- M/Chip Cryptogram Validation in Stand-In Processing
- Mastercard® Contactless Mapping Service
- Mastercard Digital Enablement Service (MDES)
- Mastercard In Control™ Mapping Service
- Mastercard® Masterpass™
- Mastercard® *Identity Check*™ Accountholder Authentication Value (AAV) Verification
- Mastercard® *Identity Check*™ Dynamic AAV Verification in Stand-In Processing
- Personal Identification Number (PIN) verification

For more information about AMS, refer to the *Account Management System User Manual*. For detailed information about the remaining services listed above, refer to Authorization Services Details.

Account Management System

Account Management System (AMS) provides issuers with the ability to identify and to flag specific accounts that require special handling for services such as the Electronic Warning Bulletin, Contactless Mapping Service, Product Graduation, and Enhanced Value.

Address Verification

The Address Verification Service (AVS) reduces the risk of non–face-to-face transactions through validation of the cardholder's billing address. AVS supports transmission of address

data, allowing the user to compare the billing address requested for the transaction with the billing address on file for the cardholder.

Card Validation Code Verification

Card Validation Code (CVC) is a card security feature.

CVC 1 is a code algorithmically derived by the issuer and encoded in the magnetic stripe. This code helps the issuer determine if the card is genuine or counterfeit.

CVC 2 is a three-digit code algorithmically derived by the issuer and indent printed on the signature panel to the right of the account number.

CVC 3 is a code algorithmically derived by a Mastercard® contactless magnetic stripe profile card or device. This code is used by the issuer to validate the contactless card or device that submitted the transaction as genuine. Mastercard supports validation services for dynamic CVC 3.

Chip CVC is a code algorithmically derived by the issuer and encoded in the Track 2 Equivalent Data field contained in the chip.

Cardholder Authentication

Mastercard is working to assist issuers and governments globally to reduce cost and eliminate fraud in their benefit disbursement process. To support those efforts, Mastercard provides a new indicator for cardholder authentication to enable certain government programs to confirm the identity of the cardholder.

When populated, this authentication indicator signifies that the account holder was authenticated using a biometric match.

This authentication indicator uses details stored on the EMV Chip card to authenticate the intended cardholder.

Mastercard offers the following authentication service options:

- Authentication Service Type 1
- Authentication Service Type 2

Digital Secure Remote Payment

A DSRP is an electronic commerce Transaction that contains cryptographic information, in the form of either full EMV chip data passed in DE 55 or a cryptographic value derived from an M/Chip cryptogram passed in either the Universal Cardholder Authentication Field (UCAF) or the Digital Payment Data Field (DE 104). Subsequent to the initial DRSP transaction, a related transaction for a partial shipment may occur, in which case, cryptographic information is not passed. When a DSRP transaction contains tokenized account information, MDES performs token mapping and cryptographic validation services.

Expert Monitoring Solutions Hosted by Mastercard

Expert Monitoring Solutions hosted by Mastercard provide issuers with a comprehensive suite of fraud solutions designed to detect and prevent fraudulent transactions and provide global acquirers with a real-time fraud scoring solution for merchants on U.S.-issued, dual message card-not-present (CNP) authorization transactions.

Global Automated Referral Service

Global Automated Referral Service (GARS) supports issuer call referrals by providing the acquirer with a single phone number to respond to any call referral. This increases the completion rate of call referrals issued.

M/Chip Cryptogram Pre-validation

The M/Chip Cryptogram Pre-validation service is for issuers that use the M/Chip Select 2.0, M/Chip Lite 2.1, M/Chip 4.0 (Mastercard, EMV CSK, and EMV2000 session key derivation methods), M/Chip™ Advance, and EMV CCD-compliant chip cards.

This service validates the Authorization Request Cryptogram (ARQC) and generates the Authorization Response Cryptogram (ARPC) on behalf of an issuer.

M/Chip Cryptogram Validation in Stand-In Processing

The M/Chip Cryptogram Validation in Stand-In Processing service is available for issuers that use the M/Chip Select 2.0, M/Chip Lite 2.1, M/Chip 4.0 (Mastercard, EMV CSK, and EMV2000 session key derivation methods), M/Chip™ Advance, and EMV CCD-compliant chip cards.

NOTE: All issuers globally that participate in Stand-In processing must have M/Chip Cryptogram Validation in Stand-In Processing performed during Stand-In processing.

The M/Chip Cryptogram Validation in Stand-In Processing service supports issuers that process chip transactions on an ongoing basis, including the validation of the Authorization Request Cryptogram (ARQC) and generation of the Authorization Response Cryptogram (ARPC) on their hosts when the issuer is signed out, the transaction cannot be delivered to the issuer, or the issuer timed out.

Mastercard Contactless Mapping Service

Mastercard offers the Contactless Mapping Service as an optional service that helps issuers process contactless transactions by translating a unique contactless account number into a primary account number (PAN) that issuers can process with minimal impact.

The Contactless Mapping Service is not available to issuers that support the use of online PIN with a card or device product. If PAN mapping is performed in a transaction using online PIN, the PIN validation will fail.

Mastercard Digital Enablement Service

Mastercard offers MDES to allow issuers to digitize card accounts into smart devices or secure cloud-based solutions. MDES enables issuers to support proximity and remote payments from smart devices and remote payment applications without having to make extensive upgrades to their systems.

Mastercard In Control Mapping Service

Mastercard In Control™ provides capabilities using virtual card numbers at the point-of-interaction. Mastercard In Control leverages the same data elements for mapping a virtual card number (VCN) and a real card number (RCN).

Mastercard Masterpass

Mastercard® 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.

Mastercard *Identity Check* AAV Verification

Mastercard offers a Mastercard® *Identity Check*™ dynamic and static Accountholder Authentication Value (AAV) verification service on every authorization transaction that contains the Universal Cardholder Authentication Field (UCAF™) data regardless of whether the issuer's host system is available or unavailable to respond to the Authorization Request/0100 message.

NOTE: Mastercard Identity Check will replace Mastercard *SecureCode* as the consumer-facing brand for Mastercard's Identity suite of authentication solutions by December 2019. For more information, refer to *Global Security Bulletin* No. 6, 15 June 2017 or the *Mastercard Identity Check Program Guide*.

NOTE: Effective November 2019 with Release 19.Q4, Mastercard *Identity Check* AAV validation will be enhanced for SPA2 version AAVs.

Mastercard *Identity Check* AAV Verification in Stand-In Processing

Mastercard offers AAV verification service for authorization transactions processed by the Stand-In System that contain AAV data in DE 48 (Additional Data—Private Use), subelement 43 (Universal Cardholder Authentication Field [UCAF™]) of the Authorization Request/0100 message.

NOTE: All issuers globally that participate in Stand-In processing must have *Identity Check* AAV verification in Stand-In performed during Stand-In processing if they perform self-validation during normal authorization processing.

Issuers may request that Stand-In System processing only perform the AAV verification test when the issuer's host system is unavailable to respond to the Authorization Request/0100 message containing AAV data.

NOTE: Mastercard Identity Check will replace Mastercard® *SecureCode*™ as the consumer-facing brand for Mastercard's Identity suite of authentication solutions by December 2019. For more information, refer to *Global Security Bulletin* No. 6, 15 June 2017 or the *Mastercard Identity Check Program Guide*.

PIN Verification

Personal identification number (PIN) is a proven technology for authenticating the identity of the cardholder. Mastercard provides an optional PIN verification service for all purchase transactions that contain a PIN. A PIN Verification in Stand-In System processing service also is available.

Reporting

Mastercard produces a variety of authorization-related reports that display customer authorization activity and that help customers plan and manage their authorization process.

For more information about reports and sample report layouts, refer to Reports.

EMV Chip Card Technology

EMV chip card technology offers substantial benefits and unique transaction features. EMV chip cards offer a secure means to authenticate both the card and the cardholder.

Business Benefits of EMV Chip Card Technology

EMV chip card technology offers four major business benefits to the payment business:

- Reduces fraud—both counterfeit and "lost, stolen, never received" fraud.
- Enhances credit control.
- Reduces operational costs.
- Provides a platform for added-value opportunities.

Functions Unique to EMV Chip Card Technology

M/Chip cards and EMV chip cards offer unique transaction features, such as:

- Fully offline—Through card and terminal interaction, an EMV transaction may take place in a fully offline mode.
- Offline personal identification number (PIN)—Depending on product rules and thus EMV chip card personalization and terminal capabilities, the PIN may be checked offline.
- Offline and Online CAM—Allows verification if an EMV chip card is genuine.
- Control of offline spending—Allows a method of controlling the maximum number of consecutive offline transactions, maximum cumulative amount, and risk assessment of the transaction.

NOTE: EMV chip card is a generic name for all EMV card applications (for example, M/Chip, SECCOS [Germany], CPA [EMVCo], UKIS [UK], VSDC [Visa], and APSS [Austria]). M/Chip is the Mastercard recommended EMV application (that is, the Mastercard chip card application that supports the EMV transaction flow with the terminal). M/Chip is designed to support specific Mastercard products' features/requirements.

For more information about EMV transactions, refer to EMV Transactions.

Chapter 2 Basic Authorization Concepts

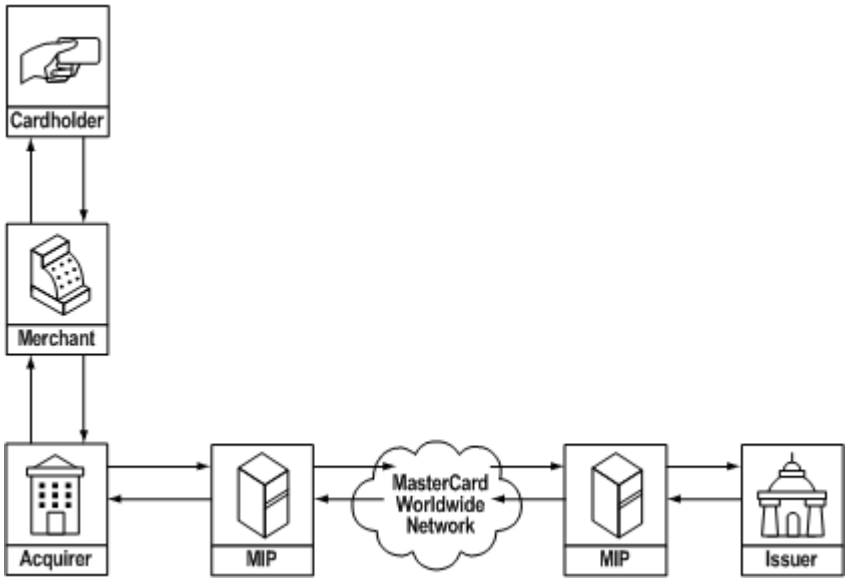
This section presents basic and alternative authorization concepts used by the Mastercard Authorization Platform.

Participants in Authorization Processing

There are entities that participate in a typical authorization transaction in relation to each other and the Mastercard Network.

Participants in a Typical Authorization Transaction

The following diagram illustrates participants in a typical authorization transaction.



Cardholder

A cardholder is a person to whom a card has been issued or a person who is authorized to use the card. In an authorization transaction, the cardholder presents the card or cardholder account number as payment in exchange for goods or services.

Merchant

The merchant is a retailer, or any other person, firm, or corporation that (pursuant to a merchant agreement) agrees to accept credit cards, debit cards, or both, when properly presented.

Acquirer

An acquirer is a licensed customer that acquires the data relating to a transaction from the card acceptor or merchant and submits that data for authorization. The acquirer also supports clearing and settlement functions to exchange funds between the issuer and the merchant.

Issuer

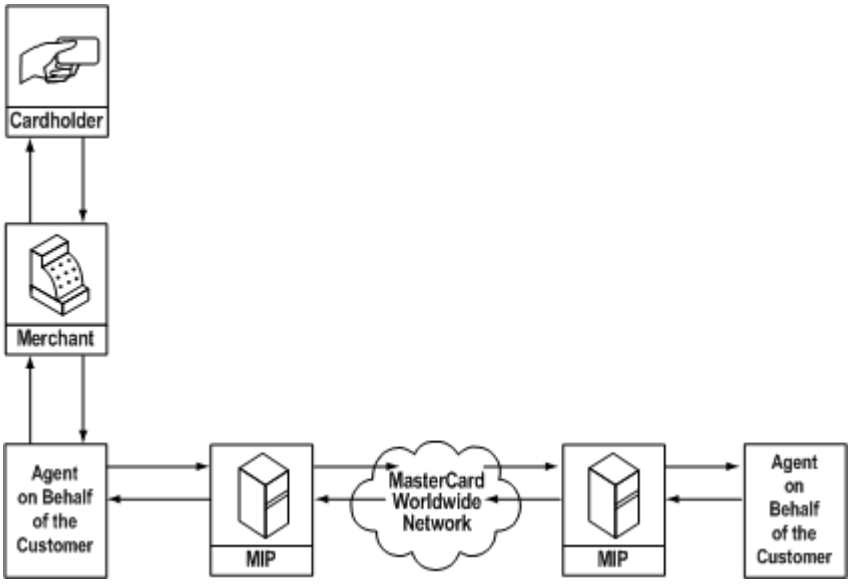
An issuer is a licensed customer that issues cards and is responsible for approving or declining authorization requests. The issuer also bills cardholders and supports clearing and settlement functions to exchange funds between the cardholder and the acquirer.

Other Participants

Other entities may participate in the authorization transaction in place of the issuer and acquirer.

Other Participants in a Typical Authorization Transaction

This diagram illustrates other entities that may participate in the authorization transaction in place of the issuer and acquirer. It shows these entities in relation to each other and to the cardholder, merchant, and the Mastercard Network.



As this diagram shows, an issuer or acquirer may contract with an agent to perform any of a variety of authorization functions on behalf of the customer. The agent may assist a customer in such activities as issuing cards, processing authorization transactions, or processing card portfolios.

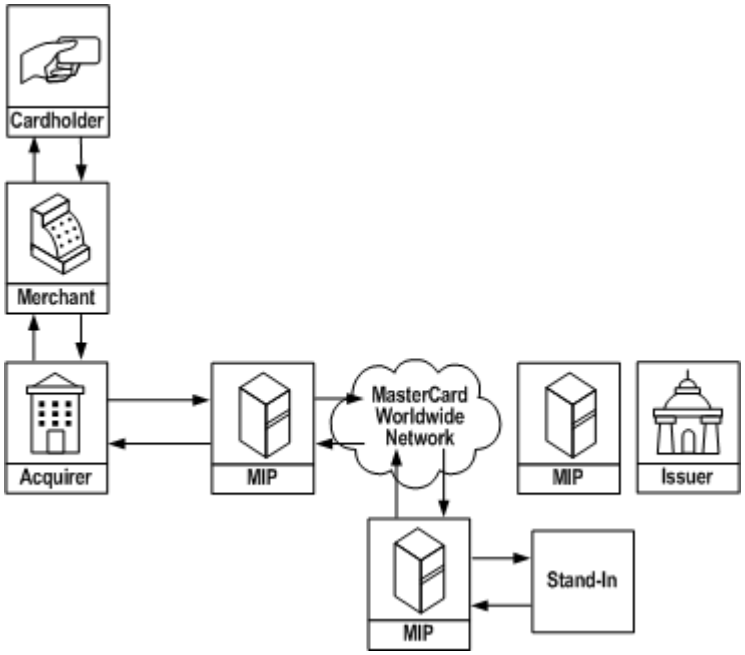
NOTE: Throughout this manual, functional references to issuers and acquirers also refer to others acting as authorized agents for issuers or acquirers. Mastercard customers are responsible for the acts and omissions of their agents, including those with respect to Mastercard rules, regulations, policies, and procedures.

Mastercard Acting On-behalf of Issuers

These diagrams show that Mastercard can act on behalf of the issuers.

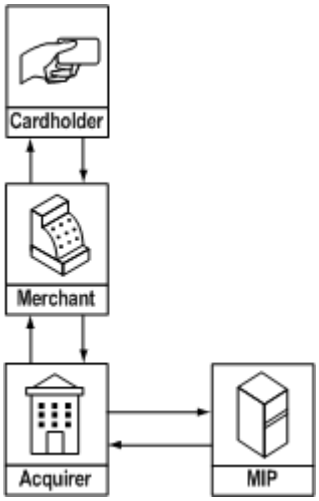
Mastercard Stand-In System Processing Acting in Issuing Capacity

Mastercard Stand-In System acts on behalf of the issuers by receiving authorization requests and generating authorization responses based on the issuer's predetermined parameters.



Mastercard X-Code Processing Acting in Issuing Capacity

Mastercard X-Code System performs issuer functions by receiving and responding to authorization requests at the acquirer MIP.



Accessing the Authorization Platform

To process authorization activity, acquirers and issuers must access the Mastercard Network. This network is the path by which they send and receive authorization messages and related data.

Selecting a particular authorization processing access method depends on a number of factors, including:

- Physical installations present at the point-of-interaction and at the customer site
- Volume of incoming and outgoing authorizations
- Customer location

For help in selecting an appropriate access method, contact a Customer Implementation Services specialist.

Acquirer Methods

Online host-to-MIP access is available to acquirers. There are several confirmations for connectivity to a MIP or MIPs for online access.

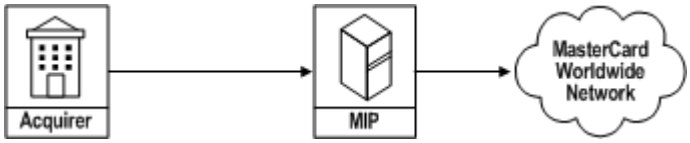
NOTE: Mastercard discontinued support of telex call referrals. Customers that previously used telex services must register to use Global Automated Referral Service (GARS). For more information about GARS, refer to Global Automated Referral Service.

Online Host-to-MIP Access

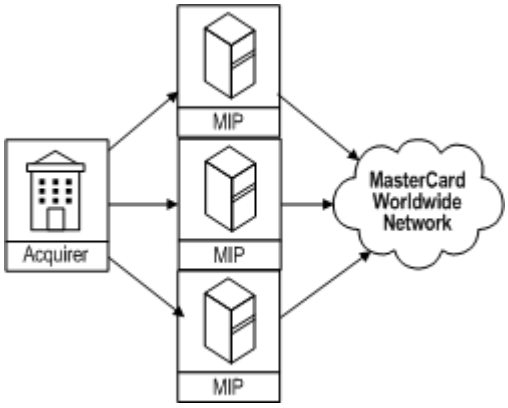
The following diagrams show configurations for connectivity to a MIP or MIPS for online access.

Acquirer Online—Direct Host to MIP Connectivity

To have direct connectivity to a MIP, the acquirer must have a host computer that can support this type of connectivity.

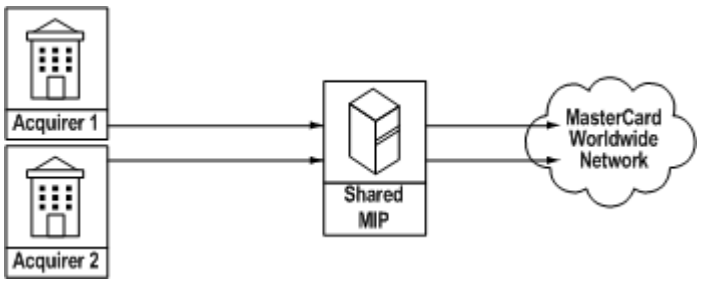


Acquirer Online—Direct Host to Multiple MIP Connectivity



Acquirer Online—Shared MIP Connectivity

When several acquirers have connectivity to a shared MIP, the MIP is located at the site of one of the acquirers. Other acquirers access the MIP via a dedicated phone line. The acquirer with the MIP on-site controls the MIP console.



Issuer Methods

Issuers may choose the online host-to-MIP access to the Mastercard Network.

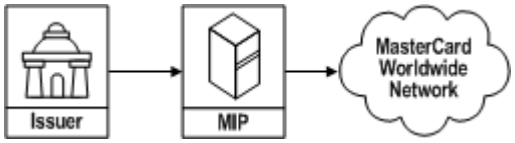
Online Host-to-MIP Access

Online host-to-MIP issuers receive authorization requests from the Authorization Platform via a MIP connected to the issuer's host. They format and return authorization request responses directly using the messages outlined in the *Customer Interface Specification* manual.

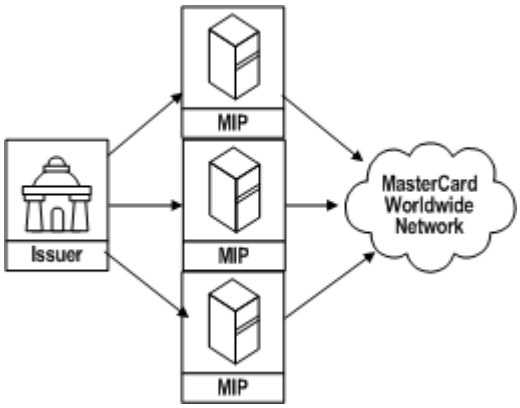
The following diagrams show configurations for connectivity to a MIP or MIPs for online access.

Issuer Online—Direct Host to MIP Connectivity

To have direct connectivity to a MIP, the issuer must have a host computer that can support this type of connectivity.

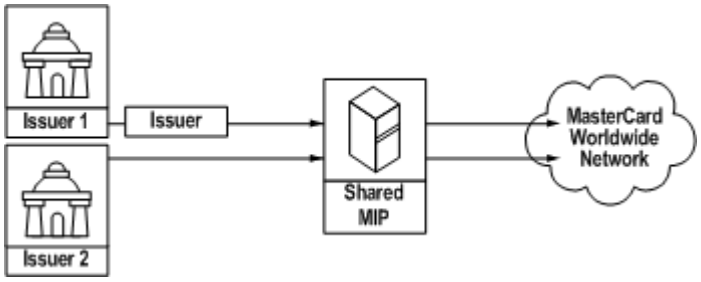


Issuer Online—Direct Host to Multiple MIP Connectivity



Issuer Online—Shared MIP Connectivity

When several issuers have connectivity to a shared MIP, the MIP is located at the site of one of the issuers. Other issuers access the MIP via a dedicated phone line. The issuer with the MIP on-site controls the MIP console.



Authorization Responses

Every authorization request receives an authorization response that directs the acquirer or the merchant on how to proceed with the transaction.

The response received is typically a code that identifies the action that the merchant should take. The format of the authorization response depends on the acquirer's access method.

If the acquirer is online, the Authorization Request Response/0110 message includes a two-digit response code in DE 39 (Response Code). This code informs the acquirer of the action to be taken (approve, decline, refer to card issuer, capture card, or valid). For a complete list of all possible DE 39 response codes and the actions they should prompt, refer to the *Customer Interface Specification* manual.

Regardless of the format in which the authorization response is received, the response always prompts one of the following actions on the part of the merchant:

- Approve
- Decline
- Refer to card issuer
- Capture card
- Valid (not declined)—used for non-financial transaction types only

Approve

The transaction is authorized as reported.

For magnetic stripe, chip, and key-entered transactions, the issuer provides a six-digit authorization code to the acquirer when it approves a transaction for the purchase of goods or services or cash disbursement.

The merchant still must perform its normal review process (steps such as verifying the signature on the card are often included) before completing the transaction.

Decline

The merchant may not complete the transaction. The merchant may return the card, but may not accept the card in payment for the program or service for that transaction amount.

Refer to Card Issuer

The acquirer or merchant must contact the card issuer for further instructions. The call referral is a fraud prevention tool that the issuer should use when it suspects or is attempting to prevent fraud at the point-of-interaction. Acquirers may use the Global Automated Referral Service (GARS). GARS will route acquirer calls to the Stand-In System if the issuer is not registered to receive GARS calls. A Stand-In approval response will be a valid response to the call referral.

Mastercard encourages effective issuer use of the refer to card issuer authorization response through a tiered pricing structure for excess call referral transactions. Higher charges apply for lower transaction amounts, and lower charges apply for higher transaction amounts. For more information, refer to the *Mastercard Consolidated Billing System* manual.

Mastercard Stand-In System processing never generates a refer to card issuer response in the following situations:

- When the transaction is a mail order/telephone order (MO/TO) or electronic commerce transaction
- When the acquirer is responding to a refer to card issuer response, the issuer is unavailable, and Stand-In System processes the GARS transaction
- When the transaction is an ATM transaction
- When the issuer's call center is closed

Capture Card

The acquirer or merchant must use its best efforts to retain the card by reasonable and peaceful means. For instructions on how to return a recovered card to the issuer, refer to the *Security Rules and Procedures* manual.

Valid

Issuers provide a valid response when processing balance inquiry, account status inquiry, or other non-financial types of requests. The valid response indicates to the acquirer or merchant that the request was completed successfully by the issuer, that is, the balance returned, address verification response information provided, if requested, and so on. Merchants use the information returned in the response message to provide information to the cardholder or to determine if further authorization decisioning is required.

X-Code Processing

X-Code processing applies only when the acquirer is online. It can occur at either of the following locations: acquirer host or acquirer MIP.

These descriptions apply only to Mastercard card programs. For X-Code processing of all other card brands, refer to X-Code Processing of Non-Mastercard Card Programs.

Acquirer Host X-Code Processing

Acquirer host X-Code processing occurs when the acquirer host cannot communicate with the acquirer MIP.

Acquirer Host X-Code Flow

1. The acquirer creates an authorization request; however, the acquirer host cannot communicate with the acquirer MIP.
2. The acquirer responds to the authorization request based on the rules for acquirer host X-Code processing.
3. The acquirer may be required to phone the issuer for approval based on the rules for X-Code processing.

Rules for Acquirer Host X-Code Processing

For acquirer host X-Code processing, the acquirer must approve and bear liability for the transaction, after validating that the account is not listed as restricted on the Electronic Warning Bulletin file, when the transaction amount is less than or equal to USD 300, except in the circumstances listed below.

The issuer bears liability for authorization requests that it approves. The acquirer must phone the issuer for approval in any of the following instances:

- The transaction amount is more than USD 300.
- The card is not present.
- The merchant suspects that the card may be stolen or counterfeit, or the transaction or the customer causes the merchant to be suspicious.
- The transaction type is one of the following: PIN transactions, unique, mail order/telephone order, electronic commerce order, Payment Transaction, or non-financial transactions (such as balance inquiry, PIN management).

If the transaction amount is more than USD 300 and the acquirer cannot reach the issuer, the acquirer may do any of the following:

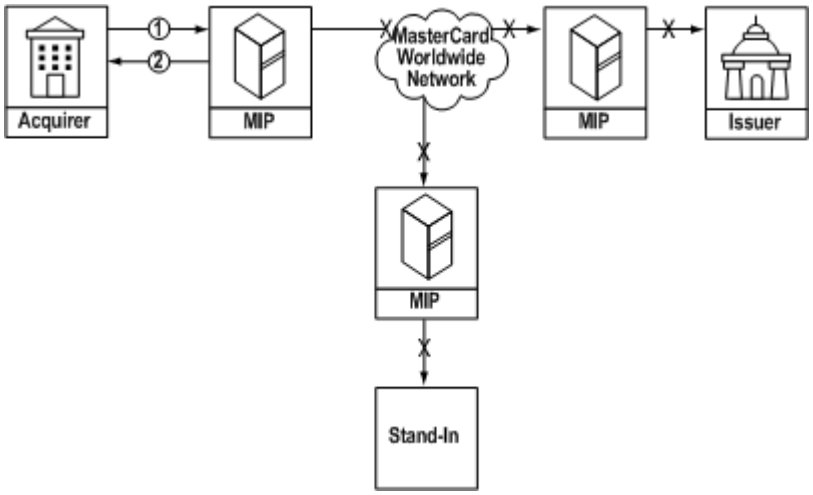
- Approve the transaction (and bear liability for the total amount)
- Decline the transaction
- Continue attempting to reach the issuer

If the acquirer has not phoned the issuer for approval, the acquirer can create an Authorization Advice/0120—Acquirer-generated message to notify the issuer of the approved authorization based on the previously stated rules for X-Code processing.

Acquirer MIP X-Code Processing

Acquirer MIP X-Code processing occurs when the acquirer MIP cannot communicate with the Mastercard Network or the acquirer MIP does not receive a response from the issuer or the Stand-In System within the time frame established by Mastercard.

Acquirer MIP X-Code Flow



1. The authorization request is routed to the acquirer MIP on its way to the issuer. However, one of the following scenarios occurs:
   - The acquirer MIP cannot communicate with the Mastercard Network.
   - The Mastercard Network cannot communicate with the issuer MIP and the Mastercard Network cannot communicate with the Stand-In MIP.
   - The Mastercard Network cannot communicate with the issuer MIP and the Stand-In MIP cannot communicate with the Stand-In host.
   - The Mastercard Network cannot communicate with the Stand-In MIP and the issuer MIP cannot communicate with the issuer host.
2. The acquirer MIP generates an authorization response as follows:

MIP X-Code Authorization Response	Type of Transaction
Decline	– Account Status Inquiry Service requests – ATM Installment Inquiry – AVS transactions – Balance inquiries – Internet gambling transactions (MCC 7995 and CAT Level 6) involving U.S. region-issued cards – Private Label transactions – Product Inquiry Service – Transactions that contain a PIN – Transactions that contain the merchant suspicious indicator – Transactions that occur at a cardholder-activated terminal (CAT)/Level 1 – Transactions using a Mastercard card not eligible for X-Code processing
Refer to Card Issuer	– Cash disbursement – Payment Transaction – Unique – Transactions using a Mastercard card that is eligible for X-Code processing and the transaction exceeds the Mastercard X-Code limits
Capture Card	Transactions for accounts that are listed on the Electronic Warning Bulletin file
Approve	Transactions that are less than or equal to the Mastercard X-Code limits and do not meet any of the criteria listed above

The Authorization Platform generates Authorization Advice/0120 messages to report the results of X-Code processing. Online issuers can retrieve the messages using the process described in Online Messages.

MIP X-Code Limits

Established X-Code limits are listed in table format. Transactions must be less than or equal to these limits to be approved.

Type of Transaction	MIP X-Code Limits
Transactions using: • MBK—Mastercard Black • MCH—Mastercard Premium Charge • MCT—Titanium Mastercard • MCW—World Mastercard™ Card • MFB—Flex World Elite • MFD—Flex Platinum • MFE—Flex Charge World Elite • MFH—Flex World • MFL—Flex Charge Platinum • MFW—Flex Charge World • MHP—HELOC Platinum Mastercard • MHW—HELOC World Mastercard • MNW—Mastercard New World • MPL—Platinum Mastercard® Card • MUW—Mastercard World Domestic Affluent • MWD—World Deferred • MWE—Mastercard World Elite • MWR—World Retailer Centric Payment • WBE—World Mastercard® Black Edition • WMR—World Mastercard Rewards	USD 950

Type of Transaction	MIP X-Code Limits
Transactions using: • MAB—World Elite™ Mastercard® Business • MAC—Mastercard® Corporate World Elite® • MBD—Mastercard Professional Debit Business Card • MBS—Mastercard® B2B Product • MCB—Mastercard BusinessCard® Card • MCG—Gold Mastercard® Card • MCM—Mastercard Corporate Meeting Card • MCO—Mastercard Corporate • MDB—Debit Mastercard BusinessCard Card • MDQ—Middle Market Corporate Card • MEB—Mastercard Executive BusinessCard Card • MEO—Mastercard Corporate Executive Card® • MHG—HELOC Gold Mastercard • MLA—Mastercard Central Travel Solutions Air • MLC—Mastercard Micro-Business Card • MLD—Mastercard Distribution Card • MLL—Mastercard Central Travel Solutions Land • MPB—Mastercard Preferred BusinessCard • MPC—Mastercard Professional Card • MWB—World Mastercard® for Business • MWO—Mastercard Corporate World • TCB—Mastercard Business Card—Immediate Debit • TCO—Mastercard Corporate—Immediate Debit • TEB—Mastercard Executive BusinessCard Card—Immediate Debit • TEO—Mastercard Corporate Executive Card—Immediate Debit • TLA—Mastercard Central Travel Solutions Air—Immediate Debit • TPB—Mastercard Preferred Business Card—Immediate Debit • TPC—Mastercard Professional Card—Immediate Debit	USD 600

Type of Transaction	MIP X-Code Limits
Transactions using: • MAP—Mastercard Commercial Payments Account • MCC—Mastercard® Credit Card (mixed BIN) • MCF—Mastercard Corporate Fleet Card® • MCP—Mastercard Corporate Purchasing Card® • MCS—Mastercard® Standard Card • MCV—Merchant-Branded Program • MDM—Middle Market Fleet Card • MDN—Middle Market Purchasing Card • MGF—Mastercard® Government Commercial Card • MHC—Mastercard Healthcare Credit Non-substantiated • MHS—HELOC Standard Mastercard • MIC—Mastercard Credit Standard Student Card • MNF—Mastercard® Public Sector Commercial Card • MPE—Name for GCMS Product ID MPE • MRF—European Regulated Individual Pay • MRO—Mastercard Rewards Only • MRP—Standard Retailer Centric Payments • MSP (Muse Mastercard) • TCF—Mastercard Fleet Card—Immediate Debit • TCP—Mastercard Purchasing Card—Immediate Debit • TDN—Middle Market Mastercard Purchasing Card—Immediate Debit • TNF—Mastercard Public Sector Commercial Card—Immediate Debit	USD 400
Transactions using: • MDL—Business Debit Other Embossed • WDR—World Debit Mastercard Rewards	USD 250
In-flight Commerce Terminal/Level 4 gaming transaction (TCC is U and MCC is 7995). For CAT Level 4 non-gaming transactions, X-Code limits apply.	USD 350

Type of Transaction	MIP X-Code Limits
Transactions using all other Mastercard cards: ACS, AMX, BPD, CBL, CIR, DAG, DAP, DAS, DCC, DDB, DLG, DLH, DLI, DLP, DLS, DLU, DOS, DSV, DWF, JCB, MAQ, MAV, MBB, MBC, MBE, MBF, MBM, MBP, MBT, MBW, MCA, MCE, MCU, MDG, MDH, MDI, MDJ, MDK, MDO, MDP, MDR, MDS, MDT, MDU, MDW, MEC, MED, MEP, MET, MFR, MHA, MHB, MHD, MHH, MHK, MHL, MHM, MHN, MIA, MIB, MID, MIG, MIH, MIJ, MIK, MIL, MIP, MIS, MIU, MLB, MLE, MLF, MOC, MOG, MOP, MOW, MPA, MPD, MPF, MPG, MPH, MPJ, MPK, MPM, MPN, MPO, MPP, MPQ, MPR, MPT, MPV, MPW, MPX, MPY, MPZ, MRB, MRC, MRG, MRH, MRJ, MRK, MRL, MRS, MRU, MRW, MSA, MSB, MSD, MSF, MSG, MSI, MSJ, MSM, MSN, MSO, MSQ, MSR, MSS, MST, MSV, MSW, MSX	USD 0

Liability for X-Code Transactions

The issuer is liable for transactions that are approved under acquirer MIP X-Code, up to the MIP X-Code limits specified in previous table.

X-Code Processing of Non-Mastercard Card Programs

Acquirer Host X-Code processing of non-Mastercard cards is subject to the guidelines of the individual card brand.

Acquirer MIP X-Code processing of non-Mastercard cards is the same as for Mastercard cards with the following exceptions and clarifications.

This table shows MIP X-Code limits for non-Mastercard cards.

Type of Transaction	MIP X-Code Limit	Response if the transaction is greater than the limit
All Visa	0	Decline
Non-Mastercard, non-Visa MO/TO, electronic commerce, ATM, and merchant suspicious	0	Decline
All other non-Mastercard, non-Visa	0	Refer to Card Issuer

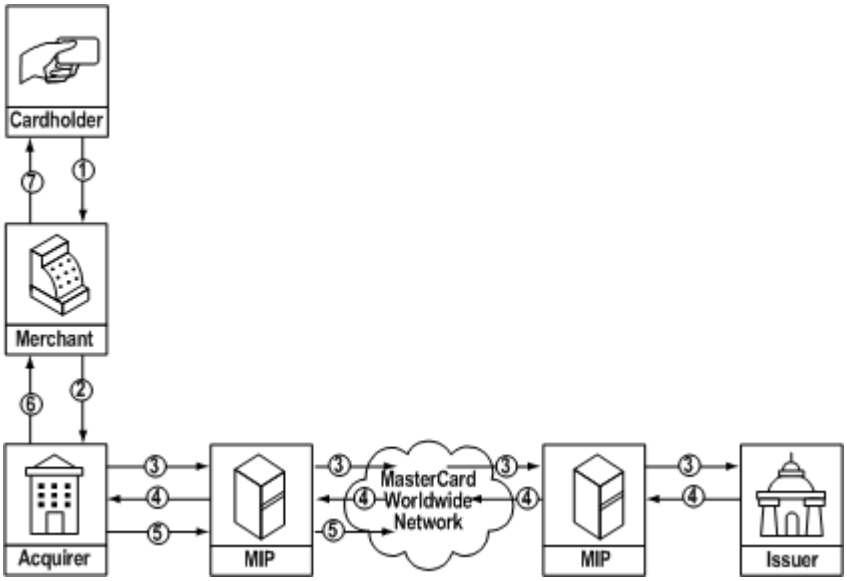
Chapter 3 Mastercard Authorization Message Flows

This section explains the flow of authorization messages that involve a Mastercard card.

Basic Authorization Flow

Although the authorization process contains many variables for routing and authorizing, it is helpful to have an understanding of the basic flow of an authorization request.

The following diagram illustrates the basic authorization flow. This flow assumes that the card involved is a Mastercard® card, that the issuer and acquirer are online customers, and that the issuer has instructed Mastercard to forward all requests.



1. The cardholder presents the card to the merchant for a face-to-face transaction or provides the card number, expiration date, name, and address when placing a mail, phone, or electronic commerce (e-commerce) order.
2. The merchant forwards the transaction to the acquirer for approval.
3. The acquirer requests authorization for the transaction by generating an authorization request message. The authorization request travels through an acquiring Mastercard interface processor (MIP) to the Mastercard Network, through an issuer MIP, and then to the issuer's host.
4. The issuer returns an authorization response message to the acquirer to indicate what action the merchant should take for the transaction. The authorization response travels through the Mastercard Network to the acquirer.
5. Online acquirers may send an authorization acknowledgement message confirming receipt of the response.
6. The acquirer responds to the merchant.
7. The merchant completes the transaction according to the authorization response returned.

NOTE: Throughout the remainder of this section, diagrams omit reference to the cardholder and merchant.

Variations on the Basic Authorization Flow for Mastercard Cards

Authorization flows will vary from the basic authorization flow when certain situations apply.

- Authorization processing occurs at the acquirer MIP.
- The issuer is online but the transaction cannot follow the primary path.
- The EMV chip card authorizes the transaction offline.

NOTE: Throughout this manual, the acquirer MIP in the diagrams refers to which MIP accepts the authorization request and forwards it through the Mastercard Network.

Authorization Processing Occurs at the Acquirer MIP

The acquirer MIP (and not the issuer) processes the authorization transaction when any of these situations occurs.

- MIP edits at the acquirer MIP cause an error response.
- X-Code processing applies.
- On-behalf processing applies.

MIP Edits Cause an Error Response by the Acquirer MIP

The acquirer MIP performs certain editing functions to ensure validity and inclusion of required fields. If the transaction does not pass certain edits, the authorization request goes no further than the MIP, which returns an error response. To determine which fields are mandatory, which are dependent on specific conditions, and which are optional, refer to the *Customer Interface Specification* manual.

X-Code Processing Applies

Refer to Basic Authorization Concepts.

On-behalf Processing Applies

MIP performs on-behalf services and may reject transactions per issuer or issuer- or cardholder-established criteria such as for Mastercard In Control™ processing.

For more information about on-behalf processing, refer to Authorization Services Details.

Issuer Is Online but the Transaction Cannot Follow the Primary Path

If a transaction involving an online issuer cannot follow the basic authorization flow, it follows a secondary path or a tertiary path.

If the Authorization Platform cannot route these transactions via the primary path to the issuer, it may result in a response indicating the requested service is not available. This can occur for any of the following services:

- Transactions that contain an Account Status Inquiry Service or Product Inquiry Service request receive a response of service not available.
- Transactions that contain an authorization request and an AVS request—the authorization request receives the appropriate authorization response and the AVS request receives a response of service not available.
- Balance inquiry transactions at ATM and POS receive a response of service not available.
- ATM Credit Card Cash Advance in Installments transactions receive a response of service not available.
- PIN management transactions receive a response of service not available.
- Funding transactions with a credit card at an ATM receive a response of service not available.
- Private label prepaid card activation plus initial load transactions receive a response of service not available.
- Refund transactions receive a response of service not available.

For details about processing flows and transaction responses for these services, refer to the *Customer Interface Specification* manual.

Secondary Path for Online Customers—Stand-In System Processing

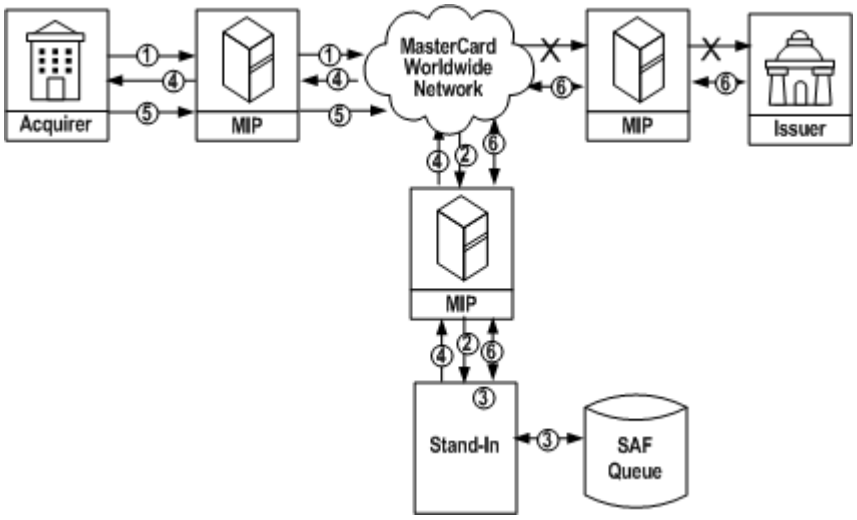
Stand-In System processing is mandatory for Mastercard credit products in all regions. Issuers may choose to block Stand-In System processing for debit products in all regions, except in the U.S. region.

If any of the following conditions apply for online issuers that support the Stand-In System as their secondary path, the system routes the transaction to Stand-In processing:

- The issuer is not signed in.
- The transaction could not be delivered to the issuer.
- The issuer does not respond with an Authorization Request Response/0110 message in the allotted amount of time, causing a time out at the acquiring MIP. For more information about response times, refer to Routing Timer Values.
- The issuer's response message contains invalid formatting or information resulting in an issuer edit error.

In these cases, the transaction follows the flow depicted in the following diagram.

Secondary Path for Online Customers—To Stand-In System Processing



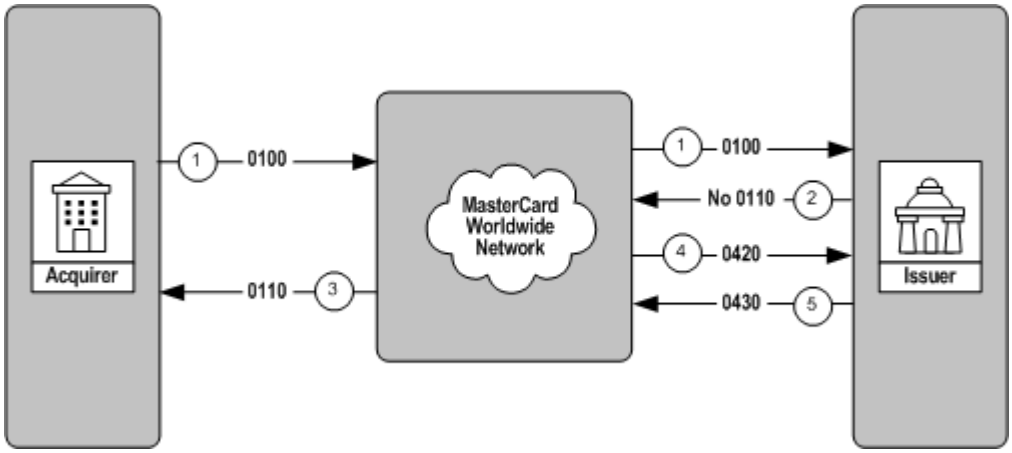
1. After receiving the merchant request for authorization, the acquirer generates an authorization request, which travels through the Mastercard Network.
2. The Mastercard Network, unable to route the authorization request to the online issuer, routes it to Stand-In processing.
3. Stand-In processing generates an authorization response, based on the issuer's parameters. Stand-In processing also generates authorization advice messages, as appropriate, and stores them in a store-and-forward (SAF) queue.
4. The Mastercard Network routes the Stand-In authorization response to the acquirer.
5. Online acquirers may send an authorization acknowledgement message confirming receipt of the response.
6. When issuer connectivity is re-established, the issuer will retrieve the SAF messages generated by Stand-In processing to adjust cardholder available-to-buy positions appropriately. For the format and contents of a SAF message, refer to the *Customer Interface Specification* manual.

No Secondary Path for Online Customers

If a secondary authorization path does not exist for an issuer or is not allowed based on program or service rules and the online issuer does not respond or responds late to an Authorization Request/0100 message, which causes a time out, the Authorization Platform responds to the acquirer with a decline response.

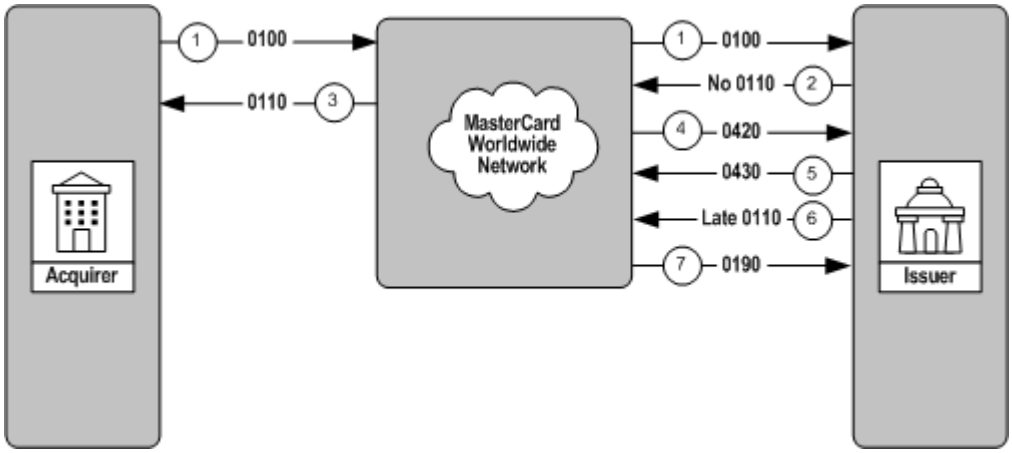
No Secondary Path for Online Customers—No Issuer Response

The transaction follows the flows depicted in the following diagrams.



1. The acquirer sends the Authorization Request/0100 message to the Authorization Platform, and the Authorization Platform forwards the Authorization Request/0100 message to the issuer.
2. The Authorization Platform does not receive the issuer's Authorization Request Response/0110 within the response time allowed for the issuer.
3. The Authorization Platform sends the Authorization Request Response/0110 to the acquirer where DE 39 (Response Code) = 91 (Issuer Authorization System or Issuer Inoperative).
4. The Authorization Platform sends a Reversal Advice/0420 message containing the following values to the issuer because no issuer response is received:
   - DE 39 = 82 (Time out at issuer)
   - DE 60, subfield 1 = 402 (Banknet advice: IPS time-out error)
5. When the issuer receives the Reversal Advice/0420 message, it must generate a Reversal Advice Response/0430 message to acknowledge receipt of the Reversal Advice/0420 message.

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

NOTE: A response is not necessary from the issuer after the Authorization Platform sends an Authorization Response Negative Acknowledgement/0190 message.

Tertiary Path for Online Customers—X-Code Processing

If neither the primary path nor the secondary path is available for the transaction, X-Code processing is performed at the acquirer MIP.

Chapter 4 Acquirer and Issuer Responsibilities

This section discusses acquirer and issuer responsibilities relating to participation in the Mastercard Authorization Platform.

Acquirer Responsibilities

As Mastercard customers, acquirers enter into written agreements with their merchants. These acquirer-merchant agreements must in substance contain certain provisions described in the Mastercard Rules.

NOTE: The acquirer is responsible for making applicable Mastercard rules, regulations, procedures, and policies known to its merchants and is responsible for merchant violations of them.

Acquirers must provide adequate and reasonable authorization services to their merchants, regardless of their location. Acquirers that have entered into an agreement with merchants also have responsibilities regarding the following:

- Processing authorization requests
- Assisting in investigation of counterfeits and criminal cases
- Billing

Processing Authorization Requests

To process authorization requests, acquirers must be able to perform certain tasks.

- Access the Mastercard Network
- Create and send authorization request messages
- Receive the authorization response
- Maintain authorization transaction logs
- Support partial approvals
- Support reversal request messages
- Support account balance responses
- Support incremental preauthorization processing
- Support point-of-sale balance inquiries
- Send authorization completion advices
- Support preauthorization, undefined authorization, and final authorization transactions

Access the Mastercard Network

Acquirers must have access to the Mastercard Network to generate authorization requests and receive authorization responses.

Acquirer options for establishing access to the network are addressed in Basic Authorization Concepts and in the *Data Communications Manual*.

Create and Send Authorization Requests

For all transactions other than On-Us (any transaction in which the acquirer and issuer are the same customer), the acquirer formats and sends an authorization request. Acquirers must forward authorization requests under all conditions identified in the *Transaction Processing Rules* and according to the following specifications.

Acquirers must route all authorization transactions for Account Level Management, Mastercard In Control™ Virtual Card Number (VCN), Mastercard In Control Real Card Spend Control, and Contactless Mapping Service account ranges to the Dual Message System for processing. Account Level Management, Mastercard In Control, and PAN Mapping Service account ranges are identified in the Integrated Product Messages (IPM) Mastercard Parameter Extract (MPE) Table IP0040T1 Issuer Account Range.

Bank Identification Number and Issuing Account Range Management

Acquirers must use consistent Mastercard bank identification number (BIN) and issuing account range maintenance procedures to maintain a positive acceptance experience for cardholders. Consistent BIN and issuing account range maintenance procedures allow merchants to successfully accept and process Mastercard transactions, thereby preventing valid accounts from being declined at the point-of-interaction.

Acquirers can comply with this mandate by ensuring that their merchants submit all authorization requests containing a Mastercard issuing account number either within the 510000–559999 BIN range or within the 222100–272099 BIN range. Alternatively, acquirers can comply with this mandate by maintaining accurate records of all active Mastercard issuing account ranges and ensuring these records are updated on their merchants' systems within six calendar days of Mastercard notification.

To comply with this mandate, acquirers can use one of the following methods:

- Acquirers can use the Mastercard Parameter Extract (MPE) file, specifically Table IP0040T1 Issuer Account Range, to update their merchants. This file is replaced in its entirety with each Global Clearing Management System release (bi-annually) and supplemented by a daily update file that contains add, change, and delete records. In addition, an acquirer can request a full replacement file by contacting the Global Customer Service team.
- Acquirers can use the BIN Table Resource File to update their merchants. The BIN Table Resource File is an optional, daily full file account range replacement file. For information about the BIN Table Resource File transmission and layout, refer to File Layouts.

Acquirers that use the MPE file or the BIN Table Resource File must ensure that the file is deployed on their merchants' systems within six calendar days from the date that Mastercard distributes each updated file.

This mandate applies to authorization processing in dual message (01xx) environments used for Mastercard® and Debit Mastercard® transactions. Mastercard will monitor acceptance compliance. Failure to comply with one of the methods listed above may result in noncompliance assessments as described for Category A of the compliance framework set out in Rule 3.1.2.1, Noncompliance Categories of the *Mastercard Rules*.

Card-Read Data Storage Standards

No card-read data may be displayed, replicated, or stored by any acquirer, merchant, point-of-interaction (POI) terminal or other device, or representative of the acquirer or merchant (including Third Party Processors [TPPs] and Data Storage Entities [DSEs]), except card account number, expiration date, service code, and cardholder name, if present. Refer to the *Mastercard Rules* and the *Security Rules and Procedures* manual for the detailed rules and noncompliance assessments that apply.

Cash Disbursement

The *Transaction Processing Rules* contains specific procedures related to processing cash disbursement.

Electronic Commerce Transactions

Mastercard monitors authorization data originating from electronic commerce (e-commerce) merchants. Acquirers with merchants that fail to identify e-commerce transactions properly are subject to noncompliance assessments.

Mastercard also monitors and identifies merchants and acquirers to verify that they do not resubmit declined Authorization Request/0100 messages with different values in these data elements. Merchants and acquirers should not present Authorization Request/0100 messages using one card acceptor business code (MCC) or with e-commerce transaction identifiers and then, when declined, subsequently resubmit the transaction with different MCCs or with e-commerce transaction identifiers to bypass issuer strategies and obtain issuer approval.

Expired Card

Acquirers should forward, and not decline, any transactions with an expired expiration date. Issuer-approved expired card transactions are not eligible for chargeback if the Authorization Request/0100 message accurately presents the expiration date. For more information about chargeback rights associated with expired cards, refer to the *Chargeback Guide*.

Invalid BIN

Acquirers must forward an authorization request even if the bank identification number (BIN) appears to be invalid. An acquirer may not decline a transaction unless it has received a response of invalid card number from the Authorization Platform.

Mail Order/Telephone Order Batch Authorization Request/0100 Messages

Unless agreed to otherwise by the acquirer and issuer, under no circumstances can an acquirer or its merchant submit batch Authorization Request/0100 messages presorted in BIN order.

Service Provider and Merchant Identification

Acquirers must clearly identify the payment facilitator, sub-merchant, and/or independent sales organization that may be participating in a transaction. This enables accurate acceptance location information, strengthening fraud monitoring and authorization screening, and provides clarity about the transaction to issuers and cardholders.

Acquirers must be prepared to support DE 48 (Additional Data—Private Use), subelement 37 (Additional Merchant Data), subfield 1 (Payment Facilitator ID), subfield 2 (Independent Sales Organization ID), and subfield 3 (Sub-Merchant ID) whenever a payment facilitator or independent sales organization participates in a transaction.

Acquirers must be prepared to support the following authorization and financial transaction messages that may contain a combination of DE 48, subelement 37, subfields 1, 2, and 3 when applicable:

- Authorization Request/0100
- Authorization Advice/0120—Acquirer-generated
- Authorization Advice/0120—System-generated
- Financial Transaction Request/0200
- Financial Transaction Advice/0220

The field descriptions for the following DE 43 (Card Acceptor Name/Location for all transactions) and DE 61 (Point-of-Service [POS] Data) subfields include the payment facilitator and the sub-merchant location information:

- DE 43 (Card Acceptor Name/Location), subfield 1 (Card Acceptor Name)
- DE 43, subfield 3 (Card Acceptor City)
- DE 43, subfield 5 (Card Acceptor State, Province, or Region Code)
- DE 61, subfield 13 (POS Country Code [or Sub-Merchant Information, if applicable])
- DE 61, subfield 14 (POS Postal Code [or Sub-Merchant Information, if applicable])

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 three, seven, or 12 characters in length, followed by an asterisk and the sub-merchant name. DE 43, subfields 3 and 5 and DE 61, subfields 13 and 14 must contain the location information of the sub-merchant, not the payment facilitator.

For details about data requirements, refer to the *Customer Interface Specification* manual.

Support Preauthorization, Undefined Authorization, and Final Authorization Transactions

Acquirers in the Asia/Pacific, Canada, Latin America and Caribbean, and the United States regions must be able to support properly coding authorization requests as preauthorization, undefined authorization, and final authorization transactions.

Acquirers in the Europe and Middle East/Africa regions must be able to support properly coding authorization requests as preauthorization and final authorization transactions.

Acquirers in the Europe region must ensure that any authorization request for an amount greater than zero must be properly coded as either preauthorization or final authorization according to message coding requirements.

Acquirers must submit the clearing presentment for an approved final authorization or undefined authorization transaction within seven calendar days of the authorization date. Acquirers must submit the clearing presentment for an approved preauthorization transaction within 30 calendar days of the latest preauthorization date.

Voice Authorization Requests

Acquirers that initiate an authorization request based on a phone call from the merchant must verify the account number with the merchant to ensure that it was correctly relayed before declining an authorization.

Receive the Authorization Response

When the acquirer receives the authorization response, the acquirer passes the response on to the merchant.

The acquirer bears responsibility for application of the response. If, in response to an authorization request, the acquirer is instructed to obtain or to hold on to a card or is given other instructions, the acquirer must inform the merchant that it shall use its best efforts, by reasonable and peaceful means, to comply with such instructions.

For the authorization responses that acquirers may receive, refer to Basic Authorization Concepts.

Call Referral Responses

Acquirers have the following additional responsibilities regarding call referral responses.

- Establish a merchant call referral response rate of 60 percent.
- Monitor individual merchant performance.
- Encourage, where possible or appropriate, three-way communication to allow merchants, cardholders, and issuers to exchange information during a call referral response call.
- Develop and distribute educational materials for merchants.
- Apply all call referral standards to the rules governing Member Service Providers (MSPs). The *Mastercard Rules* describes MSP responsibilities.

Minimum Authorization Response Wait Time

For Mastercard and Debit Mastercard POS transactions, there are minimum authorization response wait times.

For Mastercard and Debit Mastercard POS transactions, when sending an Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or Reversal Request/0400 message, acquirers in Brazil, the Canada region, Netherlands, U.K., and the U.S. region must wait at least 10 seconds for the authorization response.

For Mastercard and Debit Mastercard POS transactions, when sending an Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or Reversal Request/0400 message, acquirers in all other countries must wait at least 12 seconds for the authorization response.

The acquirer must ensure that its host does not apply authorization response wait time parameters that time out before the minimum authorization response wait time has elapsed.

Maintain Authorization Logs

Acquirers that process authorizations must maintain, for at least 120 days, a record or log of all authorization transactions. The log must include all data files pertinent to each request and corresponding authorization response.

If an authorization transaction occurred at an electronic terminal, the acquirer must maintain a log containing the following information:

- Authorization code given by the issuer or the transaction certificate (TC) given by the EMV chip card
- Substitute number generated by the acquirer and printed on the terminal receipt, if not the same as the authorization code
- Number of days allowed for a presentment, in the case of a delayed delivery because of a partial payment
- Indication that the merchant reported that the card may be stolen or counterfeit or that the transaction caused the merchant to be suspicious, if this situation occurred

Support Partial Approvals

Acquirers must be able to support partial approvals.

As indicated in Table 1: Acquirer Mandate to Support Partial Approvals, Reversal Requests, and Account Balance Responses (U.S. and Canada Region Only), Mastercard mandates that acquirers providing authorization services for U.S. and Canada region merchants in the MCCs listed, and merchants in the MCCs listed, must support partial approvals for all Debit Mastercard® account ranges they acquire, including all prepaid Debit Mastercard accounts. This requirement applies only to card present transactions occurring at attended terminals and at cardholder-activated terminals (CATs) identified with MCC 5542 (Fuel Dispenser, Automated).

Effective 2020 with Release 20.Q2, an acquirer of a merchant included in any of the MCCs listed in Table 2: Effective Dates for Acquirer Mandate to Support Partial Approvals and Account Balance Responses Globally, for card present transactions conducted at attended terminals only) or MCC 5542 must support partial approvals for all Debit Mastercard, Maestro, and prepaid Mastercard card account ranges. Acquirers in the United Kingdom must support this mandate in their host systems. Mastercard reserves the right to expand the number of markets that may be required to support prior to 2020.

Support Reversal Request Messages

Acquirers must be able to support reversal request messages.

As indicated in Table 1: Acquirer Mandate to Support Partial Approvals, Reversal Requests, and Account Balance Responses (U.S. Region Only), Mastercard mandates that acquirers providing authorization services for U.S. region merchants in the MCCs listed must support full and partial reversals for all Mastercard® and Debit Mastercard® account ranges they acquire, including all prepaid Debit Mastercard accounts (with certain MCCs initially exempted).

For more information about reversal request messages, refer to Online Authorization Messages.

Support Account Balance Responses

Acquirers must support account balance responses.

U.S. Region

As indicated in Table 1: Acquirer Mandate to Support Partial Approvals, Reversal Requests, and Account Balance Responses (U.S. Region Only), Mastercard mandates that acquirers providing authorization services for U.S. region merchants in the MCCs listed must support account balance response for transactions initiated at point-of-sale (POS) terminals for all prepaid Debit Mastercard accounts they acquire. This requirement applies only to card present transactions occurring at attended terminals.

Effective in 2020 with Release 20.Q2, the acquirer of a merchant included in any of the MCCs listed in Table 2: Effective Dates for Acquirer Mandate to Support Partial Approvals and Account Balance Responses Globally (for card present transactions conducted at attended terminals only) must support account balance responses for all prepaid card account ranges (Mastercard, Debit Mastercard, and Maestro). This mandate does not apply to acquirers in the United Kingdom. Mastercard reserves the right to expand the number of markets that may be required to support prior to 2020.

Canada Region

As indicated in Table 3: Acquirer Mandate to Support Partial Approvals, Reversal Requests, and Account Balance Responses (Canada Region Only), Mastercard mandates that acquirers providing authorization services for Canada region merchants in the MCCs listed except MCC 5542 (Automated Fuel Dispenser) must support account balance response for transactions initiated at point-of-sale (POS) terminals for all prepaid Debit Mastercard accounts they acquire. This requirement applies only to card present transactions occurring at attended terminals.

Support Incremental Preauthorization Processing

Acquirers processing incremental preauthorization transactions on the Dual Message System are required to use DE 48 (Additional Data—Private Use), subelement 63 (Trace ID) in Authorization Request/0100 and Authorization Advice/0120—Acquirer-generated messages.

For more information about incremental preauthorization transactions, refer to Incremental Preauthorization Standards.

Support Point-of-Sale Balance Inquiries

U.S. region acquirers must support point-of-sale (POS) balance inquiry transactions for all prepaid Debit Mastercard and prepaid Maestro card accounts.

Support Surcharge Amount

Acquirers that acquire transactions for merchants that are permitted to assess a surcharge must be able to send the surcharge amount in DE 28 (Transaction Fee Amount) in Authorization Request/0100 and Authorization Advice/0120 messages.

NOTE: Acquirers must comply with local rules and regulations when applying the surcharge. Acquirers must disclose the fee to the cardholder and ensure that the cardholder agrees to the fee before the transaction can occur.

Send Authorization Completion Advices

Acquirers must be able to send authorization completion advices.

Acquirers of automated fuel dispenser (AFD) merchants located in the U.S. and Canada regions must 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 no more than 60 minutes after the issuer approved its original Authorization Request/0100 message.

Acquirers in the Europe region are required to send Authorization Advice/0120—Acquirer-generated messages containing DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code), value 191 (Acquirer Processing System [APS] Completed Authorization Transaction) no more than 20 minutes after the completion of Maestro CAT Level 1 petrol transactions.

For incomplete AFD transactions, acquirers in the Europe region have the option to send a zero value in DE 4 (Amount, Transaction), along with value 191 (Acquirer Processing System (APS) Completed Authorization Transaction) in DE 60 (Advice Reason Code) in Authorization Advice/0120—Acquirer-generated messages, which serves as a notification to the issuer to

remove any unnecessary holds to the cardholder's open-to-buy balance. Acquirers outside the Europe region should submit a Reversal Request/0400 message to reverse an incomplete AFD transaction.

Table 1: Acquirer Mandate to Support Partial Approvals, Reversal Requests, and Account Balance Responses (U.S. Region Only)

The MCCs listed in the following table should now support the acquirer mandate requirements for partial approvals, full and partial reversals, and account balance responses in the U.S. region.

MCC	Description
4111	Transportation—Suburban and Local Commuter Passenger, including Ferries
4812	Telecommunication Equipment including Telephone Sales
4814	Telecommunication Services
4816	Computer Network/Information Services
4899	Cable, Satellite, and Other Pay Television and Radio Services
5111	Stationery, Office Supplies
5200	Home Supply Warehouse Stores
5300	Wholesale Clubs
5310	Discount Stores
5311	Department Stores
5331	Variety Stores
5399	Miscellaneous General Merchandise Stores
5411	Grocery Stores, Supermarkets
5499	Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores
5541	Service Stations (with or without Ancillary Services)
5542	Fuel Dispenser, Automated
5732	Electronic Sales
5734	Computer Software Stores
5735	Record Shops
5812	Eating Places, Restaurants
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies

MCC	Description
5921	Package Stores, Beer, Wine, and Liquor
5941	Sporting Goods Stores
5942	Book Stores
5943	Office, School Supply and Stationery Stores
5999	Miscellaneous and Specialty Retail Stores
7829	Motion Picture-Video Tape Production-Distribution
7832	Motion Picture Theaters
7841	Video Entertainment Rental Stores
7996	Amusement Parks, Carnivals, Circuses, Fortune Tellers
7997	Clubs—Country Membership
8011	Doctors—not elsewhere classified
8021	Dentists, Orthodontists
8041	Chiropractors
8042	Optometrists, Ophthalmologists
8043	Opticians, Optical Goods, and Eyeglasses
8062	Hospitals
8099	Health Practitioners, Medical Services—not elsewhere classified
7999	Recreation services—not elsewhere classified
8999	Professional Services—not elsewhere classified
9399	Government Services—not elsewhere classified

Acquirers of merchants in the MCCs listed in this table should now support these requirements across their terminal base. For merchants with newly deployed stand-alone terminals, this software should be the standard. Upgrades to existing stand-alone terminals are required to support at this time. For the purposes of this section, stand-alone terminals are terminals that are not integrated into a merchant's POS system, such that the transaction amount must be manually entered into the terminal.

Table 2: Effective Dates for Acquirer Mandate to Support Partial Approvals and Account Balance Responses Globally

Effective dates by MCC for the acquirer mandate to support partial approvals and account balance responses in all regions outside the U.S. and Canada are listed in table format. Mastercard reserves the right to expand the number of markets that may be required to support prior to 2020.

Effective Date	MCC	Description
2020 (Release 20.Q2)	5310	Discount Stores
	5311	Department Stores
	5411	Grocery Stores, Supermarkets
	5541	Service Stations (with or without Ancillary Services)
	5542	Automated Fuel Dispenser (partial approval support only)
	5621	Women's Ready to Wear Stores
	5691	Men's and Women's Clothing Stores
	5732	Electronic Sales
	5812	Eating Places, Restaurants
	5814	Fast Food Restaurants
	5912	Drug Stores, Pharmacies
	5999	Miscellaneous and Specialty Retail Stores

Table 3: Acquirer Mandate to Support Partial Approvals, Reversal Requests, and Account Balance Responses (Canada Region Only)

The MCCs listed in the following table should now support the acquirer mandate requirements for partial approvals, full and partial reversals, and account balance responses in the Canada region.

MCC	Description
4812	Telecommunication Equipment including Telephone Sales
4814	Telecommunication Services including but not limited to prepaid phone services and recurring phone services
4816	Computer Network/Information Services
5200	Home Supply Warehouse Stores
5310	Discount Stores
5311	Department Stores
5331	Variety Stores
5411	Grocery Stores, Supermarkets
5499	Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores

MCC	Description
5541	Service Stations (with or without Ancillary Services)
5542	Fuel Dispenser, Automated
5621	Women's Ready To Wear Stores
5631	Women's Accessory And Specialty Stores
5641	Children's And Infant's Wear Stores
5651	Family Clothing Stores
5661	Shoe Stores
5691	Men's And Women's Clothing Stores
5732	Electronic Sales
5734	Computer Software Stores
5735	Record Shops
5812	Eating Places, Restaurants
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5921	Package Stores, Beer, Wine, and Liquor
5941	Sporting Goods Stores
5942	Book Stores
5945	Game, Toy, and Hobby Shops
5947	Gift, Card, Novelty, and Souvenir Shops
5977	Cosmetic Stores
5999	Miscellaneous and Specialty Retail Stores
7399	Business Services—not elsewhere classified
8999	Professional Services—not elsewhere classified
9399	Government Services—not elsewhere classified

Acquirers of merchants in the MCCs listed in this table should now support these requirements across their terminal base. For merchants with newly deployed stand-alone terminals, this software should be the standard. Upgrades to existing stand-alone terminals are required to support at this time. For the purposes of this section, stand-alone terminals are terminals that are not integrated into a merchant's POS system, such that the transaction amount must be manually entered into the terminal.

Assisting in Investigation of Counterfeits and Criminal Cases

Refer to the *Security Rules and Procedures* manual for information about a customer's responsibility to provide assistance as necessary to Mastercard and other customers that are performing investigations.

Billing

All authorization processing activities are billed through the Mastercard Consolidated Billing System (MCBS). Charges and credits to the acquirer are listed as billing events, and include the following categories of authorization activity:

- Use of the network (acquirer access fees)
- Use of value-added services
- Call referrals (calls to the issuer)
  - The acquirer receives a credit for responding to call referrals within established time frames. This applies only if the acquirer uses the Global Automated Referral Service (GARS).
  - The acquirer may request a credit for call referral responses that did not use GARS. The credit covers the costs of contacting the issuer. The acquirer requests the credit via a Fee Collection/1740 message.

For a description of these value-added services and information about GARS, refer to Authorization Services Details. For a complete description of billing events for authorization services, refer to the *Mastercard Consolidated Billing System* manual.

Issuer Responsibilities

Issuers have responsibilities regarding aspects of participation in the Mastercard Authorization Platform.

Issuers are responsible for:

- Encoding and validating the card validation code 1 (CVC 1) value
- Encoding and validating the Chip CVC
- Imprinting and validating the card validation code 2 (CVC 2) value
- Personalizing and validating the card validation code 3 (CVC 3) value
- Generating and validating Accountholder Authentication Value (AAV)
- Issuing and validating personal identification number (PIN) data
- Validating the authorization request cryptogram (ARQC) and generating the authorization response cryptogram (ARPC)
- Processing authorization requests
- Supporting point-of-sale balance inquiries (U.S. region prepaid card issuers only)
- Call referral responses
- File maintenance
- Billing

Encoding and Validating the CVC 1 Value

Issuers must encode the magnetic stripe on all cards with the CVC 1 value.

Online issuers also must validate the CVC 1 value when they receive the Authorization Request/0100 message if the Authorization Request/0100 message contains value 80 or 90 in subfield 1 of the Point-of-Service (POS) Entry Mode field.

Issuers must indicate a CVC 1 validation failure by placing a value of Y in subelement 87 of the Additional Data field in the Authorization Request Response/0110 message.

For information about the placement of the CVC 1 value within the magnetic stripe, refer to Authorization Services Details.

Encoding and Validating the Chip CVC

Full chip issuers must ensure that the CVC stored on the chip (the Chip CVC) in the Track 2 Equivalent Data (tag 57) has a different value than stored on the card's magnetic stripe (the CVC 1).

For chip transactions (DE 22 [Point-of-Service (POS) Entry Mode], subfield 1 [POS Terminal PAN Entry Mode] = value 05 [PAN auto-entry via chip]), full chip issuers validate the chip cryptogram included in DE 55 (Integrated Circuit Card (ICC) System-related Data), instead of the CVC included in DE 35 (Track 2 Data). If that chip transaction does not include DE 55 ICC system-related data, issuers validate the CVC included in DE 35.

Magnetic stripe grade issuers and issuers using the Chip to Magnetic Stripe Conversion service that want to leave their host systems completely unchanged may use the same CVC in the chip and on the magnetic stripe.

Magnetic stripe grade issuers and issuers that want to leave their host systems completely unchanged may use the same CVC in the chip and on the magnetic stripe.

For more information on the Chip CVC and related requirements, refer to the *M/Chip Requirements* document and the *Security Rules and Procedures* manual.

Imprinting and Validating the CVC 2 Value

Issuers must imprint the CVC 2 value on the signature panel of the card.

For information about the verification process performed by the issuer, refer to Authorization Services Details.

Personalizing and Validating the CVC 3 Value

All contactless cards and devices must be personalized to support the generation of a dynamic CVC 3 value when performing a contactless magnetic stripe profile transaction. For contactless transactions containing a CVC 3 value, issuers must verify the CVC 3 value when processing the authorization received from a contactless transaction or use one of the Mastercard contactless CVC 3 Pre-validation services.

Issuers must verify the CVC 3 value when processing the authorization received from a contactless transaction.

If there is an issue with the CVC 3, issuers may optionally provide DE 48 (Additional Data—Private Use), subelement 87 (Card Validation Code Result) containing value E (Length of unpredictable number was not a valid length), value P (Unable to process), or value Y (Invalid) in their Authorization Request Response/0110 messages.

Generating and Validating Accountholder Authentication Value

Issuers are required to establish a secure operational facility for performing cardholder authentication processing and Accountholder Authentication Value (AAV) generation for e-commerce transactions under requirements of the Mastercard® program. All AAVs must be generated using the Mastercard Secure Payment Application (SPA) algorithm.

With the EMV® 3-D Secure protocol and the Mastercard Identity Check program, Mastercard has created a new SPA algorithm called SPA2. For more information about this new algorithm, refer to the *SPA2 AAV for the Mastercard Identity Check Program* manual on Mastercard Connect™.

All facilities must adhere to Mastercard security requirements regarding operations of cardholder authentication processing platforms. For more information, refer to the *Identity Check ACS Security Requirements*.

Mastercard requires that issuers validate the SPA AAV in real time before generating the authorization response; Mastercard has implemented this requirement to raise the minimum security standards for electronic commerce (e-commerce) transactions and align with the European Union's PSD2 requirements for dynamic linking. In support of this activity, Mastercard has made available an on-behalf-of SPA AAV validation service that is invoked as transactions flow through the authorization network and can be configured to perform validation on all transactions or only during Stand-In processing.

Mastercard will updgrade its on-behalf-of SPA AAV service with SPA2 AAV to support the dynamic linking requirement; this will become the minimum service standard for Mastercard's on-behalf-of SPA AAV validation service through which the following data will be verified in combination:

- PAN
- SPA2 AAV
- Directory Server (DS) transaction ID
- Amount

Issuers have the option to perform AAV self-validation, which must be coordinated with their ACS Service.

At a minimum, issuers are required to maintain the SPA AAV and all information required to perform the validation for the requisite transaction in the event of a customer chargeback or other dispute involving the transaction. Mastercard recommends a storage period of at least 180 days.

Issuing and Validating PIN Data

Issuers must be able to receive and process Mastercard authorizations that contain a PIN.

For more information about preparing issuers' systems to receive and to process PIN authorization requests, refer to Authorization Services Details and for information about PIN translation processing capabilities for Europe region customers, refer to PIN Processing for Europe Region Customers.

Validating the ARQC and Generating the ARPC

Issuers must validate the Authorization Request Cryptogram (ARQC) that the EMV chip card generates to indicate that the transaction must go online to the issuer for authorization.

Issuers also must generate the Authorization Response Cryptogram (ARPC), which contains the decision to approve or decline the online authorization request (used for non–face-to-face EMV chip card transactions completed from cardholder-controlled remote devices).

For more information about M/Chip Processing services that can validate the ARQC and generate the ARPC on behalf of an issuer, refer to Authorization Services Details.

Processing Authorization Requests

Issuers receive authorization requests from acquirers and provide authorization responses directing acquirers about how to handle the transactions. Each issuer is responsible for the provision of authorization service 24 hours a day, every day of the year at its own expense.

In addition, each issuer participating in the Mastercard Authorization Platform or any local or regional message switching service with other customers must have adequate back-up procedures and personnel. The issuer must be able to process incoming and outgoing interchange authorizations if the customer's connection with the Mastercard Authorization Platform or the local or regional service becomes inoperable for any reason. Each issuer also is responsible for the authorizations that it or its agent generates, including gratuities included in the total transaction amount and any transaction resulting from a variance granted by Mastercard pursuant to the *Mastercard Rules*.

To provide authorization responses, most issuers access the Mastercard Authorization Platform online, through connectivity between the issuer host and a MIP.

To process authorization requests, issuers must be able to perform the following.

- Establish Stand-In processing authorization parameters
- Maintain an authorization log
- Support AVS requests for U.S. and Canada issuers
- Support partial approvals
- Support reversal request messages
- Support account balance responses
- Support authorization advice completion messages
- Support incremental preauthorizations
- Support identification of preauthorizations, undefined authorizations, and final authorizations

[1] Issuers may optionally adapt the way they process authorizations to take advantage of the new information received with each authorization to identify it as a preauthorization, undefined authorization, or final authorization.

Establish Stand-In Processing Authorization Parameters

All issuers must complete the *Stand-In Processing Worksheet* (Form 041) to establish parameters for Stand-In authorization processing.

For more information about Stand-In processing and completing the Stand-In Processing Worksheet, refer to Stand-In Processing and Setting Stand-In Parameters.

NOTE: Stand-In System processing is mandatory for Mastercard credit products in all regions. Issuers may choose to block Stand-In System processing for debit products in all regions, except in the U.S. region.

Maintain an Authorization Log

Issuers must maintain written records, logs, or computer records of all authorizations granted showing the date of issue for at least 120 days.

Support AVS Requests

Mastercard requires all acquiring and issuing processors to code for, support, and integrate into their systems the data elements, subelements, and values associated with Address Verification Service (AVS).

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

For additional information about this requirement, refer to the Global Safety and Security Standards Roadmap.

NOTE: Mastercard does not require acquirers or issuers to enroll in these optional products and services, unless Participation Requirements state otherwise. Acquirers and issuers 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.

Support Partial Approvals

Mastercard mandates that all issuers in the U.S. region must support partial approvals for all Debit Mastercard account ranges they issue, including all prepaid Debit Mastercard accounts. Issuers can test their abilities to transmit partial approval messages.

Effective in 2020 with Release 20.Q2, issuers globally must support partial approvals for Debit Mastercard, Maestro, and prepaid Mastercard card account ranges. Issuers in the United Kingdom are required to support partial approvals by 2014 (Release 14.Q2) for all Debit Mastercard, Maestro and Prepaid Mastercard card account ranges. Issuers in the Canada region are required to support partial approvals by 2015 (Release 15.Q2) for all Debit

Mastercard and Prepaid Mastercard card account ranges. Mastercard reserves the right to expand the number of markets that may be required to support prior to 2020.

For more information about partial approvals, refer to Authorization Services Details.

Support Reversal Request Messages

Mastercard mandates that all issuers in the U.S. region must support both full and partial reversals for all Mastercard® and Debit Mastercard account ranges they issue, including all prepaid Debit Mastercard accounts (with certain MCCs initially exempted). Issuers can test their abilities to process reversal request messages.

For all Mastercard and Debit Mastercard account ranges including prepaid, a U.S. region issuer receiving a Reversal Request/0400 message or Reversal Advice/0420 message must release any hold placed on the cardholder's account for the amount specified within 60 minutes of matching the reversal message to a previous authorization request message.

For more information about reversal request messages, refer to Online Authorization Messages.

Support Account Balance Responses

Mastercard mandates that all issuers in the U.S. region must support account balance response for transactions initiated at point-of-sale (POS) terminals for all Debit Mastercard prepaid account ranges they issue (excluding when the prepaid product is flex benefits, government, and payroll). Mastercard mandates that all issuers in the Canada region must support account balance response for all prepaid Mastercard accounts.

Issuers can test their abilities to transmit available balances in the appropriate fields of response messages.

Effective in 2020 with Release 20.Q2, issuers must support account balance response for prepaid card account ranges (Mastercard, Debit Mastercard, and Maestro). This mandate does not apply to issuers in the United Kingdom. Mastercard reserves the right to expand the number of markets that may be required to support prior to 2020.

For information about account balance responses, refer to Authorization Services Details.

Support Authorization Advice Completion Messages

Mastercard and Debit Mastercard issuers in the U.S. and Canada regions must release any excess hold amount placed on the cardholder's open-to-buy (OTB), if any, no more than 60 minutes after receiving the Authorization Advice/0120 completion message for an automated fuel dispenser transaction.

Issuers globally must receive a zero value in DE 4 (Amount, Transaction) in the Authorization Advice/0120 messages for incomplete AFD transactions acquired in the Europe region. Mastercard recommends that issuers identify zero amount AFD transactions from merchants in the Europe region using DE 61 (Point-of-Service [POS] Data), subfield 13 (POS Country Code [or Sub-Merchant Information, if applicable]), when populated by the acquirer. Issuers will receive a Reversal Request/0400 message to reverse an incomplete AFD transaction from acquirers outside the Europe region.

Support Incremental Preauthorizations

Issuers processing incremental preauthorization transactions through the Dual Message System must support DE 48 (Additional Data—Private Use), subelement 63 (Trace ID) in Authorization Request/0100 messages.

Issuers will match all preauthorizations resulting from one event to a single clearing record:

- Upon receipt of the transaction clearing record, the issuer must use the unique identifier provided by the acquirer in the clearing record to match the original preauthorization and any additional approved preauthorizations to the transaction.
- Upon matching all preauthorizations to the clearing record, the issuer must release any hold placed on the cardholder's account in connection with the original preauthorization and any additional approved preauthorizations that are in excess of the transaction amount.

Issuers are expected to support and recognize DE 48, subelement 63 or recognize incremental preauthorizations.

For more information about incremental preauthorization transactions, refer to Incremental Preauthorization Standards.

Support Account Status Inquiry Service Responses

Issuers must respond to Account Status Inquiry Service requests with an applicable response in DE 39 (Response Code) of the Authorization Request Response/0110 message.

Issuers must be able to receive and to process the CVC 2 value when present in DE 48, subelement 92 of the Authorization Request/0100 message, and to provide a valid CVC 2 response in DE 48, subelement 87 of the Authorization Request Response/0110 message as specified in Card Validation Code 2 Verification. If presented, issuers in the U.S. region must validate the cardholder address. Issuers should not place cardholder funds on hold when receiving a request under this service.

For information about Account Status Inquiry Service responses, refer to Account Status Inquiry Service.

Support Identification of Final Authorizations

Issuers globally must be able to clearly distinguish a final authorization for authorizations originated by card acceptors/acquirers.

Issuers must recognize values 0 (Normal Authorization/Undefined Finality) and 1 (Final Authorization) in DE 48 (Additional Data—Private Use), subelement 61 (POS Data Extended Condition Codes), subfield 5 (Final Authorization Indicator) to distinguish a final authorization from a preauthorization or undefined authorization in Authorization Request/0100 and Authorization Advice/0120 messages.

Issuers must release any hold that they may have placed on the cardholder's account after expiry of the payment guarantee period for the particular authorization, at the latest. The payment guarantee period is seven days for final and undefined authorizations.

Support Surcharge Amount

Issuers must be able to receive surcharge amounts in DE 28 in Authorization Advice/0120 messages and return the surcharge amount in Authorization Advice Response/0130 messages.

Supporting Point-of-Sale Balance Inquiries

U.S. region issuers must support point-of-sale (POS) balance inquiries for prepaid Debit Mastercard and prepaid Maestro card accounts.

Call Referral Responses

Issuers have certain responsibilities regarding call referral responses.

- Be available to respond to all call referrals at the time of issuance.
- Process an Authorization Advice/0120 message that informs the issuer that Stand-In Processing responded to the Authorization Request/0100 message that prompted a call referral response.
- Not issue call referrals to merchant categories that represent unattended point-of-interaction (POI) transactions including:
  - Automated teller machines (MCC 6011)
  - Cardholder-activated terminals (CAT) (including MCC 5542)
- Not issue call referrals under any circumstances to the following merchant categories:
  - Fast food (quick service) restaurants (MCC 5814)
  - Mail order and direct marketing (MCCs 5960–5969)
- Apply all call referral standards to Member Service Providers (MSPs). The *Mastercard Rules* describes MSPs.
- Not use call referrals as a primary method for activating new or reissued cards to minimize the impact on cardholders and merchants at the point-of-interaction.
- Adhere to the following minimum standards for all call referrals, domestic and international, whether processed through Global Automated Referral Service (GARS) or direct customer-to-customer communications. The standards apply to the amount of time the issuer has to respond to incoming referral calls from acquirers and to the average monthly duration of each referral call:
  - On an incoming phone call (voice or GARS) from an acquirer, the issuer must answer the call within 30 seconds. Then the issuer must retrieve the call from its queue and initiate discussion with the acquirer within the next 30 seconds. The issuer also must limit the duration of each call to five minutes, measured as a monthly average.

Issuers that use card activation programs are encouraged to:

- Place stickers on the front of new cards and send them with mailing inserts instructing cardholders to activate their accounts.
- Call cardholders who have not activated their accounts one week after cards are mailed.
- Respond to an authorization request on an inactivated card with a call referral.

All phone calls processed through GARS that are not answered by the issuer within the required time frames are routed to the Mastercard Stand-In System for processing. Mastercard uses the issuer-defined Stand-In parameters to complete the transaction.

Charges to the issuer apply for the following:

- Completed GARS calls initiated by the acquirer
- Noncompliance assessment for Stand-In processing if the issuer fails to answer a GARS call within 30 seconds
- Reimbursement to the acquirer for call referral responses that did not use GARS (requested in the Fee Collection/1740 message)

Contact the Global Customer Service team for any of the following:

- Questions or problems concerning GARS
- Billing inquiries
- Requests for a Stand-In Processing Worksheet to update Stand-In processing parameters or phone numbers

NOTE: Mastercard discontinued support of telex call referrals. Customers that previously used telex services must register to use GARS. For more information about GARS, refer to Global Automated Referral Services.

File Maintenance

Issuers maintain the account listings of restricted, negative, and positive cards used by Stand-In processing for online customers.

Issuers can list accounts in the following files:

- Premium Listings
- Stand-In Account File, Electronic Warning Bulletin, or Local Stoplist

Issuers also maintain account listings if they participate in Payment Cancellation, Contactless Mapping Service, Dynamic CVC 3 Validation Services for the Contactless Application Transaction Counter (ATC), Enhanced Value, or Product Graduation services.

For more information about these files, including how to access the files, record formats, and detailed instructions for performing file maintenance, refer to the *Account Management System User Manual*.

Billing

All authorization processing activities are billed through the Mastercard Consolidated Billing System (MCBS).

Charges to the issuer include the following categories of authorization activity:

- Use of the Mastercard Network (issuer access fees)
- Use of value-added services
- Call referrals (charge to the issuer for issuing call referral responses and for receiving response calls from acquirers)

For a complete description of billing events for authorization services, refer to the *Mastercard Consolidated Billing System* manual.

Chapter 5 Online Authorization Messages

The authorization messages that online issuers and acquirers use to process authorizations are described in this section.

Message Types

The message types supported by the Authorization Platform are listed in table format. Check marks (√) indicate who initiates the message.

Online issuers and acquirers should use this information in conjunction with the *Customer Interface Specification* manual. For debit transactions (02xx messages), refer to the *Single Message System Specifications* manual.

Message Category		Message Initiator		
		Mastercard	**Issuer**	**Acquirer**
Authorization/01xx Messages				
0100	Authorization Request			√
0110	Authorization Request Response	√	√	
0120	Authorization Advice	√	√	√
0130	Authorization Advice Response	√	√	
0180	Authorization Acknowledgement			√ (optional for acquirers)
0190	Authorization Response Negative Acknowledgement	√		
Issuer File Update/03xx Messages				
0302	Issuer File Update Request		√	
0312	Issuer File Update Request Response	√		
Reversal/04xx Messages				
0400	Reversal Request			√
0410	Reversal Request Response	√	√	
0420	Reversal Advice	√		
0430	Reversal Advice Response		√	
Administrative/06xx Messages				

	Message Category	Message Initiator		
0600	Administrative Request			√
0610	Administrative Request Response		√	
0620	Administrative Advice	√	√	√
0630	Administrative Advice Response	√	√	√
Network Management/08xx Messages				
0800	Network Management Request	√	√	√
0810	Network Management Request Response	√	√	√
0820	Network Management Advice	√		

Authorization Data Accuracy Initiative Mandate

Accurate information in the authorization message is critical in evaluating the risk of fraud associated with a transaction. Investigation of the present quality of the data and customer feedback has indicated that improving the quality of data in specific authorization and clearing messages will help improve fraud prediction, prevention, detection, and research.

All acquirers processing transactions must provide accurate information in DE 7 (Transmission Date and Time), DE 41 (Card Acceptor Terminal ID), and DE 61 (Point-of-Service [POS] Data), subfield 14 (POS Postal Code [or Sub-Merchant Information, if applicable]).

Monitoring Approach

The Mastercard Data Integrity Monitoring Program will be used to monitor compliance to the Standards. Compliance level requirements within the Data Integrity program range from 0 to 98 percent depending on the acquirer volumes.

Compliance mandates for the Authorization Platform are as follows:

- 14 October 2011—Monitoring and customer reporting of DE 7, DE 41, and DE 61, subfield 14 begins
- 12 October 2012—Mastercard will begin enforcement of DE 7 and DE 61, subfield 14
- 19 April 2013—Mastercard will begin enforcement of DE 41

The monitoring period is longer than past edits introduced in the Data Integrity Program to provide customers with the needed time to modify their systems and procedures.

DE 7—Transmission Date and Time

DE 7 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). Each message initiator must assign a value in DE 7 to the originating request message.

The transmission date and time provided in DE 7 must be within three minutes of the UTC recorded by the Mastercard Network.

DE 41—Card Acceptor Terminal ID

Mastercard requires the presence of DE 41 with all card-read transactions at card acceptor locations with multiple POS devices.

DE 61—Point-of-Service (POS) Data, Subfield 14 (POS Postal Code [or Sub-Merchant Information, if applicable])

To validate the postal code in the authorization message, Mastercard will compare it to the postal code in the related clearing record. The content, format, and presentation of the postal code must match between DE 61, subfield 14 in the authorization message and DE 43 (Card Acceptor Name/Location), subfield 4 (Card Acceptor postal [ZIP] Code) in the clearing message.

Mastercard will begin enforcing compliance with this requirement beginning 12 October 2012. Exemptions from this validation are transactions at merchants in countries or provinces that do not have postal codes, and card-not-present transactions.

For More Information

- For more information about the Standards used for compliance, refer to the *Data Integrity Monitoring Program* manual.
- For details about data requirements, refer to the *Customer Interface Specification* manual.

Using Authorization Messages

For information about exception processing, refer to the *Customer Interface Specification* manual.

Authorization messages are not intended for posting to the cardholder's account for billing purposes. Customers should delay posting to the cardholder's account until clearing and settlement are complete. For detailed information about clearing and settlement, refer to the *GCMS Reference Manual* and the *Settlement Manual*.

Routing Timer Values

Routing timer values that apply to acquirer-generated Authorization Request/0100, Authorization Advice/0120, and Reversal Request/0400 messages are listed in table format. All Network Management/08xx, Issuer File Update/03xx, Administrative/06xx, and system-

generated Authorization Advice messages remain unchanged and retain their current timer attributes.

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*	3	12*
Mastercard—POS PIN for Credit**	18	6	24
Mastercard—ATM	12	6	18
Debit Mastercard—POS	Same as Mastercard Credit—POS		
Maestro—All	18***	6	24
Cirrus—ATM	18	6	24
Private Label—POS	12	6	18
AMEX—POS	12	6	18
Visa—POS	12	6	18

***** For Mastercard and Debit Mastercard POS 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.

****** 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.

******* 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 Bulletins*.

Processing Authorization Transactions

Issuers receive authorization-related messages from acquirers for transactions for their cardholders. They must respond to these messages with response messages. Issuers that use on-behalf services also receive messages from Mastercard.

Authorization Request/0100 and Authorization Request Response/0110 Messages

When issuers receive Authorization Request/0100 messages, they must decide whether to approve or decline a transaction. Issuers may use a variety of checks using the data contained in the request and the spending limits in the cardholder's activity file. After issuers perform the validation checks appropriate for the transaction, they send back an Authorization Request Response/0110 message.

Authorization Request/0100 and Authorization Request Response/0110 Flow

The following diagram illustrates 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.

Authorization Advice/0120 and Authorization Advice Response/0130 Messages

The Authorization Advice/0120 and Authorization Advice Response/0130 message process are illustrated by diagrams.

Authorization Advice/0120—Acquirer-generated

Acquirers can send the Authorization Advice/0120 message when the following situations occur.

- The acquirer approves the Authorization Request/0100 message using acquirer host X-Code rules when the Authorization Request/0100 message cannot be sent to the Authorization Platform or when the Authorization Request Response/0110 message is not received from the Authorization Platform.

- The dual message acquirer completes a preauthorized automated fuel dispenser (AFD) transaction.
- Europe region acquirers complete a preauthorized petrol transaction (Maestro transactions only). For information about Maestro preauthorized petrol transaction processing for Europe region customers, refer to the *Customer Interface Specification* manual.

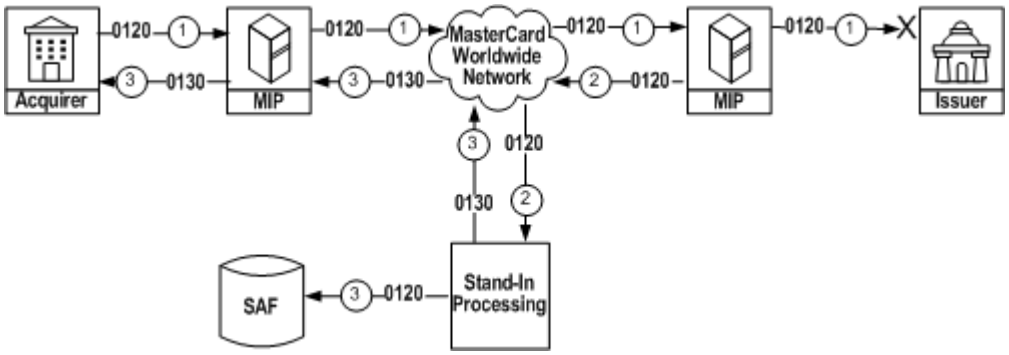
Authorization Advice/0120—Acquirer-generated (Issuer Available)
The following flow illustrates an Authorization Advice/0120 message when the issuer is available to receive the Authorization Advice/0120 message and respond with an Authorization Advice Response/0130—Issuer-generated message.

Authorization Advice/0120—Acquirer-generated and Authorization Advice Response/0130—Issuer-generated (Issuer Available) Flow

1. The acquirer initiates an Authorization Advice/0120—Acquirer-generated message containing DE 60, subfield 1, value 190 (Acquirer Processing System [APS] Approved) or 191 (Acquirer Processing System [APS] Completion Authorization Transaction), and then passes the 0120 message to the Authorization Platform. The Authorization Platform inserts DE 48 (Additional Data—Private Use), subelement 15 (Authorization System Advice Date and Time), and then sends the Authorization Advice/0120—Acquirer-generated messages 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 Advice/0120—Acquirer-generated (No Response from Issuer)
The following flow illustrates an Authorization Advice/0120—Acquirer-generated message when no response is received from the issuer.

Authorization Advice/0120—Acquirer-generated and Authorization Advice Response/0130—System-generated (Issuer Unavailable)



1. The acquirer initiates an Authorization Advice/0120—Acquirer-generated message containing DE 60, subfield 1, value 190 (Acquirer Processing System [APS] Approved) or 191 (Acquirer Processing System [APS] Completion Authorization Transaction), and then forwards the 0120 message to the Authorization Platform. The Authorization Platform inserts DE 48 (Additional Data—Private Use), subelement 15 (Authorization System Advice Date and Time) and sends the Authorization Advice/0120—Acquirer-generated messages to the issuer.
2. The Authorization Platform determines that the Authorization Advice/0120—Acquirer-generated message cannot be delivered to the issuer or the issuer did not respond. The Authorization Platform routes the Authorization Advice/0120—Acquirer-generated message to the Stand-In System.
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 System Advice Date and Time).

NOTE: Customers in the Europe region that route to an alternate issuer host for alternate processing, instead of Stand-In processing, will continue to receive advices. Alternate issuer host processing does not send Authorization Advice/0120 or Reversal Request/0400 messages to the alternate host.

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. Acquirers in the Europe region are required to send Authorization Advice/0120—Acquirer-generated messages to the issuer in no more than 20 minutes after the completion of Maestro CAT Level 1 petrol transactions. 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, subelement 63 (Additional Data, Trace ID) has been added to the acquirer-generated authorization advice/0120 layout as conditional data to further assist issuers in matching an AFD completion advice to the original preauthorization.
  - DE 48 (Additional Data—Private Use), 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.

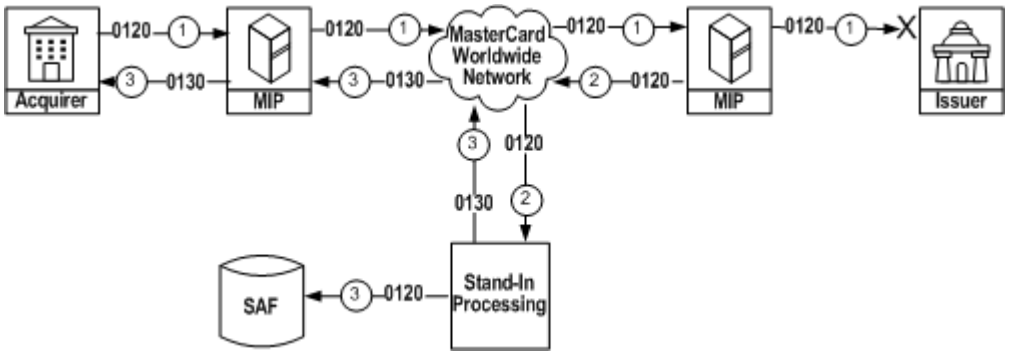
Track Data in AFD Advice Message—Issuers

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.

Authorization Advice/0120—Acquirer-generated when Responded to by Stand-In System (No Response from Issuer or Issuer Unavailable)

The following flow illustrates an Authorization Advice/0120—Acquirer-generated message when responded to by the Stand-In System when the issuer does not respond in time or is unavailable to respond.

Authorization Advice/0120—Acquirer-generated when Responded to by Stand-In System Flow



1. The acquirer initiates an Authorization Advice/0120—Acquirer-generated message containing DE 60, subfield 1, value 190 (Acquirer Processing System [APS] Approved) or 191 (Acquirer Processing System [APS] Completion Authorization Transaction), and then passes the 0120 message to the Authorization Platform. The Authorization Platform inserts DE 48 (Additional Data—Private Use), subelement 15 (Authorization System Advice Date and Time).
2. The Authorization Platform determines that the Authorization Advice/0120—Acquirer-generated message contains value 000001 in DE 121 indicating that the Authorization Request Response/0110 message was responded to by the Stand-In System. The Authorization Platform forwards the Authorization Advice/0120—Acquirer-generated message to the Stand-In System.
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. This ensures that the issuer receives the acquirer advice after the Authorization Advice/0120—System-generated message. The Stand-In System responds to the acquirer with an Authorization Advice Response/0130—System-generated message containing DE 48, subelement 15 (Authorization System Advice Date and Time).

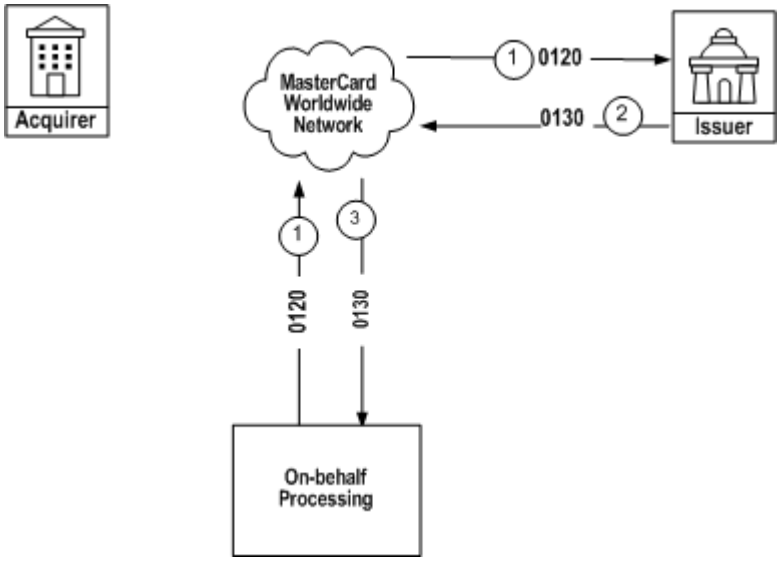
Authorization Advice/0120—System-generated

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.

Authorization Advice/0120—System-generated messages may be generated with on-behalf processing that occurred for the following services:

- Stand-In System
- X-Code System
- Mastercard In Control™ processing services
- Pre-validation services
- Transaction blocking services
- Payment Cancellation

Authorization Advice/0120—System-generated and Authorization Advice Response/0130—Issuer-generated Flow



1. On-behalf 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.

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

When issuers receive an advice, they should determine whether to adjust the cardholder's open-to-buy balance. For specific requirements related to advice messages arising from U.S. and Canada region automated fuel dispenser transactions, refer to Cardholder-Activated Terminals.

Acquirer Response Acknowledgement/0180 Messages

The Authorization Platform provides an optional response acknowledgement for authorization messages. This process uses Authorization Acknowledgement/0180 messages.

Acquirers are not required to support Authorization Acknowledgement/0180 messages; however, Mastercard encourages acquirers to support these messages. Acquirers can select this option at network configuration time.

Acquirer Response Acknowledgement/0180 Flow

The following diagram illustrates the Acquirer Response Acknowledgement process that is used to support authorization-related messages.

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 (POI)

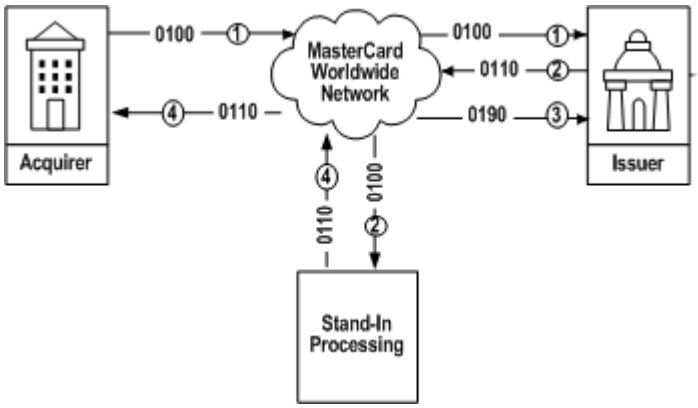
An Authorization Acknowledgement/0180 message does not necessarily indicate that the transaction was successfully completed at the POI.

Authorization Response Negative Acknowledgement/0190 Messages

If the issuer host generates an invalid or late Authorization Request Response/0110 message, the Stand-In System (if applicable for the issuer) or 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.

Issuer's 0110 Could Not Be Successfully Processed Flow

The following diagram illustrates the sequence if the issuer generates an invalid or late response.



1. The acquirer sends the Authorization Request/0100 message.
2. The issuer generates an invalid or late Authorization Request Response/0110 message and forwards it to the Authorization Platform. The Authorization Platform routes the Authorization Request/0100 message to Stand-In processing.
3. The Authorization Platform sends an Authorization Response Negative Acknowledgement/0190 message to the issuer. If the issuer response is late, the Authorization Platform sends a Reversal Advice/0420 message prior to sending the Authorization Response Negative Acknowledgement/0190 message.
4. The Authorization Platform or the Stand-In System (when applicable) generates the Authorization Request Response/0110 and sends it to the acquirer.

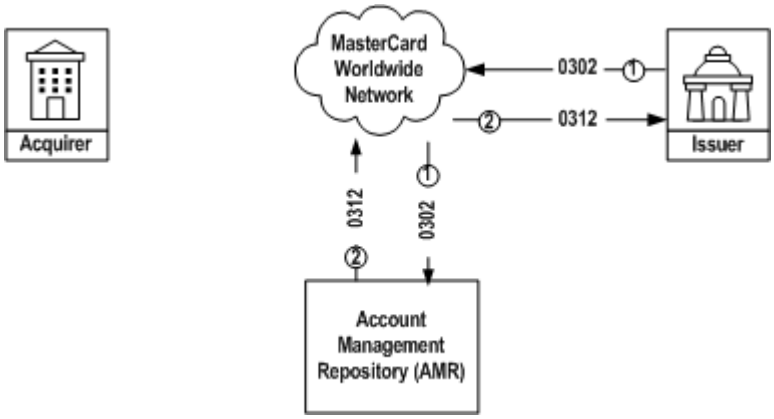
Processing Issuer File Update Messages

Issuers use the Issuer File Update Request/0302 message to update individual data files 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 can select when they participate in one or more of the Mastercard program and service offerings.

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

The following diagram illustrates the standard Issuer File Update Request/0302 and Issuer File Update Request Response/0312 message process.



1. The 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 Code field in the Issuer File Update Request Response/0312 message indicates whether the issuer file update was completed successfully.

Processing Reversal Request/Advice Messages

The Authorization Platform supports two types of reversals: system-generated and acquirer-generated.

Acquirer-generated messages include the Reversal Request/0400 and the Reversal Request Response/0410. System-generated messages include the Reversal Advice/0420 and the Reversal Advice Response/0430.

The Authorization Platform supports both full reversal and partial reversal functionality using the Reversal/04xx messages.

Reversal Request/0400 and Reversal Request Response/0410 Messages

An acquirer may choose to use reversal functionality based on certain conditions.

- The response message cannot be delivered to the merchant.
- The response message contains errors.
- A response message was not received.
- The response message was received too late.

A merchant may choose to use full reversal functionality to reverse the full amount of the original authorization amount. Partial reversal functionality is useful in adjusting a portion of the original authorization amount. For example:

- 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.
- The chip card declined a transaction that was approved by the issuer.

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.

When processing a Reversal Request/0400 or Reversal Advice/0420 message, issuers must appropriately adjust the cardholder's open-to-buy balance.

For full reversals, issuers should adjust the open-to-buy balance using the original approved amount stored in DE 6 (Amount, Cardholder Billing).

For partial reversals, issuers should adjust the open-to-buy balance by removing the original approved amount and applying the replacement amount stored in DE 95 (Replacement Amounts).

Reversal Request/0400 and Reversal Request Response/0410 Flow

The following diagram illustrates the flow of the Reversal Request/0400 and Reversal Request Response/0410 messages to reverse the Authorization Request/0100 message.

1. The acquirer initiates a Reversal Request/0400 message and submits 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 submits it to the Authorization Platform.
4. The Authorization Platform forwards the Reversal Request Response/0410 message to the acquirer.

Additionally, if the issuer host generates an invalid or late Reversal Request Response/0410 message, the Authorization Platform sends an Authorization Response Negative Acknowledgement/0190 message to the issuer.

Reversal Advice/0420 and Reversal Advice Response/0430 Messages

The Authorization Platform supports system-generated reversals that reverse the effect of a previous authorization transaction.

When the Authorization Platform determines that no issuer Authorization Request Response/0110 is received or the issuer's approved Authorization Request Response/0110 was unused or was undelivered, it generates a Reversal Advice/0420 message and sends it to the issuer. The issuer responds to a Reversal Advice/0420 message with a Reversal Advice Response/0430 message to indicate positive receipt of the Reversal Advice/0420 message.

When the Authorization Platform determines that it cannot deliver a Reversal Request/0400 message to the issuer because the issuer is signed out or unavailable, or when no issuer Reversal Request Response/0410 is received or the issuer's Reversal Request Response/0410 was unused, the Authorization Platform creates a Store-and-Forward (SAF) Reversal Advice/0420 message. The issuer responds to a Reversal Advice/0420 message with a Reversal Advice Response/0430 message to indicate positive receipt of the Reversal Advice/0420 message.

If the reversal is a partial reversal, the Authorization Platform provides the Reversal Advice/0420 message where DE 95 (Replacement Amounts), subfield 1 (Actual Amount, Transaction) contains a value other than all zeros and contains a value less than the amount in DE 4 (Amount, Transaction).

NOTE: Customers in the Europe region that route to an alternate issuer host for alternate processing, instead of Stand-In processing, will continue to receive advices. Alternate issuer host processing does not send Authorization Advice/0120 or Reversal Request/0400 messages to the alternate host.

Reversal Advice/0420 and Reversal Advice Response/0430 Flow

The following diagram illustrates the standard Reversal Advice/0420 message process.

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.

Authorization Reversal Mandate

The authorization reversal mandate has various requirements.

Acquirers must ensure that a merchant submits 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 finalization of the transaction. The reversal requirement does not apply to card acceptor business code MCC 5542 (Fuel Dispenser, Automated) transactions or to Mastercard contactless transit aggregated or transit debt recovery transactions.

This mandate enables issuers to more accurately manage the card's open-to-buy and addresses cardholders' and regulators' concerns with current practices.

NOTE: Since 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, 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.

Processing Administrative Request/Advice Messages

The Authorization Platform supports certain Administrative Request/Advice messages.

- Administrative Request/0600
- Administrative Request Response/0610
- Administrative Advice/0620
- Administrative Advice Response/0630

Administrative Request/0600 and Administrative Request Response/0610 Messages

Administrative Request/06xx—Customer Data messages allow participating customers to transmit customer data. customers can use the Administrative Request/06xx messages for Mastercard, private label, and other eligible card products.

This optional processing can provide the following benefits to customers:

- Private label issuers may reduce or eliminate the costs of maintaining multiple connections for each private label merchant.
- Mastercard issuers obtain an additional channel to secure applications, which is especially useful for instant credit.
- Acquirers can experience increased transaction volumes.

While there are many potential uses for Administrative Request/06xx—Customer Data messages, the following usages support the exchange of customer application and account data:

- Credit application request and response
- Credit application inquiry and response
- Account lookup inquiry and response
- Account maintenance request and response
- User lookup inquiry and response
- Counteroffer reply and response
- Preapproved offer inquiry and response

NOTE: Administrative Request/06xx—Customer Data messages should be used only for these intended purposes, as defined in DE 60 of the 0600 message.

Issuers that choose to participate in the exchange of Administrative Request/06xx—Customer Data messages are assigned an account range by Mastercard that can only be used for these messages and not used in any authorization, reversal, or administrative advice messages.

To participate in Administrative Request/06xx messaging, customers must complete the *Administrative Requests—Customer Data Participation* (Form 860), and submit the form to the Global Customer Service team.

Administrative Request/0600 Message

The Authorization Platform receives an Administrative Request/0600 message from an acquirer and applies applicable processing.

The Administrative Request/0600 message contains customer data in DE 113–119 (Reserved for National Use) and the usage type 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 is set at a default of 30 seconds, except DE 60 = 6500090 (Business application request) is set at 45 seconds.

Administrative Request Response/0610 Message

The Authorization Platform applies applicable processing if the issuer sends an Administrative Request Response/0610 message.

The Authorization Platform provides an Administrative Request Response/0610 message to the acquirer that contains one of the following responses:

- The issuer's response data, if the issuer provided a timely response
- A system-generated response provided by the Authorization Platform

NOTE: Issuers must be signed in to the Authorization Platform to receive Administrative Request/0600 messages. Issuers use Network Management/08xx messages for Authorization Platform sign in. For more information about Network Management/08xx messages, refer to the *Customer Interface Specification* manual.

Mastercard logs the Administrative Request/06xx—Customer Data messages for audit, billing, operational, reporting, and statistical purposes. Mastercard does not log any of the customer information contained in DE 113–DE 119 (Reserved for National Use) of Administrative Request/06xx—Customer Data messages. These data elements are passed through the Mastercard Network and no processing occurs on the content of the data elements.

Administrative Request/0600 and Administrative Request Response/0610 Flow

The following diagram illustrates the standard Administrative Request—Customer Data process.

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 Advice/0620 and Administrative Advice Response/0630 Messages

Administrative Advice/0620 and Administrative Advice Response/0630 messages are administrative messages that two parties participating in a given Mastercard program or service offering can 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.

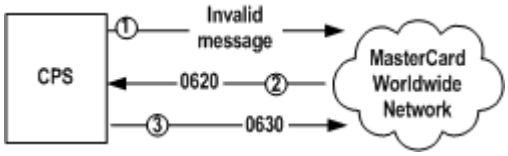
Administrative advice messages are used for the following reasons:

- 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.
- To transmit administrative (free-format) textual messages between any two parties participating as customers on the Authorization Platform.

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

Invalid Message—Administrative Advice/0620 and Administrative Advice Response/0630 Flow

The following diagram illustrates the administrative advice message process used to return an invalid message.



1. A customer processor system (CPS) generates an invalid message and forwards it to the Authorization Platform.
2. The Authorization Platform returns an Administrative Advice/0620 message to the CPS, with an appropriate error condition code indicating the point at which the Authorization Platform terminated message parsing or message processing.

3. The CPS acknowledges receipt of the Administrative Advice/0620 message and returns an Administrative Advice Response/0630 message to the Authorization Platform.

Administrative Advice/0620 and Administrative Advice Response/0630 Flow

The following diagram illustrates the administrative advice message process used to transmit administrative (free-format) textual messages between any two parties participating as customers on the Authorization Platform.

1. A customer processor system (CPS) generates an Administrative Advice/0620 message and forwards it to the Authorization Platform. Note that the CPS may be an issuer, an acquirer, or any other customer processing facility communicating via the Mastercard Network.
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.

NOTE: Customers should not use Administrative Advice/0620 messages in lieu of available 0100, 0120, and 0400 messages.

Using Network Management Request Messages

The Authorization Platform uses network management messages to coordinate system or network events or tasks. These messages also are used to communicate network status conditions. Network management messages can be customer-initiated or Authorization Platform-initiated.

Typical uses of customer-initiated network management messages include the following:

- Sign in to and sign out from the Authorization Platform
- Activate or deactivate socket connections
- Request network connection status
- Perform encryption key management tasks

Typical uses of system-initiated network management messages include the following:

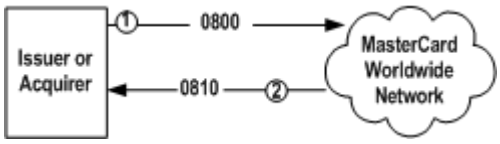
- Request network connection status

- Perform encryption key management tasks

Standard Network Management/08xx Messages

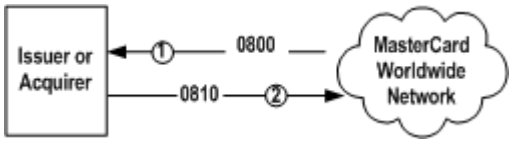
Diagrams illustrate the exchange of Network Management Request/0800 and Network Management Request Response/0810 messages.

Network Management/0800—Customer-initiated Flow



1. The customer sends a Network Management Request/0800 message to the Authorization Platform. DE 70 (Network Management Information Code) indicates the type of customer-initiated network management request message.
2. The Authorization Platform generates a Network Management Response/0810 message to acknowledge receipt of the Network Management Request/0800 message.

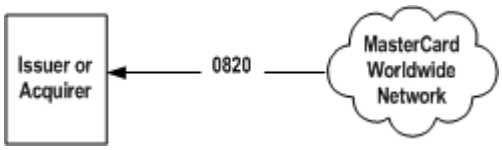
Network Management/0800—System-initiated Flow



1. The Authorization Platform generates the Network Management Request/0800 message. DE 70 indicates the type of system-initiated network management request message.
2. The customer generates a Network Management Response/0810 message to acknowledge receipt of the Network Management Request/0800 message.

Network Management Advice/0820—System-initiated Flow

The following diagram illustrates the standard Network Management Advice/0820 message process between the Authorization Platform and the customer. The Network Management Advice/0820 message does not require a response.



Authorization Sign In/Sign Out

A Network Management Request/0800 message is used to carry out an Authorization Platform sign in that allows issuers to manage the activities and the status of a given routing destination for a group of account ranges.

A routing destination is a predefined set that consists of Mastercard Interface Processors (MIPs) and the issuer host connections available for transaction processing. Each routing destination is assigned a Group Sign-in ID (GSI).

To identify the issuer's readiness to receive authorization messages, the Authorization Platform requires a sign-in message or a sign-out message to be delivered to the Authorization Platform. The sign in signifies the readiness of the issuer to receive transactions for all the account ranges over all the MIPs and issuer host connections in the group.

Issuers must include one of the following values in DE 70 to indicate the type of sign-on/sign-off request:

- 001 = Sign-on (by prefix)
- 002 = Sign-off (by prefix)
- 061 = Group sign-on (by Mastercard group signon)
- 062 = Group sign-off (by Mastercard group signon)
- 063 = Group sign-on alternate issuer route
- 064 = Group sign-off alternate issuer route

The Mastercard Worldwide Network does not track session status information for an acquirer. Therefore, Authorization Platform sign-on/sign-off for acquirers is not required. However, acquirers optionally may send Authorization Platform sign-on/sign-off messages if required by their acquirer host or vendor software.

Acquirers optionally submitting an Authorization Platform sign-on/sign-off message must include one of the following values in DE 70 to indicate the type of sign-on/sign-off request:

- 061 = Group sign-on (by Mastercard group signon)
- 062 = Group sign-off (by Mastercard group signon)

Session Management

The Mastercard Network offers two options to verify the status of network connections using network management messages.

- At the Mastercard Interface Processor (MIP) level using a session activation request
- At the Authorization Platform application level using an echo test message

Mastercard also supports use of zero length probe messages to detect broken sockets or Transmission Control Protocol/Internet Protocol (TCP/IP) sessions that no longer exist. The customer and the MIP can send a zero length message to an idle socket that contains a two-byte header set to 0x0000. For more information about managing socket connections, refer to the *Data Communications Manual*.

Session Activation/Deactivation

Session activation (and deactivation) allows the issuer to control when an established socket connection is ready to receive transactions. This provides the ability for the issuer to make a TCP/IP socket connection and to indicate that the connection is ready to receive traffic (activate) or to stop receiving traffic (deactivate).

This level of session management is not relevant for acquirers as the Mastercard Network will always accept and respond to acquired transactions on established sockets. The session activation process is only relevant to acquirers for performing a local probe of the sockets connected to the MIP.

Issuers that choose to perform session management at this level are required to send an activation request using the Network Management Request/0800—Host Session Activation message for each socket connection before receiving authorization message traffic. If an issuer does not participate in Enhanced Session Management, all host connections for that issuer are considered active (that is, ready to receive transactions) once the issuer's sockets are open.

Issuers must include one of the following values in DE 70 to indicate the type of session activation/deactivation request:

- 081 = Host session activation
- 082 = Host session deactivation

Session-based Network Routing

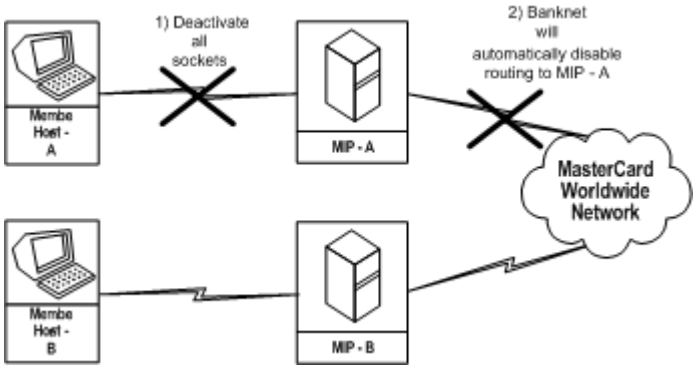
Mastercard supports a configurable option on the Mastercard Network that uses the TCP/IP to automatically manage load balancing of transactions between MIPs with available connections.

This feature is typically used when an issuer is load balancing message traffic across multiple MIPs, potentially at different sites, and Mastercard needs to detect when a given MIP should be considered disabled so that no further transactions are routed to that MIP until it is enabled.

Upon receiving the transaction from the acquirer MIP, the issuer MIP tries to deliver the transaction to the issuer host. If the MIP detects that all the socket connections to the issuer host are de-activated, the corresponding MIP is disabled. Once the MIP is disabled, it no longer receives traffic for that MIP until it is enabled. The MIP will not be re-enabled until an issuer host activates a socket connection with the MIP.

Session-based Network Routing Flow

The following diagram illustrates the Session-based Network Routing option.



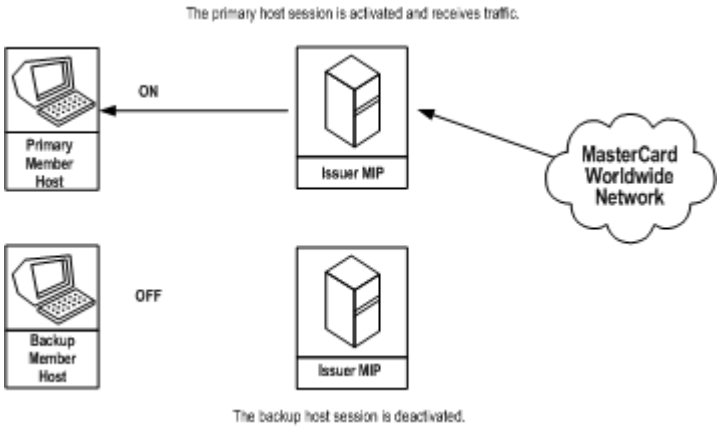
Session Activation and Transaction Routing

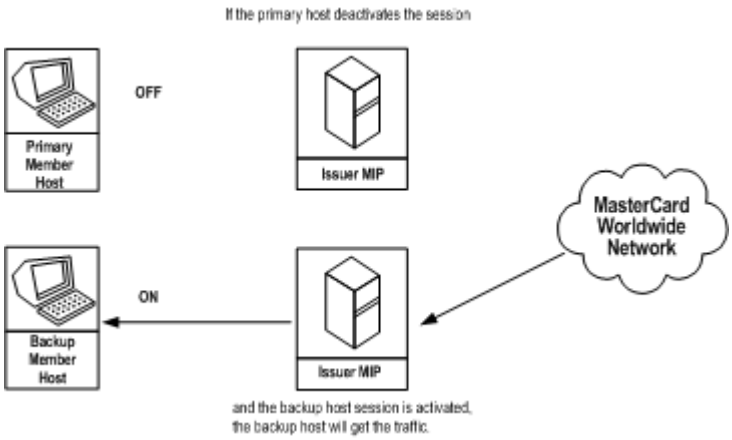
Session activation and session-based network routing can be used by customers to control the delivery of the issuer traffic.

For example, an issuer with a primary and backup host may want to control the distribution of its traffic to one or to the other host. The prerequisite is that both hosts and related MIPs are defined in the same destination route. The customer must activate at least one session from the primary, and then sign on with its GSI from the host. If the issuer wants to put its primary host in maintenance and get the traffic on the backup host, the issuer will need to de-activate the primary host session and activate at least one of the backup host sessions. Combined with session-based network routing, traffic will be automatically routed to the backup host.

Session Activation and Transaction Routing Flow

The following diagrams illustrate session activation and transaction routing.





To participate in Enhanced Session Management and Session-based Network Routing options, customers must complete the *Session Management Member Participation Enrollment Form* (Form 868), and submit the form to the Global Customer Service team.

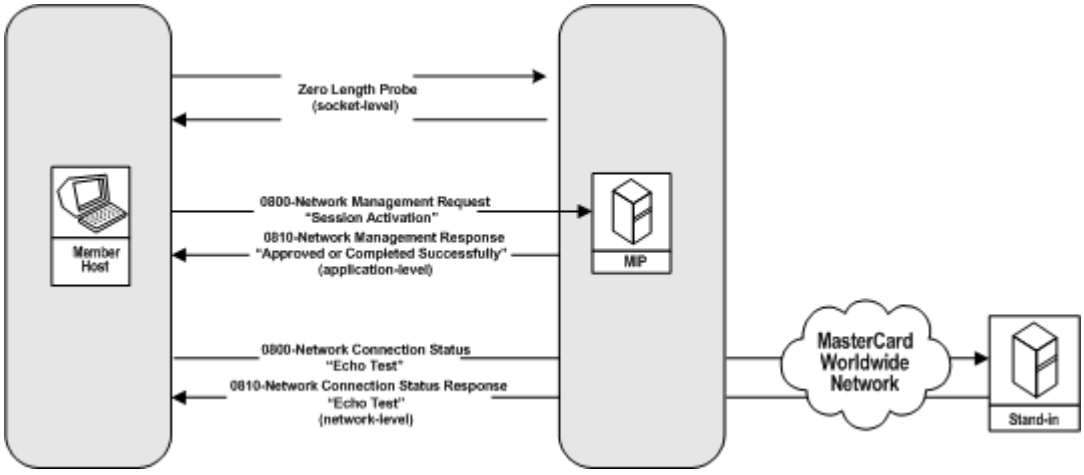
Network Connection Status

Network connection status (echo test) messages allow issuers and acquirers to check the status of their connection to the Mastercard Network. Issuers and acquirers that choose to perform session management at this level are required to send an activation request using a Network Management Request/0800—Network Connection Status message and include DE 70 value 270 (Network connection status—echo test).

Best Practices

As a best practice, Mastercard recommends that customers use any one or a combination of these network connectivity management options, as illustrated in the following diagram. These varying levels of probes are recommended in place of using a repeat sign-in Network Management Request/0800 message to verify host connectivity to Mastercard.

Network Connectivity Management Options



Store-and-Forward (SAF) Message Retrieval (Issuers)

The Authorization Platform places advice messages into the SAF queue. The SAF queue retains all of these messages for four days for the issuer to retrieve.

Issuers receive SAF messages after signing on to the Mastercard Network using a Network Management Request/0800 message containing DE 70 with value 001 (Sign on [by prefix]) or 061 (Group Sign on [by Mastercard group sign-on]) or when the Authorization Platform SAF processing recognizes that the issuer is available.

When an issuer has a large number of SAF records (for example, because of an extended outage) and they are not able to process them through the preferred method of multiple SAF sessions with Mastercard due to a technical problem, issuers can contact their Customer Service Representative to request the retention and restoration of their SAF messages beyond the current four-day limitation.

Dynamic PIN Encryption Key (PEK) Exchange

The dynamic PEK exchange process is facilitated between the Authorization Platform and customers via the Network Management/08xx messages.

The Authorization Platform generates dynamic PEKs at least once per 24-hour period for each customer key zone.

The process in which the Authorization Platform initiates the key exchange process is as follows:

1. The Authorization Platform sends a Network Management Request/0800 message with DE 70, value 161 (Encryption Key Exchange) to the customer to change the PEK.
2. The customer responds with a Network Management Request Response/0810 message.
3. The Authorization Platform completes the key exchange process by sending a Network Management Advice/0820 message.

The customer also can request that the Authorization Platform initiate the key exchange process as follows:

1. The customer sends a Network Managment Request/0800—PEK Exchange-On Demand message to the Authorization Platform in which DE 70 contains values 162 (Solicitation for Encryption Key Exchange) or 163 (Solicitation for Encryption Key Exchange - TR-31 Keyblock).
2. When the Authorization Platform receives the Network Managment Request/0800—PEK Exchange-On Demand message to initiate the key exchange, the Authorization Platform responds with a Network Management Request Response/0810 message, thus immediately initiating the standard, four-step key exchange sequence provided above.

Possible PEK Exchange Triggers

Possible PEK exchange triggers include the following:

- Customer requests the generation of new key through an online Network Managment Request/0800—PEK Exchange-On Demand message.
- The Sanity-error-counter threshold is reached.

- The amount of time elapsed since a new key was last issued is more than 12 hours.
- Mastercard manually initiates the PEK exchange sequence.

NOTE: The Dynamic PEK Exchange service is not available in the Europe region.

Chapter 6 Stand-In Processing

The Stand-In Processing section describes the Stand-In processing facility at Mastercard. It explains the tests that Stand-In System processing performs and the order in which Stand-In processing performs them to ensure appropriate authorization responses.

Stand-In Processing Service

Stand-In processing is a standard Mastercard service that responds to authorization requests that have been routed to the Mastercard Network on behalf of the issuer.

Stand-In processing is mandatory for Mastercard credit products in all regions. Issuers may choose to block Stand-In System processing for debit products in all regions, except in the U.S. region.

Stand-In processing is available to all issuers 24 hours a day, 365 days a year. However, Stand-In processing responds only when the issuer does not respond, is unavailable, cannot be reached, or provides an invalid response resulting as follows:

- Stand-In processing responds for online issuers only when the issuer is not signed in, the transaction cannot be delivered to the issuer, the issuer MIP times out (does not receive an authorization response within specified time limits), or the issuer's response message contains invalid formatting or information resulting in an issuer edit error.

Stand-In processing does not apply to the following types of transactions.

Transaction Type	Authorization Response from Stand-In Processing
Account Status Inquiry Service	Service not available
ATM Credit Card Cash Advance in Installments transactions	Service not available
Balance inquiry transactions at ATM and POS	Service not available
PIN management transactions	Service not available
Product Inquiry Service	Service not available
Funding transactions with a credit card at an ATM **NOTE: This is limited to non-Europe acquired funding transactions. If the transaction is Europe acquired, it could be processed in the Stand-In System.**	Service not available
Private label prepaid card activation plus initial load transactions	Service not available
Refund transactions	Service not available
Card activation transactions	Decline

For details about transaction processing for each of the above transaction types, refer to the *Customer Interface Specification* manual.

How Stand-In Processing Works

Stand-In processes authorization requests according to a series of tests.

To determine an authorization response, these tests rely on data in the authorization message and some or all of the following data provided by the issuer:

- Selective Range Blocks
- Account Listings (Negative or Premium)
- Stand-In Processing Parameters
- Stand-In Processing Validation Services

Selective Range Blocks

Issuers may list a range of account numbers to indicate that they have not issued the numbers to cardholders.

Account Listings

Issuers may list accounts in the Stand-In Account File as Negative (lost/stolen/fraud) or Premium Listings for valued/preferred cardholders.

Issuers may list individual card numbers to identify exception accounts that are processed differently than regular accounts. They can list these accounts with either higher limits to ensure approval, such as the limits for Premium Listings or as Negative for lost/stolen/fraud or unpaid/over limit accounts that must be declined.

If Stand-In processing determines that an account is listed in the Stand-In Account File, Electronic Warning Bulletin, or Local Stoplist, Stand-In processing is modified, as described in Stand-In Account File Test. For a description of how to list accounts, refer to the *Account Management System User Manual*.

Stand-In Processing Parameters

Issuers use the *Stand-In Processing—Transaction Category Code Global Parameters* (Form 0041g) to view the current Mastercard default parameters for processing authorization requests.

Issuers may define the following within the Stand-In application on Mastercard Connect™:

- Amount limits that apply for a particular combination of parameters in the authorization request
- Accumulative number and amount limits that are calculated over a specified number of days

Stand-In processing is based on limits and transaction amounts in U.S. dollars.

For information about brand product categories and associated card products, refer to the *Stand-In Processing Worksheet—Brand Product Categories Addendum* (Form 0041a).

Stand-In Processing Validation Services

The issuer provides the key components from the issuer's security service calculation. For transactions that meet the criteria, Stand-In processing validates the security service for the services the issuer has chosen.

For issuers that participate in a validation service, Stand-In processing applies the appropriate validation test.

Issuers that want to subscribe to one of the validation services must use the *Key Validation Service Specification Form* (Form 0735).

NOTE: Only Europe region customers' PIN keys are managed via On-behalf Key Management (OBKM). Non-Europe region customers' PIN keys are managed using the *Hard Copy Key Exchange* (Form 0723), which is processed through Key Management Services (KMS) in Waterloo, Belgium.

Issuers must subscribe to all Stand-in validation services that are applicable to their program(s), including—but not limited to—the following:

- M/Chip Cryptogram Validation
- Token Validation
- Card Validation Code 1 (CVC 1) Verification
- Card Validation Code 3 (CVC 3) Verification
- Mastercard® *Identity Check*™ Dynamic AAV Verification

Personal Identification Number (PIN) Verification in Stand-In Processing remains optional.

Stand-In Tests

The Stand-In tests systematically review the authorization request to determine an appropriate authorization response.

Selective Range Blocks Test

The Selective Range Blocks test determines whether the account number in the transaction falls within a blocked range. If it does, Stand-In processing can issue a response of "do not honor" for any authorization request within the blocked ranges.

Issuers may block a range of account numbers to indicate that they have not issued the numbers to cardholders, preventing a known, unsupported vector or temporarily responding to a known fraud event. Issuers may establish range blocks within the Stand-In application on Mastercard Connect™.

The Stand-In application will manage and automatically block:

- Newly issued ranges of account numbers.

- Transactions that contain any of the following gambling card acceptor business codes (MCCs):
  - 7800—Government Owned Lottery (U.S. Region Only)
  - 7801—Internet Gambling (U.S. Region Only)
  - 7802—Government Licensed Horse/Dog Racing (U.S. Region Only)
  - 7995—Gambling Transactions
  - 9406—Government-owned Lottery (Specific Countries)

Stand-In Account File Test

The Stand-In Account File test determines whether the Stand-In Account File lists the account number in the transaction as an exception account.

Stand-In processing returns an authorization response based on the entry reason as follows:

- If Stand-In processing determines that an account is listed in the Stand-In Account File with entry reason F (fraud), P (capture card), or X (counterfeit), it immediately generates a capture card response.
- Negative accounts listed in the Electronic Warning Bulletin or Local Stoplist files generate an authorization response of capture card.
- If the account is listed with entry reason C (credit), L (lost), O (other), S (stolen), or U (unauthorized use), Stand-In processing returns a response based on the issuer's input from the Stand-In Account File test.
- If the account is listed in the Stand-In Account File with entry reason V (Premium Listings), Stand-In processing continues testing. Stand-In processing uses the tests that are applicable for these types of premium/preferred accounts.

For information about exceptions and additions to Stand-In processing, refer to Exceptions and Additions to the Stand-In Process.

Expiration Date Test

The expiration date test determines whether the expiration date provided in the request message is less than the current year and month, or is more than 10 years in the future.

M/Chip Cryptogram Validation Test

M/Chip Cryptogram Validation in Stand-In Processing is a M/Chip processing service for all EMV chip card issuers.

NOTE: All issuers globally that participate in Stand-In processing must have M/Chip Cryptogram Validation in Stand-In Processing performed during Stand-In processing.

The M/Chip Cryptogram Validation in Stand-In Processing service supports issuers that process chip transactions on an on-going basis, including the validation of the authorization request cryptogram (ARQC) and generation of the authorization response cryptogram (ARPC) on their hosts 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 authorization processing for issuers that use the M/Chip Select 2.0, M/Chip Lite 2.1, M/Chip 4.0 (Mastercard, EMV CSK, and EMV2000 session key derivation methods), and *M/Chip™ Advance*.

Mastercard also supports EMV Common Core Definition (CCD), which specifies a minimum common set of card application implementation options, card application behaviors, and data element definitions to create a transaction that complies with EMV standards.

Stand-In processing performs this test only if the transaction meets the following criteria:

- The issuer has requested participation in this service.
- The transaction contains chip card data elements.

For transactions that qualify for this service, Stand-In processing:

- Validates the ARQC and the TVR/CVR fields according to issuer-defined patterns
- Approves or declines the transaction
- Generates the ARPC
- Creates the Authorization Request Response/0110 message
- Creates the Authorization Advice/0120 message

For more information about the M/Chip Cryptogram Validation in Stand-In Processing service, refer to Authorization Services Details.

PIN Verification Test

Mastercard offers a PIN verification service for transactions processed by the Stand-In System that contain unverified PIN data in Authorization Request/0100 messages. Issuers that want Mastercard to verify the PIN on transactions processed by Stand-In must provide PIN processing parameters to Mastercard.

Stand-In processing will bypass the PIN Verification Test and proceed to the next sequential Stand-In test, unless the issuer participates in either a PIN pre-validation or PIN validation in Stand-In service.

For more information about the PIN Verification in Stand-In processing service, refer to Authorization Services Details.

CVC 1 Test

The card validation code 1 (CVC 1) test is a processing service for all issuers that use magstripe technology.

NOTE: Effective 1 April 2017 based on region specific effective dates per *Global Operations Bulletin* No. 4, 1 April 2016, Revised Standards for Validation Services During Stand-In Processing, all issuers globally that participate in Stand-In processing must have CVC 1 Verification in Stand-In performed during Stand-In processing.

Stand-In processing performs the test only if the transaction meets the following criteria:

- The issuer has requested participation in this service.

- The authorization request contains full-unaltered Track 1 or Track 2 data and value 80 or 90 in Point-of-Service (POS) Entry Mode field.

A value of 80 indicates that a chip-capable terminal was unable to process a chip card 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.

A value of 90 indicates that the PAN was entered 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.

Mastercard supports issuers participating in CVC 1 validation in Stand-In processing services by responding to the authorization message on behalf of the issuer. Mastercard considers the results of the CVC 1 validation in DE 48 (Additional Data—Private Use), subelement 87 (Card Validation Code Result) 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.

If an issuer participates in CVC 1 prevalidation services and is unavailable to respond to the authorization request, Mastercard considers the results of the CVC 1 prevalidation in DE 48, subelement 71 (On-behalf Services) when the transaction is processed by the Stand-In System.

Stand-In processing does not verify CVC 2 values.

CVC 3 Test

CVC 3 validation in Stand-In is a processing service for all issuers that use contactless magstripe technology.

NOTE: Effective 1 April 2017 based on region specific effective dates per *Global Operations Bulletin* No. 4, 1 April 2016, Revised Standards for Validation Services During Stand-In Processing, all issuers globally that participate in Stand-In processing must have Dynamic CVC 3 Validation in Stand-In Processing performed during Stand-In processing.

CVC 3 validation in Stand-In processing services are available for transactions that derive from proximity chip functionality with magnetic stripe Track 1 or Track 2 data containing a CVC 3 value.

Mastercard supports issuers participating in CVC 3 validation in Stand-In processing services by responding to the authorization message on behalf of the issuer. Mastercard considers the results of the CVC 3 validation in DE 48, subelement 71 (On-behalf Services) when responding to the Authorization Request/0100 message.

If the issuer participates in one of the CVC 3 pre-validation services and is unavailable to respond to the authorization request, Mastercard considers the results of the CVC 3 pre-validation when the transaction is processed by the Stand-In System.

For information about the CVC 3 validation in Stand-In processing services, refer to Authorization Services Details.

AAV Verification Test

The Mastercard® *Identity Check*™ AAV Verification in Stand-In Processing test is a required service.

Issuers must request that Stand-In processing perform the AAV verification test when the issuer's host system is unavailable to respond to the Authorization Request/0100 message containing AAV data.

For more information about the Mastercard *Identity Check* AAV Verification in Stand-In processing service, refer to Authorization Services Details.

Transaction Limits Test

To perform the Transaction Limits Test, Stand-In processing compares the applicable amount in the authorization request to the transaction limit designated by the issuer in the Stand-In application on Mastercard Connect™.

Issuers designate transaction limits by combinations of the transaction limits parameters. Combinations may include any or all of the following parameters:

- Country Code—The country code is a three-digit, numeric code that identifies the country. Issuers may use these codes to establish higher or lower transaction limits for a country or countries where the transaction is acquired.
- Promotion Code—The promotion code is a six-character, alphanumeric code that the issuer establishes to identify transactions that meet the requirements for an issuer's promotional program. Issuers may use these codes to establish particular transaction limits for transactions that meet their program requirements.
- Cardholder-activated terminal (CAT) level indicator—CAT level indicator is a one-digit, numeric code that identifies transactions that occur at one of the four types of CATs or that use electronic commerce or transponder technology. Issuers may use these codes to establish particular transaction limits for CAT transactions.
- Transaction Category Code (TCC)—TCC is a one-character, alphabetic code that identifies the type of transaction. Issuers may use these codes to establish particular transaction limits based on the type of transaction.
- Card Acceptor Business Code (MCC)—MCC is a four-digit, numeric code that identifies the card acceptor business/merchant category that best describes the business conducted. Issuers may use these codes to establish higher or lower transaction limits for certain merchants.

For a list of valid numeric country codes, valid TCCs, and valid MCCs, refer to the *Quick Reference Booklet*. For more information about promotion code requirements in authorization messages and CAT level values (DE 61, subfield 10), refer to the *Customer Interface Specification* manual.

Mandatory Mastercard Parameter Combinations

Issuers must have certain transaction limit parameter combinations to ensure compliance with Mastercard established transaction limits. The required parameter combinations are described on the following pages. These parameter combinations apply to a specific BIN and use one of the 19 combinations available to the issuer.

Transaction Category Code Parameter (Mastercard-established minimum limits or higher issuer-defined limits)

All issuers must have transaction limits by TCC. Mastercard has established minimum TCC limits. Issuers may establish higher limits for some or all TCCs, and they may establish different limits for card present and card-not-present point-of-interaction situations.

Current issuer-defined TCC limits are available on the Stand-In application on Mastercard Connect™.

Accumulative Limits Test

To perform the Accumulative Limits test, Stand-In processing compares the cumulative number of transactions approved on the current day and over the previous two, three, and four groups of days with the parameters for those numbers designated by the issuer.

Stand-In processing also compares the cumulative amount of all transactions approved on the current day and over the past two, three, and four groups of days with the parameters for those amounts designated by the issuer.

Accumulative Limit Parameters

All issuers must have accumulative limits defined.

Mastercard has established minimum Accumulative limits, which are defined in the *Stand-In Processing—Transaction Category Code Global Parameters* form (Form 0041g). Issuers may set limits that differ from the Mastercard default limits.

For example, assume the issuer designated the following accumulative limits:

Current Day	four transactions and USD 1,200
Day 2	six transactions and USD 1,200
Day 3	six transactions and USD 1,200
Day 4	six transactions and USD 1,200

A cardholder that had two transactions approved by Stand-In processing for a total dollar amount of USD 500 on Day 1 would have available a maximum of four more transactions and USD 700 that could be approved through Stand-In during the following three days.

For an MO/TO request, if the cumulative number or dollar amount in the request exceeds the limit established by the issuer, Stand-In processing generates a response of decline.

For any other type of transaction, if the cumulative number or dollar amount in the request exceeds the limit established by the issuer, Stand-In processing generates a response of "decline."

Stand-In Response

If Stand-In processing performs all of the Stand-In tests without generating a response of "decline," Stand-In processing approves the authorization request. It also adds the transaction amount to the cardholder's accumulative record in preparation for the next comparison with the Accumulative Limits.

Exceptions and Additions to the Stand-In Process

Stand-In processing performs the tests as described earlier in the order listed, until it generates an authorization response.

For the following types of transactions, however, Stand-In processing modifies processing or performs additional steps:

- Automated Negative Listing Service
- Online Transactions
- Premium Listings
- Automated Premium Listings

Automated Negative Listing Service

The Automated Negative Listing Service will automate adding lost and stolen cards to the Stand In Negative List. This service will benefit issuers that would like to minimize internal costs associated to managing their lost/stolen account listings by automating the listings based upon the issuer's authorization response.

Issuers outside of the Europe region that participate in Stand-In processing can choose to participate in the Automated Negative Listing Service. Issuers in the Europe region are systematically enrolled in the Automated Negative Listings Service and may choose to opt-out at any time.

To register in the optional new Automated Negative Listings Service, go to Mastercard Connect and click Manage My Accounts. Once inside the application, issuers can opt-in and opt-out of the service using the Update a Product process.

Issuers that participate in Stand-In processing and participate in the Automated Negative Listing Service must be aware that Mastercard will automatically list accounts to the Stand-In Negative Listing File (MCC102). Stand-In processing will add any account that was declined by issuers with response code in the Authorization Request Response/0110 message that matches a response code defined by the issuer during participation in the service and all default response codes. Dual Message System (Authorization) issuers that participate in Stand-In processing can select their own response codes via Mastercard Connect. Single Message System issuers that participate in Stand-In processing can select their own response codes via Single Message Transaction Manager.

Automated Negative Listing Service Process Flow

1. If issuers are configured for Stand-In processing, they are eligible to participate in Automated Negative Listing Service.
2. Issuers should register for the Automated Negative Listing Service.
3. Once the service is activated, Mastercard will monitor the Authorization Request Response/0110 message from the issuer.
4. When the response code on the transaction from a participating issuer matches one of the default response codes (04–Card Capture, 41–Lost Card, 43–Stolen Card) and response code(s) defined by the issuer, if any, Stand-In processing will add the account to the Negative Listing file MCC102 with the response code and entry reason code.
5. If any transaction for the account that was listed in the Negative Listing file flows through the Authorization Platform, Stand-In processing will decline the transaction on behalf of the issuer.
6. The Authorization Platform uses the internal response to create an Authorization Request Response/0110 message and sends it to the acquirer.
7. The Authorization Platform creates an Authorization Advice/0120 message and places it in the Mastercard Network for later delivery to the issuer.

NOTE: The negative listings appear on the AM700010–AA report and are identified uniquely.

Online Transactions

Stand-In processing performs all steps of the testing process as described.

In addition, for online issuers, when Stand-In processing generates an authorization response of approved, decline, or capture card, it also creates a store-and-forward (SAF) advice message, which contains the transaction data for the authorization request. The issuer can retrieve these SAF messages online (described in Online Authorization Messages).

Premium Listings

To identify Premium Listings, issuers establish transaction limits and accumulative limits in the Premium Listings section in the Stand-In account file and on the Stand-In application on Mastercard Connect™.

1. If the transaction fails the Transaction Limits Test, Stand-In processing applies the response designated in the Premium Limits Test. If the transaction passes the Transaction Limits Test, Stand-In processing proceeds to the Accumulative Limits Test.
2. During the Accumulative Limits Test, Stand-In processing applies the Days and Count Limit parameters designated by the issuer.
3. If the transaction fails the Accumulative Limits Test, Stand-In processing will decline the transaction.
4. If the transaction passes the Accumulative Limits Test, Stand-In processing adds the transaction amount to the Premium Listings accumulation amount for that cardholder. Stand-In processing compares the sum to the Premium Listings amount designated in the Stand-In Account File. If the transaction fails the Accumulative Amount Test for Premium Listings, Stand-In processing will decline the transaction.

5. If the transaction passes the Accumulative Amount Test, Stand-In processing applies the next test.

For more information, refer to Setting Stand-In Parameters.

Automated Premium Listings

The MasterCard Premium Listings offers a turnkey way to help ensure that issuer's preferred cardholders receive the reliability of service they expect, even when their systems are not available. As part of the MasterCard Stand-In Authorization, Premium Listings provides issuers with the flexibility to set unique spend level parameters for their preferred cardholders when Stand-In processing authorizes their purchases on the issuer's behalf.

Stand-In Automated Premium Listings service essentially conducts weekly data analysis to identify MasterCard's top 2 percent of highest spending cardholders globally. This service automatically adds these accounts to the Stand-In Premium Listings file. Any account already on the file will be excluded to ensure duplicates do not exist.

Existing reports with card file information on the Stand-In Account File, including the Daily Account File Activity Report, are updated to show the accounts added by the Automated Premium Listings service and differentiate between those listed by the issuer and by the service.

Card Level Support

Card level support for transactions processed by the Stand-In System allow issuers to distinguish between individual cards when the same primary account number (PAN) is used for multiple cards.

Card level support allows issuers to list accounts in the Stand-In Account File at the individual card level for a particular entry reason such as lost, stolen, premium account. Card level support also allows issuers to have the Stand-In System process accumulative limits at the individual card level.

Issuers must notify Mastercard for each account range for which they want to participate in card level support using the *Card Level Support Form* (Form 760).

Issuers that participate in card level support must ensure that the following card level information is present on cards within the specified range:

- Card Sequence Number—Three-position card sequence number distinguishes between cards that use the same PAN. This three-position number is located in the discretionary data field of Track 2 data in the magnetic stripe on the back of each card. For chip cards, the number is encoded on the chip in the EMV data element 5F34 (Application PAN Sequence Number).
- Card Expiration Date—Expiration date of the listed card.

Stand-In processing requires the presence of the following data elements in authorization requests associated with account ranges that participate in card level support:

- Card Sequence Number—DE 35 (Track 2 Data) contains the card sequence number.
- Card Expiration Date—DE 14 (Date, Expiration), DE 35 (Track 2 Data) may contain the card expiration date.

WHEN…	THEN Stand-In processing…
The card sequence number or card expiration date is not present in Authorization Request/0100 messages that are sent to Stand-In for authorization processing	Rejects the Authorization Request/0100 message by returning a DE 39 (Response Code) of 05 (Do not honor) in the Authorization Request Response/0110 message.

Card Validation Code 1 Verification in Stand-In Processing

Card validation code 1 (CVC 1) verification in Stand-In processing provides additional protection during Stand-In processing.

When the issuer times out or is unavailable, normal Stand-In processing runs through a series of tests to determine an authorization response. If the issuer is signed up for CVC 1 verification, Stand-In processing performs an additional test to verify that the CVC 1 is valid.

Mastercard requires that participating issuers provide confidential security data known as Data Encryption Standard (DES) keys to Mastercard for each account range that participates in CVC 1 verification in Stand-In processing.

Mastercard offers the following options for CVC 1 verification in Stand-In processing:

- Allow issuers to assign multiple sets of DES keys to an account range.
- Allow issuers to assign a single set of DES keys to an account range.

The issuer will receive DE 48 (Additional Data—Private Use), subelement 87 (Card Validation Code Result) in the Stand-In Authorization Advice/0120 message when the CVC 1 validation result was not valid.

NOTE: Effective on 1 April 2017 based on region specific effective dates per *Global Operations Bulletin* No. 4, 1 April 2016, Revised Standards for Validation Services During Stand-In Processing, all issuers globally that participate in Stand-In processing must have CVC 1 Verification in Stand-In performed during Stand-In processing.

NOTE: The CVC 2 value does not apply to CVC 1 verification in Stand-In processing.

Reporting CVC 1 Verification in Stand-In Processing

Regardless of the CVC 1 verification method you are using—multiple sets of DES keys or a single set of DES keys—the results of CVC 1 verification in Stand-In processing appear on the following reports:

All Customers

- Authorization Summary Report (AB505010-AA)—The Fail Reason category Invalid Chip/CVC on the Stand-In section of this report lists transactions that failed because any of the following occurred:
  - Invalid CVC (failed the CVC 1 test)
  - Invalid chip (failed the M/Chip Validation test)
  - Magnetic stripe CVC errors in DE 48 (failed at the MIP)
- Authorization Parameter Summary Report (SI737010-AA)—Participation in CVC 1 Verification in Stand-In processing displays in the On-behalf Services section of the report.

Online Customers

Store-and-forward records contain value 0028 in positions 4–7 of DE 60 (Advice Detail Code) and the MCBS Issuer Authorization Detail Report contains value 0028 under FAIL RSN.

To Participate

To implement the CVC 1 service, complete the *Key Validation Service Specification Form* (Form 735).

For More Information

For more information about the DES keys, refer to the *On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications* manuals.

Chapter 7 Authorization Services Details

This section describes Mastercard services that interface with and add value to the Mastercard Authorization Platform. This section also includes information about requesting and using these services.

Account Balance Response

The account balance response enables issuers to include account 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.

The account balance response provides cardholders with up-to-date balance information on their prepaid cards.

Issuers must provide account balance information for both approved and declined authorization responses.

When the issuer provides the available balance in the authorization response, POS and ATM terminals that are programmed to accept account balance data can display or print the available balance.

- Approved Responses—The available balance on an approved response is the account balance after the transaction amount has been deducted from the account.
- Declined Responses—The account balance response is used on a declined response to expedite split-tender purchases. For POS transactions where a prepaid card is used, this feature gives the cardholder and the merchant the information needed to process a split-tender transaction. The merchant can submit another authorization request for the purchase using a lower amount that can be approved by the prepaid issuer, and ask the cardholder to provide another form of payment for the remaining purchase amount. The available balance returned in a declined response identifies the current account balance, without deducting the declined transaction amount.

Mastercard limits the account balance response to use on prepaid accounts and in ATM transactions. Mastercard advises issuers that they must not use the unsolicited account balance response for credit or debit accounts in POS transactions. Issuers that provide unsolicited credit or debit account balance information in POS transactions increase the potential for fraudulent activity and concerns for cardholder privacy.

The Authorization Platform forwards the account balance response provided by the issuer to the acquirer only when it is returned in an ATM transaction or in a POS transaction for a prepaid account. Issuers must not transmit balance information for credit or debit accounts, unless it is for an ATM transaction. Mastercard also will remove balance information from all Maestro® and Debit Mastercard® POS purchase transactions that are initiated with a debit card (not identified to be prepaid related).

All prepaid Debit Mastercard® issuers in the U.S. region must support account balance responses.

Prepaid Debit Mastercard card issuers must provide the cardholder's account balance information in DE 54 (Additional Amounts) of the Authorization Request Response/0110 message for approved and declined authorization responses.

NOTE: The available balance returned on an approved response is the prepaid account balance after the transaction amount has been deducted. The available balance on a declined response indicates the current account balance, without deducting the declined amount.

All acquirers in the U.S. region that support merchants within select card acceptor business codes (MCCs) must support account balance responses for transactions initiated at point-of-sale (POS) terminals for all prepaid Debit Mastercard account ranges. This requirement applies only to card present transactions occurring at attended terminals. For more information about effective dates for acquirers in the U.S. region to begin supporting partial approvals, full and partial reversals, and account balance by MCC, refer to Acquirer Mandate to Support Partial Approvals, Reversal Requests, and Account Balance Responses (U.S. Region Only).

Effective in 2020 with Release 20.Q2, issuers must support account balance response for prepaid card account ranges (Mastercard, Debit Mastercard, and Maestro). The acquirer of a merchant included in any of the MCCs listed in Effective Dates for Acquirer Mandate to Support Partial Approvals and Account Balance Responses Globally (for card present transactions conducted at attended terminals only) must support account balance responses for all prepaid card account ranges (Mastercard, Debit Mastercard, and Maestro). This mandate does not apply to issuers and acquirers in the United Kingdom. Mastercard reserves the right to expand the number of markets that may be required to support prior to 2020.

Account Data Compromise Information

Mastercard provides issuers with account data compromise (ADC) event information in authorization messages.

Authorization Processing

The following stages describe authorization processing for a transaction that contains a primary account number (PAN) with and without an ADC event match.

1. The acquirer sends an Authorization Request/0100 message containing the issuer PAN via the Mastercard Network.
2. The Authorization Platform searches the database for an ADC event match for that issuer PAN.
3. If an ADC event match is found, the Authorization Platform inserts the following values in the Authorization Request/0100 message:

   – DE 48 (Additional Data—Private Use), subelement 39 (Account Data Compromise Information) containing the account data compromise event information.

   DE 48, subelement 39 contains multiple pieces of information, including up to three case key codes (unique key to identify case).

   Case key codes can be used to locate the Mastercard Alerts Full Case ID associated with a particular ADC event (for example, MCAlert Full Case ID: MCA2101-US-09). In this example, the case key code in DE 48, subelement 39 is displayed in the following

format: 021019, which displays five positions for the alert number and the first digit of the year (right justify and pad string with spaces if needed).

– DE 48, subelement 71 (On-behalf Services), subfield 1 (On-behalf [OB] Service), value 25 (Account Data Compromise Information), subfield 2 (On-behalf [OB] Result 1), value Y (Compromised Event Data Found), and subfield 3 (On-behalf [OB] Result 2), space filled.

4. If an ADC event match is not found, the Authorization Platform inserts DE 48, subelement 71, subfield 1, value 25, subfield 2, value N (Compromised Event Data Not Found), and subfield 3, space filled in the Authorization Request/0100 message. DE 48, subelement 39 is not present in the Authorization Request/0100 message.
5. The Authorization Platform forwards the Authorization Request/0100 message to the issuer.
6. The issuer approves or declines the authorization request by sending an Authorization Request Response/0110 message to the Authorization Platform.

Authorization Reports

The Authorization Parameter Summary Report (SI737010-AA) includes an ADC Event (Account Data Compromise) participant parameter in the Global Parameters section. For a sample of the Authorization Parameter Summary Report (SI737010-AA), refer to Reports.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

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.

Account Management System

Account Management System (AMS) services include account-level services that issuers use to designate special handling during authorization. Issuers can list cardholder accounts as exception accounts that receive Stand-In or chargeback protection.

Issuers can identify accounts with a preferred status in Premium Listings, providing higher dollar and transaction limits for Stand-In processing; or identify accounts that participate in services such as Electronic Warning Bulletin, Payment Cancellation, Contactless Mapping Services, Mastercard In Control, Enhanced Value, Product Graduation, and High Value.

Stand-In Account File

The Stand-In Account File (MCC102) contains a list of negative accounts, restricted accounts, and preferred (Premium Listings) accounts.

The Stand-In Account File provides information about negative accounts, restricted accounts, and preferred (Premium Listing) accounts for Stand-In processing to use when making an authorization decision on behalf of the issuer.

Issuers list the following types of accounts in the Stand-In Account File:

- Premium Listings that designate higher authorization limits for preferred cardholders
- Negative accounts that require a Stand-In authorization response of decline, refer to card issuer, or capture card for lost, stolen, fraud or accounts with credit issues
- Electronic Warning Bulletin listings for lost, stolen, fraudulent accounts, which are distributed daily to all acquirers available from AMS

Electronic Warning Bulletin File

The Electronic Warning Bulletin File (MCC103) allows issuers to define specific accounts for special handling, such as exception accounts that should be declined when listed in the Electronic Warning Bulletin (EWB).

AMS allows customers to identify and manage restricted accounts. AMS collects and distributes Mastercard restricted account listings in the Electronic Warning Bulletin File for use in authorization processing.

Generally, issuers list the following kinds of accounts in AMS:

- Lost
- Stolen
- Counterfeit
- Severe credit problems with continued activity

Listing in AMS provides issuers with the following benefits:

- Warning bulletin chargeback rights
- Capture-card response for Stand-In and X-Code processing

Local Stoplist File

The Local Stoplist File (MCC104) allows participating issuers to list exception accounts at the country and subcountry levels (such as merchant category).

This gives issuers the opportunity to select the geographical area covered by each listing to target the specific fraud problem.

- The country level listing allows issuers to list in a single country.
- The subcountry level listing allows issuers to list in a defined area such as a card acceptor business code (MCC) within a country.

Payment Cancellation File

The Payment Cancellation File (MCC105) supports Payment Cancellation for card-not-present and recurring payment transactions.

Payment Cancellation allows issuers to specify criteria to block card-not-present and recurring payment transactions identified in authorization messages and clearing records.

PAN Mapping File

The PAN Mapping File (MCC106) supports certain services.

Contactless Mapping Service

The Contactless Mapping Service leverages the PAN Mapping File (MCC106). MCC106 contains the service-eligible contactless account number and the associated cardholder PAN. Each contactless account number is unique and several contactless account numbers can be associated with a single PAN (a family with the same PAN can have multiple contactless cards or devices).

The Contactless Mapping Service is not available to issuers that support the use of online PIN with a card or device product. If PAN mapping is performed in a transaction using online PIN, the PIN validation will fail.

Mastercard supports listing accounts for MCC106 with AMS using the following methods:

- Online File Maintenance
- Bulk File Maintenance
- Mastercard eService Maintenance
- Mastercard web services

MCC106 maintenance requests submitted via the Issuer File Update Request/0302 message, Mastercard eService, or Mastercard web services are applied immediately. Maintenance requests submitted by bulk file are applied two times per day at 08:00 and 18:00 hours (St. Louis time).

Mastercard Enhanced Value File

Mastercard Enhanced Value (MCC107) supports differentiated interchange for cards registered with a specific level of rewards. MCC107 supports certain account registration files.

- Consumer Enhanced Value
- Consumer High Spend in Canada
- Premium High Spend in Canada

For detailed information, refer to the *Account Level Management User Manual*.

Mastercard Product Graduation File

Mastercard Product Graduation (MCC108) supports the migration of cardholders to different card products without changing the primary account number (for example, an issuer upgrades a Gold Mastercard® card to a World Mastercard™ card; the account is now recognized by the MCW product code and not the Gold BIN).

For detailed information, refer to the *Account Level Management User Manual*.

Mastercard High Value

Mastercard World High Value is an optional service for issuers with World Mastercard® card programs (MCW), enabling differentiated interchange on cards meeting or exceeding a specific level of spend per card annually. Mastercard monitors the card spend on behalf of the participating issuers and registers those qualifying cards for World High Value processing quarterly. This service is not available in all regions. Refer to the *Account Level Management User Manual* for additional details.

Contactless Application Transaction Counter File

The Contactless Application Transaction Counter (ATC) File (MCC109) contains the most recent ATC values for contactless cards or devices that were personalized using dynamic values in the ATC and unpredictable number (UN).

Issuers participating in the CVC 3 Validation in Stand-In Service or in the CVC 3 Pre-validation Service may provide this file to Mastercard.

Blocking Ranges of Accounts

Mastercard provides customers two ways to list account ranges to stop the acceptance of a range of cards.

The following table explains how to create two types of blocked listings.

Type of Listing	How to List	Where it Goes
Group or Series	The issuer requests the Group or Series in writing.	Mastercard adds the listing to AMS.
Range Block	The issuer establishes the range block on the Stand-In Processing Worksheet.	Mastercard adds the listing to the Account File.

The following table compares the levels of protection provided by the listing types.

Type of Listing	Levels of Protection			
	Stand-In	X-Code	Under Merchant Floor Limit	Chargeback Rights under Reason Code 4807
Group or Series	Yes	Yes	Yes	Only in catastrophic situations when approved by Mastercard
Range Block	Yes	Yes	No	No

For More Information

For more information about AMS and AMS services, refer to the *Account Management System User Manual*.

For more information about blocking ranges, refer to Stand-In Processing and Setting Stand-In Parameters.

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.

WHEN...	THEN the Authorization Platform...
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.

Data Element	Value	Comment
DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	28	Payment

Data Element	Value	Comment
DE 4 (Amount, Transaction)	Equal to or greater than 0	Equal to or greater than zero
DE 48 (Additional Data—Private Use), subelement 77 (Transaction Type Identifier)	C01, C02, C03, C04, C05, C06, C09	
DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service Request)	52	Optional AVS
DE 48 (Additional Data—Private Use), subelement 92 (CVC 2)	CVC 2	Optional CVC 2
DE 61 (Point-of-Service [POS] Data), subfield 7 (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 *MoneySend Program Guide*.
DE 18 (Merchant Type)	MCC 6536 (MoneySend Intracountry) MCC 6537 (MoneySend Intercountry)	

Data Element	Value	Comment
DE 48 (Additional Data—Private Use), subelement 77 (Transaction Type Identifier)	C07 (MoneySend Person-to-Person)	MoneySend Transaction Type Identifier
	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)	
	C65 (MoneySend Business to Business Transfer)	
	F07 (P2P Transfer)	
	F52 (Account-to-Account Transfer)	
	F53 (Agent Cash Out)	
	F54 (Credit Account Bill Payment)	
	F61 (Staged Wallet Load)	
	F64 (Prepaid/Debit Card Account Load)	
DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service Request)	52 (AVS and Authorization Request/0100)	Optional AVS

Data Element	Value	Comment
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 *MoneySend Program Guide*.

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 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 Account Level Management.

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.

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) 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.

Address Verification Service

The Address Verification Service (AVS) is a service for online customers that verifies the cardholder's billing address. This service protects against the fraudulent use of cards in non–face-to-face transactions.

Participation Requirements

You must have online access to participate in AVS.

IF the customer…	AND is located…	THEN participation is…
Issues cards	In the U.S. and Canada regions	Required

IF the customer…	AND is located…	THEN participation is…
Issues cards	In a region other than the U.S. that supports AVS use for the region	Optional, unless mandated by local country

Indicating AVS Participation During Sign-in

When the issuer signs into the Mastercard Network, the issuer can choose AVS participation options.

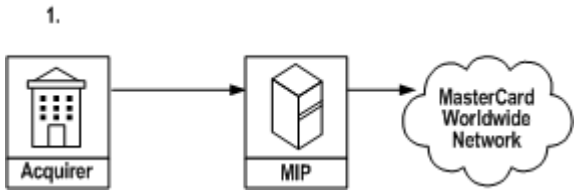
- Indicate that it does not participate in AVS using AVS Service Indicator 0
- Receive AVS data in non-condensed format using AVS Service Indicator 1
- Receive AVS data in condensed format using AVS Service Indicator 2
- Receive AVS data in condensed format using AVS Service Indicator 3
- Receive AVS data in condensed format using AVS Service Indicator 4

For more information about signing on to the Mastercard Network, refer to Online Authorization Messages.

AVS Process

Stages of the AVS transaction process.

1. The acquirer generates an Authorization Request/0100 message with non-condensed address data included in DE 120 (Record Data). When submitting AVS requests, the Authorization Request/0100 message should always contain DE 120, subfield 01 (AVS Service Indicator 1).



2. The issuer MIP applies an algorithm to construct the address key, which the issuer uses to verify the address.

3. The issuer host compares the address key in DE 120 to the address key in the issuer database.

4. The issuer generates an Authorization Request Response/0110 message with the AVS response included in DE 48 (Additional Data—Private Use), subelement 83 (Address Verification Service Response).

Address Key

The address key is the part of the Authorization Request/0100 message that contains the address data.

To achieve a complete match, the key that AVS sends in DE 120 (Record Data) must be the same as the key in the issuer's database. The address key consists of the following subelements in DE 120:

- Cardholder postal/ZIP code
- Cardholder address (condensed or non-condensed)

Cardholder Postal/ZIP Code

The cardholder postal/ZIP code has a fixed length of 9 bytes.

Using AVS Service Indicator 4, AVS will condense the cardholder postal/ZIP code to contain only numeric values, with a maximum of nine values.

NOTE: Issuers of Mastercard and Debit Mastercard cards in the Canada region must support the validation of Canadian postal codes in a U.S. ZIP code format to facilitate AVS checking at U.S. AFDs. The required format involves input of the three numeric digits of the cardholder postal code, followed by two trailing zeros to match the required ZIP code format. For example, L7M 1W9 would be entered by the cardholder as 71900. As postal codes are communicated in DE 120 (Record Data), subelement 3 (AVS Usage) in a nine-position format, L7M 1W9 would be formatted as 71900bbbb, where b is blanks or spaces.

Cardholder Address

The length of the cardholder address depends on whether it is condensed or non-condensed.

Non-condensed Using AVS Service Indicator 1—A non-condensed cardholder address includes the address data exactly as the acquirer provides it in DE 120. A non-condensed address key includes both the cardholder postal/ZIP code and the cardholder address data exactly as the acquirer provided them in DE 120.

The Authorization Platform will not truncate the address data passed from the acquirer if greater than 29 positions. DE 120 is an LLLVAR field; therefore, it will indicate the length of the data being passed.

NOTE: Some merchants or acquirers currently are limited to supporting only numeric data.

Condensed Using AVS Service Indicator 2—A condensed cardholder address using AVS Service Indicator 2 includes the first five numeric values at the beginning of the cardholder address (when scanning the address from left to right) provided by the acquirer in DE 120.

The condensed address key (cardholder postal/ZIP code plus cardholder address) is a fixed length of 14 bytes. It includes the entire cardholder postal/ZIP code and the condensed cardholder address. Mastercard left-justifies and blank-fills both portions of the key, as needed.

Stages of the process to condense the address key:

1. The condensing algorithm begins condensing with the numeric value in the left-most position.
2. The algorithm extracts the first five numeric values of the cardholder address (when scanning the address from left to right).

   The condensing algorithm ignores all special characters (such as hyphens [-], slashes [/ or \], and number signs [#]).
3. AVS constructs the condensed AVS key.

Condensed Using AVS Service Indicator 3—A condensed cardholder address includes as many as five numeric values at the beginning of the cardholder address provided by the acquirer in DE 120.

The condensed address key (cardholder postal/ZIP code plus cardholder address) is a fixed length of 14 bytes. It includes the entire cardholder postal/ZIP code and the condensed cardholder address. Mastercard left-justifies and blank-fills both portions of the key, as needed.

Stages of the process to condense the address key:

1. The condensing algorithm begins condensing with the numeric value in the left-most position.
2. The algorithm extracts up to five numeric values that appear before the first alphabetic character or space. The condensing algorithm:
   - Ignores all special characters (such as hyphens [-], slashes [/ or \], and number signs [#])
   - Excludes the portions of the address that could be open to misinterpretation, such as apartment numbers

3. When AVS finds a space or an alphabetic character, it stops examining the cardholder billing address.
4. AVS constructs the condensed AVS key.

Condensed Using AVS Service Indicator 4—A condensed cardholder address using AVS Service Indicator 4 includes only the numeric values in the cardholder postal/ZIP code (with a maximum of nine values), as well as the first five numeric values in the cardholder address received (when scanning the address from left to right) before forwarding the message to the issuer.

Stages of the process to condense the post/ZIP code and address data:

1. The condensing algorithm begins condensing with the numeric value in the left-most position.
2. The algorithm extracts up to nine numeric values in the cardholder postal/ZIP code and up to five numeric values in cardholder address (when scanning the address from left to right). The condensing algorithm ignores all special characters (such as hyphens [-], slashes [/ or \], and number signs [#])
3. AVS constructs the condensed AVS key.

Non-condensed versus Condensed

The following table provides an example of a non-condensed address key compared to a condensed address key.

Non-condensed	Condensed Using AVS Service Indicator 2	Condensed Using AVS Service Indicator 3	Condensed Using AVS Service Indicator 4
4J235 1520 Main Street, Apartment 3	4J235 _ _ _ _ 15203	4J235 _ _ _ _ 1520	4235 _ _ _ _ 15203

Example 1—Complete Match

The cardholder billing address is 1520 Main Street, Apartment 3. The issuer is using a condensed address key using AVS Service Indicator 3.

The cardholder neglects to provide the merchant with the apartment number 3, so the merchant omits the apartment number from the AVS request. However, the matching algorithm still finds a complete match.

Merchant enters...				
Postal/ZIP Code	Cardholder Address	AVS Address Key	Issuer's Address Key	Result/Explanation

Merchant enters...				
63110	1520 Main Street	63110_ _ _ _ 1520	63110_ _ _ _ 1520	Complete Match The issuer builds its address key based on the AVS algorithm. Both the issuer's address key and the AVS algorithm extract only the numeric values that precede the first space in this example (1520). Therefore, when the merchant does not enter the apartment number, this still results in a complete AVS match.

Example 2—No Match

The cardholder's address is 54 East Street; however, the cardholder provides the merchant with the address of 59 East Street.

Merchant enters...				
Postal/ZIP Code	Cardholder Address	AVS Address Key	Issuer's Address Key	Result/Explanation
63110	59 East Street	63110_ _ _ _ 59 _ _ _	63110_ _ _ _ 54_ _ _	No Match The issuer's address key does not match the cardholder address given by the cardholder.

Issuer Procedures

Stages of the process that issuers follow to receive and respond to AVS requests.

1. The issuer signs on to the Authorization Platform using a Sign-In Request/0800 message.

IF the issuer receives...	THEN the issuer signs on with value...
Non-condensed AVS data	1 in DE 94, byte 3.
Condensed AVS data using AVS Service Indicator 2	2 in DE 94, byte 3.
Condensed AVS data using AVS Service Indicator 3	3 in DE 94, byte 3.

IF the issuer receives…	THEN the issuer signs on with value…
Condensed AVS data using AVS Service Indicator 4	4 in DE 94, byte 3.
For customers using group sign-in, the value chosen applies to all BINs in the group.	

2. When the issuer receives an AVS request, the issuer verifies the cardholder billing address, matching it against the issuer's address file.
3. The issuer generates an Authorization Request Response/0110 that includes the AVS response (and an authorization response, if the AVS request accompanied an authorization request).

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

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:

- Non-Europe acquired ATM Bill Payment transactions
- Europe-acquired ATM Bill Payment transactions

Non-Europe Acquired ATM Bill Payment Processing

The ATM Bill Payment service allows cardholders to use their Mastercard® credit card or Debit Mastercard® card at any ATM to pay utilities and other bills when the service is supported domestically.

Stages describing authorization processing when a cardholder requests an ATM Bill Payment transaction:

1. The service is initiated by the cardholder at an ATM with a need to pay a bill (for example, electric bill, cable bill, phone bill).
2. The cardholder inputs biller account information, including the ATM bill pay code to identify the biller company, and then submits the bill pay request.
3. The ATM acquirer submits the payment request as a POS transaction to the Single Message System in a Financial Transaction Request/0200 message containing:
   - DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 00 (Purchase)
   - DE 18 (Merchant Type) with a MCC data value 6539 (Funding Transaction [Excluding MoneySend]). MCC 6539 is limited for use only in certain countries where the service is supported domestically.

- DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level Indicator), with one of the following values:
  - 1 (Authorized Level 1 CAT: automated dispensing machine with PIN)
  - 2 (Authorized Level 2 CAT: self service terminal)
- DE 124 (Member Defined Data) contains details relating to the bill being paid (optional)

4. The Single Message System converts the Financial Transaction Request/0200 message, and then forwards an Authorization Request/0100 message via the Mastercard Network to the issuer.
5. The issuer sends the Authorization Request Response/0110 message back to the Single Message System via the Mastercard Network.
6. The Single Message System converts the Authorization Request Response/0110 message, and then sends a Financial Transaction Request Response/0210 message to the ATM acquirer.
7. The Single Message System forwards the Financial Transaction Request Response/0210 message to the acquirer. The acquirer provides a receipt to the cardholder that contains the bill payment information (such as amount paid, date paid, and ATM bill pay code).
8. The acquirer initiates the bill paying process, paying funds directly to the biller (such as electric company, phone company).
9. The cardholder sees the bill payment transaction in his or her monthly bankcard statement.

Non-Europe acquired ATM Bill Payment transactions are not processed by the Stand-In System or X-Code System. Transactions are declined using the Authorization Request Response/0110 message containing DE 39 (Response Code), value 91 (Authorization System or issuer system inoperative).

Europe-Acquired ATM Bill Payment Processing

The ATM Bill Payment service allows cardholders to use their Mastercard®, Debit Mastercard®, Cirrus®, or Maestro® card at any ATM to pay utilities and other bills where the service is supported domestically for the Europe region.

Stages describing authorization processing when a cardholder requests an ATM Bill Payment transactions:

1. The service is initiated by the cardholder at an ATM with a need to pay a bill (for example, electric bill, cable bill, phone bill).
2. The cardholder inputs biller account information, including the ATM bill pay code to identify the biller company, and then submits the bill pay request.
3. The ATM acquirer submits the payment request as a POS transaction to Authorization Request/0100 message containing:
   - DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 00 (Purchase)
   - DE 18 (Merchant Type) with MCC data 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 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level Indicator), value 1 (Authorized Level 1 CAT: automated dispensing machine with PIN)
   - DE 124 (Member Defined Data) contains details relating to the bill being paid (optional)
4. The Authorization Platform forwards the Authorization Request/0100 message to the issuer.
5. The issuer sends the Authorization Request Response/0110 message to the acquirer.
6. The acquirer provides a receipt to the cardholder that contains the bill payment information (such as amount paid, date paid, ATM bill pay code).
7. The acquirer initiates the bill paying process, paying funds directly to the biller (such as electric company, phone company).
8. The cardholder sees the bill payment transaction in his or her monthly bankcard statement.

To Participate

Contact your regional office for information about implementation of the ATM Bill Payment service for your local market.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

ATM Credit Card Cash Advance in Installments

The ATM Credit Card Cash Advance in Installments service supports installment payments on Mastercard® credit card cash advance transactions performed at the ATM.

This service allows a cardholder 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). 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 and provide the ability to print the issuer's installment payment details on the ATM receipt. Issuers that process domestic ATM transactions may optionally support this service unless mandated by country regulations.

The ATM Credit Card Cash Advance in Installments service is available to only be acquired as single message transactions. The ATM Credit Card Cash Advance in Installments service is not available to ATM acquirers in the Europe region.

This service is optional for issuers that process domestic ATM transactions on the Dual Message System, unless mandated by country regulations.

Credit Card Cash Advance Installment Payment Transaction Processing

Credit card cash advance installment payment transactions consist of two transaction types: ATM installment inquiry and ATM installment withdrawal.

ATM Installment Inquiry

The ATM installment inquiry occurs when the cardholder requests a cash advance amount with an installment period for repayment.

Stages describing ATM installment inquiry authorization processing:

1. The cardholder requests an ATM cash advance transaction and selects an installment option for repayment.
2. The acquirer sends an ATM installment inquiry to the Single Message System as a Financial Transaction Request/0200 message.
3. The Single Message System converts the Financial Transaction Request/0200 message to an Authorization Request/0100 message, and then forwards the message to the Authorization Platform for processing.
4. The Authorization Platform forwards the installment inquiry to the issuer for approval.
5. The issuer accepts the cardholder's request, declines the request and proposes an alternate installment schedule, or declines the request. The issuer responds with an Authorization Request Response/0110 message indicating the terms and conditions of the installment payment.
   - If the issuer does not accept the cardholder's requested number of installments, but proposes an alternate installment schedule, DE 39 (Response Code) will contain value 00 (Approved or completed successfully).
   - If the issuer does not accept the requested terms or offer alternative terms, DE 39 will contain the issuer's choice of decline response, such as 05 (Do not honor).
6. The Authorization Platform forwards the Authorization Request Response/0110 message to the Single Message System.
7. The Single Message System converts the Authorization Request Response/0110 message to a Financial Transaction Request Response/0210 message, and then forwards the message to the acquirer.
8. The acquirer displays the issuer's terms and conditions on the ATM receipt.
9. The cardholder accepts or rejects the terms. If the cardholder accepts the terms, the cardholder can request withdrawal of the funds; otherwise, the transaction is canceled.

ATM Installment Withdrawal

Once a cardholder approves the terms and conditions of the issuer's installment payments, the acquirer initiates an ATM installment withdrawal transaction.

Stages describing ATM installment withdrawal authorization processing:

1. The acquirer sends an ATM installment withdrawal request to the Single Message System as a Financial Transaction Request/0200 message.
2. The Single Message System converts the Financial Transaction Request/0200 message to an Authorization Request/0100 message, and then forwards the message to the Authorization Platform for processing.
3. The issuer approves the request and responds with an Authorization Request Response/0110 message.
4. The Authorization Platform forwards the Authorization Request Response/0110 message to the Single Message System for processing.
5. The Single Message System converts the Authorization Request Response/0110 message to a Financial Transaction Request Response/0210 message, and then forwards the message to the acquirer.
6. The cardholder receives the funds and a copy of the terms and conditions is printed on the ATM receipt.

Alternate Processing

ATM Credit Card Cash Advance in Installments services are not processed by the Stand-In System or X-Code System. Transactions are declined using the Authorization Request Response/0110 message containing DE 39 (Response Code), value 91 (Authorization System or Issuer System inoperative).

To Participate

Contact your regional office for information about implementation of the ATM Credit Card Cash Advance in Installments services for your local market.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Authorization and Preauthorization Processing Standards

All authorizations initiated at Europe region and Middle East/Africa region card acceptors 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.

Benefits

Mastercard introduced a number of authorization improvements to achieve the following objectives:

- Enable a more accurate and transparent management of the card account's open-to-buy in order to improve cardholder satisfaction and address regulatory concerns with the current situation

- Redefine the issuer payment guarantee that is engaged when authorizing a transaction by introducing a maximum time limit in place of the currently unlimited duration and by defining it based on characteristics of the authorization or preauthorization request
- Permit acquirers and issuers to identify and clearly distinguish a preauthorization from a final authorization, thus giving them the option to treat them differently, to the ultimate benefit of their cardholders

Final Authorization Message Processing Standard

The process for evaluating Dual Message System (Authorization) acquirer compliance with the processing standards for final authorizations has been modified to support allowing final authorizations to be cleared within seven calendar days of the authorization date. Modification to this processing standard impacts compliance analysis for final authorizations acquired globally and undefined authorizations acquired in the Europe and Middle East/Africa regions.

Final authorizations not meeting the seven calendar day clearing requirement will be flagged as non-compliant. 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. 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 additional information, refer to the Authorization Processing Integrity Acquirer Detail Report (AB605010-AA and AB605010-FF) in the Reports chapter.

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 final authorizations and 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 (for example, the room-rate plus 15 percent).

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 will no longer benefit from the 15 percent tolerance between the authorized amount and the clearing amount for Mastercard transactions. In addition, Mastercard transactions that are chip/PIN, contactless, or card-not-present no longer benefit from the 20 percent tolerance between authorization and clearing for gratuities, unless otherwise stated below.

The 20 percent tolerance for gratuities continues to be available for card present transactions that are neither chip/PIN nor contactless and provided that the authorization is coded as a preauthorization, or where permitted, an undefined authorization.

Where these tolerances are eliminated, issuers must ensure 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.

The rule for amount tolerance between authorization amount and clearing amount with respect to gratuities is applied as follows.

The transaction amount must not exceed the authorized amount of the purpose of adding a gratuity, and any gratuity must be included in the authorization request if:

- The transaction is a card-not-present or 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 CVM

In all other scenarios (for example, gratuities on chip/PIN transactions and provision for incidentals), 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.

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 days for Mastercard authorizations properly coded as preauthorizations and is seven 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 days; only limits the maximum duration of any such hold to a maximum duration of 30 or 7 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 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 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.

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 are 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 are used to extend only the chargeback protection period associated with the original preauthorization (this supersedes the former process which required submitting a nominal amount [0.01]).

If the issuer declines the chargeback extension request and the original extension subsequently expires, the acquirer must request a new authorization.

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 (formerly Mastercard® *PayPass*™) 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), 54 (Expired Card), etc.

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 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.

NOTE: Several other options may be used when the authorization life cycle expires before the transaction is finalized:

- **Submit a new preauthorization within 30 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 days before).**
- **Use the Advance Resort Deposit process as described in section D.2 of the *Chargeback Guide* to authorize and clear the transaction at the time of the reservation.**

Authorization and Preauthorization Processing

Clear and reliable identification of authorizations provides better information about the nature of each authorization and allows issuers to optionally apply different processing to different types of authorizations, ultimately benefiting cardholders.

An authorization for an amount greater than zero at card acceptors in Asia/Pacific, Canada, Latin America and Caribbean, and United States regions may be coded as a preauthorization, final authorization, or undefined authorization in line with the following requirements. Authorizations at card acceptors in Europe and Middle East/Africa must be coded as either preauthorization or final authorization in line with the following requirements.

Final authorization processing is mandated for transactions initiated at card acceptors in the Europe region that enables issuers globally to distinguish a final authorization from a preauthorization.

NOTE: Refer to the Scenarios section for detailed scenarios for preauthorization, final authorization, undefined authorization, and chargeback extension request.

Preauthorization, Final Authorization, and Undefined Authorization Transactions

An authorization for an amount greater than zero must be identified as either preauthorization, final authorization, or undefined authorization, using the requirements listed here.

Preauthorization

An authorization for an amount greater than zero should be coded as a preauthorization if it meets one of the following three conditions:

- Authorization is requested for an estimated amount.

- The requested amount of the original authorization may be adjusted if the final Transaction Amount (amount submitted for clearing) is greater than the original amount requested.
- The transaction might not be completed for reasons other than technical failure or lack of full issuer approval. For example, the transaction might not be completed when the cardholder will be offered the choice to complete the transaction with another payment means at a later time (such as, when checking out of a hotel or returning a rental car) or when the goods ordered by the cardholder might be later found to be out of stock. The risk of technical failures such as telecommunications failure or terminal failure should not be taken into account to determine if an authorization must be coded as a preauthorization.

The authorization request is properly identified as a preauthorization when DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains value 4. Acquirers must submit the clearing presentment for a Transaction approved as a preauthorization within 30 calendar days of the latest authorization date (preauthorization or incremental authorization) in order to ensure chargeback protection provided by chargeback message reason code 4808—Authorization-Related Chargeback.

Acquirers in the Asia Pacific, Canada, Latin America and Caribbean, Middle East/Africa, and United States regions that do not reverse or clear approved preauthorizations within 30 calendar days of the original preauthorization date will be considered non-compliant with preauthorization processing standards. Non-compliant transactions will be reported on the Authorization Processing Integrity Acquirer Detail report. After the monitoring and reporting period ends, non-compliant preauthorizations will be subject to a non-compliance fee.

Preauthorization Scenarios

The following scenarios are examples in which card acceptors can use a preauthorization to benefit from its greater processing flexibility or from its more generous payment guarantee terms.

NOTE: Refer to the Scenarios section for detailed scenarios for preauthorization, final authorization, undefined authorization, and chargeback extension request.

- A hotel wants to obtain a payment guarantee at check-in for the room rate, plus a provision for possible additional expenses related to the minibar or breakfast—the hotel uses a preauthorization because it supports estimated amounts.
- Another hotel wants to obtain a payment guarantee at check-in for a hotel stay of 10 days—the hotel uses a preauthorization because the associated payment guarantee is valid for up to 30 days and the clearing presentment will take longer than seven calendar days.
- An airline wants to obtain a payment guarantee at flight-booking time for certain types of flights where the ticket may take several days to issue—the airline uses a preauthorization because the associated payment guarantee is valid for up to 30 days and the clearing presentment may take longer than seven calendar days.
- An e-commerce merchant wants to obtain a payment guarantee at order time, before it can confirm that the goods are actually available in stock—the merchant uses a preauthorization because the transaction may still be canceled if the goods are later found to be out of stock.

- Another e-commerce merchant wants to obtain a payment guarantee at order time but the items ordered may take several days to ship—the merchant uses a preauthorization because the associated payment guarantee is valid for up to 30 days and the clearing presentment may take longer than seven calendar days.

NOTE: Maestro preauthorizations are permitted only for automated fuel dispenser (AFD), Maestro contactless transit aggregated, and card-not-present (CNP) transactions.

Final Authorization

An authorization for an amount greater than zero should be coded as a final authorization if it meets the following conditions:

- Authorization is requested for the final Transaction Amount that is expected to be presented for clearing.
- The transaction is not expected to be canceled after the authorization request is approved in full (excluding non-completion for reasons of technical failure). The risk of technical failures such as telecommunications failure or terminal failure should not be taken into account to determine if an authorization must be coded as a final authorization.

Any transaction corresponding to an authorization identified as a final authorization must be presented for clearing within seven calendar days of the authorization approval date.

The 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 (Normal Request) and DE 48 (Additional Data—Private Use), subelement 61 (POS Data Extended Condition Codes), subfield 5 (Final Authorization Indicator) contains value 1 (Final Authorization). Acquirers must submit the clearing presentment for a Transaction approved as a final authorization within seven calendar days of the authorization date in order to ensure chargeback protection provided by chargeback message reason code 4808—Authorization-Related Chargeback.

Acquirers in Europe or Middle East/Africa regions that reverse an approved final authorization or do not clear an approved final authorization within seven calendar days of the authorization date or clear for a different currency or transaction amount than what was authorized will be considered non-compliant with final authorization processing standards. Acquirers in Asia Pacific, Canada, Latin America and the Caribbean, or United States regions that do not clear an approved final authorization within seven calendar days of the authorization date or clear for a different currency or transaction amount than what was authorized will be considered non-compliant with final authorization processing standards. Non-compliant transactions will be reported on the Authorization Processing Integrity Acquirer Detail report. Non-compliant final authorizations will be subject to a non-compliance fee.

In the Europe and Middle East/Africa regions, non-compliant final authorizations will be subject to a non-compliance fee if more than one percent of Final Authorizations do not meet their requirements for a given acquirer parent ICA or MCE Group ICA over the weekly billing period. If the one percent threshold is not breached, all Final Authorizations that do not meet their requirements will not be assessed a fee.

NOTE: Acquirers outside of the Europe and Middle East/Africa regions may optionally submit final authorizations, but must comply with requirements of clearing for the amount and currency authorized, and within seven calendar days if they choose to do so.

Undefined Authorization

An authorization for an amount greater than zero should be coded as an undefined authorization if it meets the following conditions:

- The final Transaction Amount may differ from the authorized amount.
- The transaction is not expected to be canceled after the authorization request is approved in full (excluding non-completion for reasons of technical failure). The risk of technical failures such as telecommunications failure or terminal failure should not be taken into account to determine authorization message coding.

The authorization request is properly identified as an undefined authorization when DE 61, subfield 7 contains value 0, and DE 48, subelement 61, subfield 5 contains value 0, or is not present. Acquirers must submit the clearing presentment for a transaction approved as an undefined authorization within seven calendar days of the authorization date in order to ensure chargeback protection provided by chargeback message reason code 4808—Authorization-Related Chargeback.

An approved undefined authorization submitted by an acquirer in the Asia Pacific, Canada, Latin America and Caribbean, or United States region that is not reversed or cleared within seven calendar days of the original authorization date will be considered non-compliant with undefined authorization processing standards. Non-compliant transactions will be reported on the Authorization Processing Integrity Acquirer Detail report and the non-compliant undefined authorizations will be subject to a non-compliance fee.

Acquirers in the Europe and Middle East/Africa regions must no longer code authorizations as undefined. An authorization must be coded either as preauthorization or final authorization. Non-compliant transactions will be reported on the Authorization Processing Integrity Acquirer Detail report and the non-compliant undefined authorizations will be subject to a non-compliance fee.

Scenarios

The following are common processing scenarios for preauthorizations, final authorizations, and undefined authorizations assuming reversal or clearing occurs prior to the authorization message chargeback expiration date.

NOTE: For each authorization type if the authorization completes after the chargeback expiration date and a chargeback extension has not been requested and approved, the acquirer must either submit a new authorization request for the completed transaction amount prior to clearing or submit the transaction for clearing without processing a new authorization and risk potential chargeback for Reason 4808 (Authorization-Related Chargeback). A sample scenario has also been provided for chargeback extension request message processing.

Preauthorization

Scenario P1: Clearing Amount Matches Preauthorization Amount

The cardholder checks into a hotel on 1 October, and the merchant submits a preauthorization for estimated charges up to USD 1,000. The cardholder checks out of the hotel on 5 October with no further charges applied to his/her bill during the stay. The acquirer submits a clearing presentment based on notification from the merchant of preauthorization completion for the full authorized amount.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	4 NA	USD 1,000	1001 MCG123456					USD 1,000
Clear 1240 5 Oct						USD 1,000	MCG123456 1001	USD 0

Scenario P2: Clearing Amount below Preauthorization Amount

The cardholder checks into a hotel on 1 October, and the merchant submits a preauthorization for estimated charges up to USD 1,000. The cardholder checks out of the hotel one day early. Final bill amount upon cardholder checkout is USD 900.

P2.A: The acquirer submits a clearing presentment within 24 hours of notification from the merchant of preauthorization completion.

Merchant/ Acquirer			Authorization				Clearing	Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	4 NA	USD 1,000	1001 MCG123456					USD 1,000
Clear 1240 4 Oct						USD 900	MCG123456 1001	USD 0

P2.B: The acquirer submits partial reversal when notified by the merchant of preauthorization completion for lower than authorized amount, and clearing will not occur within 24 hours of merchant preauthorization completion notification.

Merchant/ Acquirer			Authorization				Clearing	Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	4 NA	USD 1,000	1001 MCG123456					USD 1,000
Rvrsl 0400 4 Oct	4 NA	USD 1,000	1004 MCG56789	MCG123456 1001	USD 900			USD 900

Merchant/ Acquirer	Authorization		Clearing		Issuer
Clear 1240 6 Oct			USD 900	MCG123456 1001	USD 0

Scenario P3: Preauthorization Completes for Higher Amount than Authorized (Incremental Preauthorization)

The cardholder checks into a hotel on 1 October, and the merchant submits a preauthorization for estimated charges up to USD 1,000. The cardholder accrues additional USD 500 in charges. The final bill amount upon cardholder checkout is USD 1,500. The merchant submits an incremental preauthorization for the additional charges of USD 500 and notifies the acquirer of preauthorization completion of USD 1,500. The acquirer submits a clearing presentment based on notification from the merchant of preauthorization completion.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	4 NA	USD 1,000	1001 MCG123456					USD 1,000
Incr. 0100 5 Oct	4 NA	USD 500	1005 MCG567890	MCG123456 1001				USD 1,500
Clear 1240 5 Oct						USD 1,500	MCG123456 1001	USD 0

Scenario P4: Preauthorization Cancellation

The cardholder checks into a hotel on 1 October, and the merchant submits a preauthorization for estimated charges up to USD 1,000. At checkout, the cardholder pays the final bill with a different card.

The merchant notifies the acquirer of the full reversal. The acquirer submits the reversal upon the merchant preauthorization cancellation notification.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth Card 1 0100 1 Oct	4 NA	USD 1,000	1001 MCG123456					USD 1,000
Rvrsl Card 1 0400 5 Oct	4 NA	USD 1,000	1004 MCG567890	MCG123456 1001				USD 0
Auth Card 2 0100 5 Oct	0 1 (Final Auth)	USD 1,000	1005 MCP654321					USD 1,000

Scenario P5: Preauthorization with Installment Payments

P5.A: Installment payment terms are approved with original preauthorization (that is, at time of reservation or check-in). Installment payment terms do not change at time of transaction completion. The cardholder checks into a hotel on 1 October, and the merchant submits a preauthorization for estimated charges up to USD 1,000. A preauthorization request also includes merchant installment program ID and installment payment terms in DE 48, subelement 95 and DE 112 for the cardholder to pay in five monthly payments of USD 200,

which are approved by the issuer. The cardholder checks out of the hotel on 5 October with no further charges applied to his/her bill during the stay and original installment payment terms remain unchanged from original approved authorization. The acquirer submits a clearing presentment for first installment payment based on notification from the merchant of preauthorization completion for the full authorized amount.

Merchant/ Acquirer			**Authorization**			**Clearing**		**Issuer**
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	4 NA	USD 1,000	1001 MCG123456					USD 1,000
Clear 1240 5 Oct						USD 200	MCG123456 1001	USD 0

P5.B: Installment payment terms are approved with original preauthorization (that is, at time of reservation or check-in). The terms change at the time of transaction completion.

The cardholder checks into a hotel on 1 October, and the merchant submits a preauthorization for estimated charges up to USD 1,000. Preauthorization also includes merchant installment program ID and terms in DE 48, subelement 95 and DE 112 for the cardholder to pay in five monthly payments of USD 200, which are approved by the issuer. The cardholder checks out of the hotel on 5 October with no further charges applied to his/her bill during the stay, but the original installment payment terms change to four monthly payments for USD 250. Due to the installment payment term change, the original authorization with the original installment payment terms must first be reversed, and a new authorization processed with the new terms for approval. Once the new authorization is approved, clearing can occur for the first installment payment amount.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	4 NA	USD 1,000	1001 MCG123456					USD 1,000
Rvrsl 0400 5 Oct	4 NA	USD 1,000	1004 MCG567890	MCG123456 1001				USD 0
Auth 0100 5 Oct	0 0 (Undef Auth)	USD 1,000	1005 MCP654321					USD 1,000
Clear 1240 5 Oct						USD 250	MCP654321 1005	USD 750

P5.C: Installment payment terms are not included with original preauthorization (that is, at time of reservation or check-in). Installment payment terms are added at the time of transaction completion.

The cardholder checks into a hotel on 1 October, and the merchant submits a preauthorization for estimated charges up to USD 1,000. The option to pay in installments is not offered until cardholder checkout. The cardholder checks out of the hotel on 5 October with no further charges applied to his/her bill during the stay. During the checkout process, the cardholder is offered the option to pay in four monthly installment payment of USD 250 each. The original authorization on 1 October must first be reversed, and a new authorization that includes the installment payment terms must be submitted with the installment program ID and terms included in DE 48, subelement 95 and DE 112 for approval. Once the new authorization is approved, clearing can occur for the first installment payment amount.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	4 NA	USD 1,000	1001 MCG123456					USD 1,000
Rvrsl 0400 5 Oct	4 NA	USD 1,000	1004 MCG567890	MCG123456 1001				USD 0
Auth 0100 5 Oct	0 0 (Undef Auth)	USD 1,000	1005 MCP654321					USD 1,000
Clear 1240 5 Oct						USD 250	MCP654321 1005	USD 750

Final Authorization

Scenario F1: Final Authorization

F1.A: The cardholder makes a purchase of goods or withdrawal of cash for USD 500. The merchant notifies the acquirer of the completed authorization. The acquirer submits a clearing presentment based on notification from the merchant of authorization completion.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	0 1	USD 500	1001 MCG123456					USD 500
Clear 1240 2 Oct						USD 500	MCG123456 1001	USD 0

F1.B: Final authorization transaction is subsequently reversed due to technical issue such as acquirer to terminal response delivery error, ATM dispense error, or customer returns goods prior to completion being submitted for clearing, customer cancels e-commerce order, etc.

NOTE: In the Europe and Middle/East Africa regions, the reversal of a final authorization or completion of a final authorization for an amount different from the approved final authorization amount may attract a non-compliance fee if the number of non-compliant final authorizations exceeds 1 percent of the total final authorizations processed in a weekly billing period for an acquirer parent ICA or MCE Group ICA.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold

Merchant/ Acquirer			Authorization			Clearing	Issuer
Auth 0100 1 Oct	0 1	USD 1,000	1001 MCG123456				USD 1,000
Rvrsl 0400 2 Oct	0 1	USD 1,000	1004 MCG567890	MCG123456 1001			USD 0

Undefined Authorization

Scenario U1: Clearing Amount Matches Authorization Amount

The cardholder makes a purchase of goods for USD 500. The merchant notifies the acquirer of the completed authorization. The acquirer submits a clearing presentment based on notification from the merchant of authorization completion.

Merchant/ Acquirer			Authorization			Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	0 0 (Undef Auth)	USD 500	1001 MCG123456					USD 500
Clear 1240 2 Oct						USD 500	MCG123456 1001	USD 0

Scenario U2: Clearing Amount below Undefined Authorization Amount

The cardholder makes a purchase of goods for USD 500 on 1 October, and the merchant submits an authorization for USD 500. The cardholder returns an item for USD 100 prior to

the merchant submitting the completed authorization for clearing. The merchant notifies the acquirer of the completed authorization for USD 400.

U2.A: The acquirer submits a clearing presentment within 24 hours of notification from the merchant of authorization completion.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	0 0	USD 500	1001 MCG123456					USD 500
Clear 1240 2 Oct						USD 400	MCG123456 1001	USD 0

U2.B: The acquirer submits a partial reversal when notified by the merchant of authorization completion for lower than authorized amount, and clearing will not occur within 24 hours of merchant preauthorization completion notification.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	0 0	USD 500	1001 MCG123456					USD 500

Merchant/ Acquirer			Authorization				Clearing		Issuer
Rvrsl 0400 1 Oct	0 0	USD 500	1004 MCG567890	MCG123456 1001	USD 400				USD 400
Clear 1240 6 Oct						USD 400	MCG123456 1001		USD 0

Scenario U3: Authorization Completes for Higher Amount than Authorized

The cardholder makes an e-commerce purchase on 1 October, and the merchant submits an authorization for charges of USD 1,000. Prior to shipping, delivery charges are adjusted by USD 50. The merchant submits an additional authorization for the additional shipping charges of USD 50. The acquirer submits two clearing presentments based on notification from the merchant of authorization completion.

Merchant/ Acquirer			Authorization				Clearing	Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	0 0	USD 1,000	1001 MCG123456					USD 1,000
Auth 0100 5 Oct	0 0	USD 50	1005 MCG567890					USD 1,050
Clear 1240 6 Oct						USD 1,000	MCG123456 1001	USD 50

Merchant/ Acquirer	Authorization	Clearing		Issuer
Clear		USD 50	MCG567890	USD 0
1240			1005	
6 Oct				

Scenario U4: Authorization Cancellation

The cardholder makes a purchase of goods for USD 500 on 5 October, and the merchant submits an authorization for USD 500. The cardholder returns all goods purchased prior to the merchant submitting the completed authorization for clearing. The merchant notifies the acquirer of the full reversal. The acquirer submits the reversal upon merchant authorization cancellation notification.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	0 0	USD 1,000	1001 MCG123456					USD 1,000
Rvrsl 0400 1 Oct	0 0	USD 1,000	1001 MCG567890	MCG123456 1001				USD 0

Chargeback Extension Request

Scenario C1: Approved Chargeback Extension Request—Preauthorization Anticipated to Complete after Initial Chargeback Expiration Date

On 1 October, the cardholder makes a hotel reservation for a five-night stay in November. The cardholder check-in is not expected to occur until more than 30 days after the initial preauthorization date. On 30 October, the merchant submits a chargeback extension request message to allow for later clearing and extended chargeback protection. The cardholder checks into the hotel on 23 November. The cardholder checks out of the hotel on 28

November with no further charges applied to his/her bill during the stay. The acquirer submits a clearing presentment based on notification from the merchant of preauthorization completion.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	4 NA	USD 1,000	1001 MCG123456					USD 1,000
CB Extension 0100 31 Oct	4 NA	USD 0	1031 MCG567890	MCG123456 1001				USD 1,000
Clear 1240 28 Nov						USD 1,000	MCG123456 1001	USD 0

Scenario C2: Declined Chargeback Extension Request—Preauthorization Anticipated to Complete after Initial Chargeback Expiration Date

On 1 October, the cardholder makes a hotel reservation for a five-night stay in November. The cardholder check-in is not expected to occur until more than 30 days after the initial preauthorization date. On 30 October, the merchant submits a chargeback extension request message to allow for later clearing and extended chargeback protection. The issuer declines the chargeback extension request. The authorization expires on 31 October. The cardholder checks into the hotel on 23 November. The merchant must request a new authorization due to the previous authorization being expired and not approved for extension by the issuer. The cardholder checks out of the hotel on 28 November with no further charges applied to his/her bill during the stay. The acquirer submits a clearing presentment based on notification from the merchant of preauthorization completion.

Merchant/ Acquirer	Authorization					Clearing		Issuer
Action/MTI/ Date	DE 61, SF 7 DE 48, SE 61, SF 5	Auth Amt DE 4	Auth Trace ID DE 15, DE 63	Incr. Auth/ Rvrsl Trace ID DE 48, SE 63	Auth Rvrsl DE 95	Clear Amt DE 4	Clear Trace ID DE 63, SF 2	Hold
Auth 0100 1 Oct	4 NA	USD 1,000	1001 MCG123456					USD 1,000
CB Extension 0100 30 Oct	4 NA	USD 0	1030 MCG567890	MCG123456 1001				USD 1,000
Auth Expires 31 Oct								USD 0
Auth 0100 23 Nov	4 NA	USD 1,000	1123 MCG678901					USD 1,000
Clear 1240 28 Nov						USD 1,000	MCG678901 1123	USD 0

DE 61—DE 48 Comparison

Issuers globally must recognize values 0 (Normal Authorization/Undefined Finality) and 1 (Final Authorization) in DE 48, subelement 61, subfield 5 to distinguish a final authorization from a normal authorization/undefined finality in Authorization Request/0100 and Authorization Advice/0120 messages. When submitting Authorization Advice/0120—Acquirer-generated messages, subfield 5 should be populated with the same value as provided in the original Authorization Request/0100 message.

The following table illustrates the relationship between DE 61 and DE 48 and provides recommendation on the usage of DE 48, subelement 61, subfield 5 under various transaction conditions.

DE 61, SF 7	DE 48, SE 61, SF 5	DE 4	DE 3	Definition/ Comment	Acquirer	Issuer
0 (Normal Request)	1	>0	All	Final Authorization	Permitted.	Must be able to receive.
0	1	0	00, 01, 09, 17, 20, 28	Not permitted	Not permitted. Authorization Platform will reject (existing edit).	Not applicable. No transaction received.
0	1	0	30, 91, 92	Not permitted	Not permitted (not rejected by Authorization Platform).	May ignore DE 48, SE 61, SF 5.
0	0, not present	0	00, 01, 09, 17, 20, 28	Not permitted	Not permitted. Authorization Platform will reject (existing edit).	Not applicable. No transaction received.
0	0, not present	0	30, 91, 92	Normal Authorization	Permitted.	May ignore DE 48, SE 61, SF 5 if present.
0	0, not present	>0	All	Authorization with Undefined Finality	Permitted for card acceptors outside the Europe region; not permitted for card acceptors in the Europe region (not rejected by the Authorization Platform).	Must be able to receive.
4 (Preauthorized request)	1, 0, not present	0	00	Not permitted	Not permitted. Authorization Platform will reject when not permitted (existing edit).	No transaction received

DE 61, SF 7	DE 48, SE 61, SF 5	DE 4	DE 3	Definition/ Comment	Acquirer	Issuer
4	1	>0	00	Not permitted	Not permitted (not rejected by the Authorization Platform).	May ignore DE 48, SE 61, SF 5.
4	0, not present	>0	00	Preauthorization	Permitted.	Must be able to receive. May ignore DE 48, SE 61, SF 5 if present.
2 (*SecureCode* Phone Order)	0, 1, not present	0	00	Not permitted	Not permitted. Authorization Platform will reject (existing edit).	Not applicable. No transaction received.
2	0, 1, not present	>0	00	*Identity Check* Phone Order	Permitted.	Ignore DE 48, SE 61, SF 5 if present.
3 (ATM Installment Inquiry)	0, 1, not present	0	01	Not permitted	Not permitted. Authorization Platform will reject (existing edit).	Not applicable. No transaction received.
3	0, 1, not present	>0	01	ATM Installment Inquiry	Permitted.	Ignore DE 48, SE 61, SF 5 if present.
6 (ATC Update)	0, 1, not present	0	00	ATC Update	Permitted.	Ignore DE 48, SE 61, SF 5 if present.
6	0, 1, not present	>0	00	Not permitted	Not permitted. Authorization Platform will reject (existing edit).	Not applicable. No transaction received.
8 (Account Status Inquiry)	0, 1, not present	0	00, 28	Purchase and Payment Account Status Inquiry Service	Permitted.	Ignore DE 48, SE 61, SF 5 if present.

DE 61, SF 7	DE 48, SE 61, SF 5	DE 4	DE 3	Definition/ Comment	Acquirer	Issuer
8	0, 1, not present	>0	28	Payment Account Status Inquiry Service	Permitted.	Ignore DE 48, SE 61, SF 5 if present.
8	0, 1, not present	>0	00	Not permitted	Not permitted. Authorization Platform will reject (existing edit).	Not applicable. No transaction received.

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

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 new processing integrity fee under the new processing integrity programs and non-compliance assessments for Not Reversed or Cleared Undefined Authorization and Preauthorization, starting with the billing invoice dated 28 May 2017. The new 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 new 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 new 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.

Installment Transactions

The following section explains how installment payment authorization messages are coded.

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.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Balance Inquiries

Mastercard supports the several types of balance inquiry requests for cardholders to perform balance inquiries.

- ATM and point-of-sale (POS) terminal balance inquiries
- Short Message Service balance inquiries
- Mobile Remote Payments balance inquiries

The balance inquiry service is optional for issuers.

ATM and Point-of-Sale Terminal Balance Inquiries

The following information describes ATM balance inquiries and point-of-sale (POS) terminal balance inquiries.

ATM Balance Inquiries

The ATM balance inquiry allows Mastercard cardholders to perform a balance inquiry on the Mastercard® ATM Network.

Upon receipt of an ATM balance inquiry request, participating issuers return the available balance in the authorization response. The Authorization Platform performs any applicable currency conversion and forwards the available balance to the acquirer. The acquirer provides the available balance to the ATM terminal for display at the ATM and on the customer's printed receipt.

NOTE: Issuers in the United Kingdom (U.K.) may provide a maximum of two account balances, the ledger balance in addition to the available balance, when responding to intracountry ATM balance inquiry requests.

Point-of-Sale Terminal Balance Inquiries

The point-of-sale (POS) balance inquiry enables cardholders and acquirers to check the remaining amount of funds on a Mastercard prepaid card or private label prepaid card. This feature makes it easier for the cardholder to completely redeem the funds on the prepaid card and reduces the potential of a declined authorization request because the purchase amount exceeds the funds available on the card. Therefore, this feature can help to reduce checkout times and lost sales.

Upon receipt of a POS balance inquiry, participating issuers return the available balance in the authorization response. The Authorization Platform performs any applicable currency conversion and forwards the available balance to the acquirer. The acquirer provides the available balance to the merchant for display on the customer's printed receipt.

There are two types of POS terminal balance inquiries:

- Cardholder-initiated balance inquiry—Cardholders can ask the cashier to check a card's remaining balance before making a purchase. The cardholder and cashier can then determine whether the entire purchase amount can be funded by the prepaid card or whether a supplemental payment method (split tender) is needed to complete the purchase.
- Automated balance inquiry—Acquirers can expedite sales by sending an automatic POS balance inquiry on a specified range of prepaid accounts issued by the issuer. The cashier can then inform customers in advance whether they will need to use a split tender to complete the purchase.

Alternate Processing

ATM and POS balance inquiries are not eligible for processing by the Stand-In System or X-Code System. If the issuer is unavailable, the Authorization Platform returns an Authorization System or issuer system inoperative response to the acquirer.

Reversals of Balance Inquiry Transactions

Mastercard supports reversals of balance inquiry transactions using Reversal Request/0400 and Reversal Advice/0420 messages containing DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 30 (Balance Inquiry). In balance inquiry transactions, DE 4 (Amount, Transaction) contains a value of all zeros.

A balance inquiry reversal is generally initiated when the balance inquiry request is not completed at the point-of-interaction. An acquirer may submit a reversal in an effort to recoup any fee that may be assessed as a result of the original balance inquiry request.

To Participate

Issuers can complete the *Point-of-Sale (POS) and ATM Balance Inquiry Participation* (Form 771).

For More Information

For details about data requirements refer to the *Customer Interface Specification* manual.

Short Message Service Balance Inquiry Service

The Short Message Service (SMS) Balance Inquiry service allows cardholders with SMS-enabled mobile devices to request and receive balance information on their registered cards via their mobile phone devices.

The SMS Balance Inquiry service positions card issuers to be more competitive by providing their cardholders with convenient real-time access to their account balance information via their mobile devices. Issuers participating in the SMS Balance Inquiry service 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).

This service is only available to issuers of Mastercard® and Debit Mastercard® cards in the U.S. and Europe regions.

To Participate

Issuers that want to participate in the SMS Balance Service Program must support balance inquiries.

Issuers that want to participate in the SMS Balance Service Program must complete a contract and registration form. For more detailed information and inquiries about the SMS Balance Inquiry Service, send an email message to smsbalanceservice@Mastercard.com.

For More Information

For details about data requirements refer to the *Customer Interface Specification* manual.

Mobile Remote Payments Balance Inquiries

The Mobile Remote Payments program provides participating cardholders with access to their account balance information via an application on their mobile device. Issuers participating in the Mobile Remote Payments program will receive these balance inquiries in DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), value 82 (PAN auto entry via server).

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Cardholder-Activated Terminals

Cardholder-activated terminals (CATs) are usually unattended terminals that accept bankcards, debit, charge, and proprietary cards. These terminals are frequently installed at rail ticketing stations, gasoline stations, toll roads, parking garages, and other merchant locations.

For procedures related to authorization and other processing requirements related to each CAT level, refer to the *Transaction Processing Rules*.

Automated Fuel Dispensers

If an issuer approves an authorization request for an automated fuel dispenser transaction identified with MCC 5542 (an AFD transaction) and occurring at a merchant located in the United States or Canada, then within 60 minutes of the time that the authorization request message was sent, the acquirer must send an Authorization Advice/0120 message advising the issuer of the final transaction amount (or a Reversal Request/0400 message, if the transaction will not be completed or will finalize for a lesser amount than requested).

If after approving an authorization request for an AFD transaction, an issuer in the United States or Canada has placed a hold on cardholder funds in excess of USD 1 or CAD 1 respectively, then within 60 minutes of receiving the acquirer's advice message, the issuer must release any hold amount that exceeds the completed transaction amount specified.

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.

NOTE: As an alternative, the Trace ID of the original preauthorization may be used for clearing presentment if that same Trace ID is included in the AFD completion advice message within DE 48, subelement 63 (Additional Data, Trace ID).

For requirements about intra-European and inter-European Maestro transactions that occur at unattended POS terminals located at petrol stations, refer to the Automated Fuel Dispenser Transactions section in Card-Present Transactions of the *Transaction Processing Rules*.

IFC Blocked Gaming File

Issuers have the option to block their cardholders from participating in In-flight Commerce (IFC) gaming (CAT level 4) by listing their BINs in the IFC Blocked Gaming File. Acquirers must ensure timely delivery and installation of the IFC Blocked Gaming File to gambling service providers. IFC Blocked Gaming File access is required before every gaming transaction.

Gaming transactions are not permitted at IFC terminals acquired within Europe.

NOTE: The IFC Blocked Gaming File applies only to in-flight commerce gaming, and not to other IFC activity.

How to List BINS in the IFC Blocked Gaming File

To list BINs in this file, complete the *IFC Range Blocking for Gaming Transactions* (Form 161).

Effective Dates for the IFC Blocked Gaming File

Effective dates for the IFC Blocked Gaming File are the first and 15th day of each month. Mastercard must receive issuer listings at least two weeks before the effective date to be included in the file.

Distribution of the IFC Blocked Gaming File

Distribution of the IFC Blocked Gaming File occurs two times each month. Mastercard provides it either via a Mastercard bulk file or via Mastercard File Express. For the file layout, refer to the *IFC Blocked Gaming Transactions* (Form 161).

1. Mastercard creates the IFC Blocked Gaming File at approximately 13:00 (St. Louis time) and distributes it to acquirers' MIPs.
2. Acquirers stage the file for unloading and distribute it to their gaming service providers.
3. Gaming service providers must ensure timely delivery and installation of the IFC Blocked Gaming File to the on-board servers that monitor IFC transactions.

NOTE: Because Mastercard requires IFC Blocked Gaming File access before every gaming transaction, acquirers and gaming service providers must distribute and install the file when they receive it.

Mastercard Processing of IFC Gaming Transactions

In-flight commerce gaming transactions go directly to the issuer.

Cardholder Authentication

Mastercard offers a new indicator that provides the ability for issuers and acquirers to recognize when biometrics are used to authenticate the cardholder.

To assist issuers and governments globally to reduce cost and eliminate fraud in their benefit disbursement process, Mastercard provides a new authentication indicator to support those efforts. When populated, this authentication indicator signifies that the account holder was authenticated using a biometric match.

Transactions will be processed through the Mastercard Network through the EMV Chip contact or EMV Contactless interface (POS Entry mode value 05 or 07). Issuers and acquirers will be informed that a biometric match occurred and the cardholder is present at the time of the transaction when DE 48, subelement 17 contains either value 1 or value 2.

Participating issuers should register their new or existing account ranges for one of the authentication service options.

Authentication Service Options

- Authentication Service Type 1
- Authentication Service Type 2

Service Type Options

Mastercard will offer the following service type options to support cardholder authentication.

Authentication Service Type 1

For a specific program, issuers may choose an account range where DE 23 (Card Sequence Number) will be used to differentiate the chip's application (Cardholder Authentication vs. Standard).

- 01x (Cardholder Authentication Application) where x is the sequence number 0 to 9; the transaction is processed for the authentication service.
- 02x (Standard Application) where x is the sequence number 0 to 9; the transaction is processed as a standard transaction.

Authentication Service Type 2

For a specific program, issuers may choose an account range where a PAN will be used to differentiate the chip's application (Cardholder Authentication vs. Standard).

- PAN#1: The account range associated with PAN #1 will indicate that the Cardholder Authentication application on the chip was launched.
- PAN#2: The account range associated with PAN #2 will indicate that a standard CVM (Cardholder Verification Message) application on the chip was launched.

Authentication Service Type 1 and Authentication Service Type 2

Mastercard will populate subelement 17 (Authentication Indicator), value 1 (Transaction qualified for Authentication Service Type 1) and value 2 (Transaction qualified for Authentication Service Type 2) in DE 48 (Additional Data—Private Use) to indicate that the transaction was authenticated using biometrics.

The Authentication Indicator is forwarded to the acquirer in these messages:

- Authorization Request Response/0110
- Authorization Advice Response/0130—Issuer-generated (Responding to Acquirer-generated 0120)

The Authentication Indicator is forwarded to the issuer in these messages:

- Authorization Request/0100
- Authorization Advice/0120 (Acquirer-generated and System-generated)

If the Authentication Indicator is not populated in DE 48, subelement 17, the issuer may choose to authorize or decline the transaction.

Account Status Inquiry with Authentication Indicator

DE 48 (Additional Data—Private Use), subelement 17 (Authentication Indicator) will be populated for Authentication Service Types 1 and 2 based on the following conditions:

- Account Range is registered for Authentication Service Type 1 or 2
- DE 3 (Processing Code), value 00 (Purchase)
- DE 4 (Amount, Transaction) is zero
- Transaction is an EMV Chip with DE 22 (Point-of-Service [POS] Entry Mode) value 05 or 07
- If present, DE 55 (Integrated Circuit Card [ICC] System-Related Data), tag 9F10:
  - CVR byte1, bit1 is present with a value of 1 (successful), and
  - CVR byte2, bit2 is present with a value of 1 (biometric)
- Is an Account Status Inquiry Transaction where DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status Indicator) contains value 8 (Account Status Inquiry Service)

Authentication Indicator During Transactions other than Account Status Inquiry

DE 48, subelement 17 (Authentication Indicator) will be populated for Authentication Service Types 1 and 2 based on the following conditions:

- Account Range is registered for Authentication Service Type 1 or 2
- DE 4 (Amount, Transaction) is not 0
- Transaction is an EMV Chip with DE 22 (Point-of-Service [POS] Entry Mode) value 05 or 07
- If present, DE 55 (Integrated Circuit Card [ICC] System-Related Data), tag 9F10:
  - CVR byte1, bit1 is present with a value of 1 (successful), and
  - CVR byte2, bit2 is present with a value of 1 (biometric)

Data Requirements

Mastercard will add the following in DE 60 (Advice Reason Code):

- Subfield 1 (Advice Reason Code), values in Authorization Advice/0120
  - 160 (Authentication advice to Issuer)
  - 192 (M/Chip Offline Advice to Issuer)
- Subfield 2 (Advice Detail Code), value 0078 (M/Chip Data not Present)

The Authorization Platform performs the following system edits on Authorization Request/0100 messages and Authorization Advice/0120—Acquirer-generated messages.

WHEN...	THEN the Authorization Platform...
An Account Status Inquiry Transactions for account ranges participating in the Cardholder Authentication service – the Authorization Request/0100 message contains: • DE 2—Primary Account Number (PAN) setup for Type 1 Cardholder Authentication Service, and • DE 4 has value of zero, and • DE 23 (Card Sequence Number) contains a value of 01X, and • DE 61, subfield 7 has value of 8, and • DE 55—Integrated Circuit Card (ICC) System-Related Data is present and tag 9f10: – Cvr byte1, bit1 is present with a value other than 1 (successful), or – Cvr byte 2 bit 2 is present with the value other than 1 (biometric)	Sends the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) = 05 (Do not honor) AND Sends an Authorization Advice/0120 message with DE 60 (Advice Reason Code): • Subfield 1 (Advice Reason Code) value 160 (Cardholder Authentication Advice to Issuer), and • Subfield 2 (Advice Detail Code) value 0078 (M/Chip Biometric Data not Present)
An Account Status Inquiry Transactions for account ranges participating in the Cardholder Authentication service – the Authorization Advice/0120—Acquirer-generated message contains: • DE 2—Primary Account Number (PAN) setup for Type 1 Person Present Service, and • DE 4 has value of zero, and • DE 61, subfield 7 has value of 8, and • DE 55—Integrated Circuit Card (ICC) System-Related Data is present and tag 9f10: – Cvr byte1, bit1 is present with a value other than 1 (successful), or – Cvr byte 2 bit 2 is present with the value other than 1 (biometric)	Sends the acquirer an Authorization Advice Response/0130 message where: • DE 39 (Response Code) = 30 (Format Error), and • DE 44 = 055 (Transactions with zero as completed amount may not be adjusted)

WHEN...	THEN the Authorization Platform...
An Account Status Inquiry Transactions for account ranges participating in the Cardholder Authentication service – the Authorization Request/0100 message contains: • DE 2—Primary Account Number (PAN) setup for Type 2 Person Present Service, and • DE 4 has value of zero, and • DE 61, subfield 7 has value of 8, and • DE 55—Integrated Circuit Card (ICC) System-Related Data is present and tag 9f10: – Cvr byte1, bit1 is present with a value other than 1 (successful), or – Cvr byte 2 bit 2 is present with the value other than 1 (biometric)	Sends the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) = 05 (Do not honor) AND Sends an Authorization Advice/0120 message with DE 60 (Advice Reason Code): • Subfield 1 (Advice Reason Code) value 160 (Cardholder Authentication Advice to Issuer) • Subfield 2 (Advice Detail Code) value 0078 (M/Chip Biometric Data not Present)
An Account Status Inquiry Transactions for account ranges participating in the Cardholder Authentication service – the Authorization Advice/0120—Acquirer-generated message contains: • DE 2—Primary Account Number (PAN) setup for Type 2 Cardholder Authentication Service, and • DE 4 has value of zero, and • DE 61, subfield 7 has value of 8, and • DE 55—Integrated Circuit Card (ICC) System-Related Data is not biometric authenticated	Sends the acquirer an Authorization Advice Response/0130 message where: • DE 39 (Response Code) = 30 (Format Error) • DE 44 (Additional Response Data) = 055 (Transactions with zero as completed amount may not be adjusted)
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: • DE 39 (Response Code) = 30 (Format Error) • DE 44 (Additional Response Data) = 060 (Invalid DE 60 value)

Offline Account Status Inquiry on Account ranges set up for the Authentication Indicator

For offline EMV Chip approved Account Status Inquiry only transactions (without purchase, payment, or cash disbursement) on account ranges set up for Authentication Service Type 1 or for Authentication Service Type 2 (which can be determined by checking Integrated Product Message Mastercard Parameter Extract (MPE) Table IP0040T1: Issuer Account Range

containing an Authentication Indicator Value of 1 or 2), acquirers must be prepared to send Authorization Advice/0120—Acquirer-generated messages to the issuer with:

- DE 4 (Amount, Transaction), value zero
- DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status Indicator), value 8 (Account Status Inquiry Service)
- DE 60 (Advice Reason Code), new value 192 (M/Chip Offline Advice to issuer)
- DE 55 (Integrated Circuit Card [ICC] System-Related Data)

In addition, issuers must support and authenticate DE 55 (Integrated Circuit Card [ICC]) System Related Data).

NOTE: Issuers that have registered for this transaction authentication service and do not participate in OBS 2, will need to validate the Application Cryptogram (tag 9F26 in DE 55) and chip data as in DE 55 for Authentication transactions. In addition to their standard chip data validation processing for chip transactions, issuers may verify Subelement 9F10 – Issuer Application Data (IAD), Card Verification Results, Byte2, Bit2 will be re-used for CVM type as follows:

- **0 – Standard – non-biometric standard CVM method was used in this transaction**
- **1 – Biometric – biometric CVM method was used in this transaction**

Card Validation Code 1 Verification

Card Validation Code 1 (CVC 1) verification provides added security for the card authentication process in authorization request transactions that use magnetic stripe technology.

Card Validation Code 1

The Card Validation Code 1 (CVC 1) is a three-digit code that must be encoded on Track 1 and Track 2 in three contiguous positions in the Discretionary Data field of the magnetic stripe on all Mastercard Cards.

Issuers may calculate the CVC 1 by one of the following two methods:

- Issuer proprietary calculation—Gives the issuer the option to derive the CVC algorithmically.
- Data Encryption Standard (DES) software—Issuer may perform the calculation through a DES software application within a host system or through use of a tamper-resistant security module (TRSM).

Card Validation Code 1 On-Behalf Services

Mastercard provides several Card Validation Code 1 (CVC 1) on-behalf services to support Mastercard products. The CVC 1 on-behalf services are available for transactions that are performed using magnetic stripe technology.

To support on-behalf processing of Mastercard products, the following CVC 1 on-behalf services are available:

- CVC 1 Pre-Validation Service (OBS 11)—An optional, pre-validation service performed on authorization request transactions
- CVC 1 Validation Stand-In Service (OBS 10)—Service in which a Stand-In System processes and validates transactions when the issuer is not available; this service is mandatory for issuers with authorization systems that support magnetic stripe transactions.

NOTE: The CVC 1 Pre-Validation Service (OBS 11) is not offered to issuers in the Russian Federation processing domestic transactions.

NOTE: Effective on or before 1 April 2017, based on region-specific effective dates announced in "Revised Standards for Validation Services During Stand-In Processing," *Global Operations Bulletin* No. 4, 1 April 2016, global issuers that participate in the CVC 1 Validation Stand-In Service (OBS 10) must have CVC 1 Validation in Stand-In performed during Stand-In processing. Issuers that participate in CVC 1 Pre-Validation Service (OBS 11) do not need to participate in OBS 10 as the results from OBS 11 will be used by stand-in.

Issuers that participate in the CVC 1 On-Behalf Prevalidation Services receive the following information in the Authorization Request/0100 message:

- CVC 1 validation results inserted in DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 1 (On-behalf Service), value 11, and subfield 2 (On-behalf Result 1) with one of the following values:
  - V—Valid
  - I—Invalid CVC 1
  - K—No matching key file for this PAN, PAN expiry date combination
  - U—Unable to process

CVC 1 Validation Results for OBS 11

The following table describes the results of the CVC 1 validation for OBS 11 for Dual Message System connected issuers.

WHEN...	THEN Mastercard sends...
CVC 1 Pre-Validation was successfully completed, or when the issuer has elected to receive the validation results for further decisioning, regardless of the validation results	The issuer an Authorization Request/0100 message containing: • DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), Subfield 1 (On-behalf Service), value 11, and Subfield 2, (On-behalf Result 1) values V (Valid), I (Invalid CVC 1), K (No matching key file for this PAN, PAN expiry date combination), or U (Unable to process)

WHEN...	THEN Mastercard sends...
CVC 1 Pre-Validation was unsuccessful	The acquirer an Authorization Request Response/0110 message containing: • DE 39 (Response Code) = 05 (Do not Honor) and The issuer an Authorization Advice/0120 message containing one of the following sets of values, depending on the reason for the rejection: • Reason: Invalid CVC 1 value in the track data (DE 35 [Track 2 Data] or DE 45 [Track 1 Data]): – DE 39 (Response Code) = 05 (Do not honor) – DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 1 (On-behalf Service), values 10 or 11, subfield 2 (On-behalf Result 1) with a value of I (Invalid CVC 1) – DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code) with a reason code 0028: Reject: Invalid CVC 1 • Reason: An applicable CVC 1 validation key is unavailable: – DE 39 (Response Code) = 05 (Do not honor) – DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 1 (On-behalf Service) value 11, subfield 2 (On-behalf Result 1) with value of K (No matching key file for this PAN, PAN expiry date combination) – DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code) with a reason code 0047: CVC 1 No matching key file for this PAN, PAN expiry date combination, status unknown • Reason: Mastercard is unable to complete the CVC 1 validation service processing due to a technical issue: – DE 39 (Response Code) = 05 (Do not honor)

WHEN...	THEN Mastercard sends...
	– DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 1 (On-behalf Service), values 10 or 11, subfield 2 (On-behalf Result 1) with a value of U (Unable to process) – DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code) with a reason code 0036: Reject: CVC 1 Unable to process

CVC 1 Validation Results for OBS 10

The following table describes the results of the CVC 1 validation for OBS 10 for Dual Message System connected issuers.

WHEN...	THEN Mastercard sends...
Stand-In processes the transaction	The issuer an Authorization Advice/0120 message containing: • DE 48 (Additional Data—Private Use), subelement 87 (Card Validation Code Result), value Y (Invalid CVC 1)

Participating in CVC 1 On-Behalf Services

CVC 1 on-behalf services are currently available to issuers that process through the Dual Message System.

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.

CVC 1 Validation Stand-In Service (OBS 10)

This service is mandatory for issuers with authorization systems that support magnetic stripe transactions.

CVC 1 Pre-Validation Service (OBS 11)

Issuers that choose to participate in the optional CVC 1 Pre-Validation Service (OBS 11) must register by contacting their CIS representative.

NOTE: Issuers that enroll account ranges in the CVC 1 Pre-Validation Service that are already enrolled in the existing CVC 1 Validation Service in Stand-In Service must request the removal of those account ranges from the existing CVC 1 Validation Service in Stand-in service.

Alternate Processing of Invalid CVC 1 Validation Results

Mastercard considers the results of the CVC 1 validation in (a) DE 48, subelement 71 (On-behalf Services) when responding to the Authorization Request/0100 message for issuers participating in pre-validation services and (b) DE 48, subelement 87 (Card Validation Code Result) when responding to the Authorization Request/0100 message for issuers participating in the Stand-In validation service. If the results are invalid, Mastercard uses the issuer's instructions from the decision matrix as set in the key file.

Issuers participating in one of the CVC 1 on-behalf services should reference the KMS interface section defined in the *On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications* manuals for information about CVC 1 validation keys.

Authorization Reports for CVC 1 On-Behalf Services

The Authorization Parameter Summary Report (SI737010-AA) lists the name of the on-behalf service in which the issuer is participating for an account range and displays the issuer selection for participating in the Card Validation Code 1 (CVC 1) processing service.

For a sample of the Authorization Parameter Summary Report (SI737010-AA), refer to Reports. For a sample of the Daily Account File Activity Report (AM700010-DD), refer to the *Account Management System User Manual*.

Card Validation Code 2 Verification

Card validation code 2 (CVC 2) verification provides added security for the card authentication process in authorization requests.

CVC 2

CVC 2 is a three-digit code algorithmically derived by the issuer and indent- printed on the signature panel to the right of the account number.

CVC 2 is one of several card authentication methods currently used by Mastercard to combat fraud. The use of CVC 2 deters fraudulent use of an account number.

NOTE: Stand-In processing does not verify CVC 2 values.

Conditions for CVC 2 Verification

CVC 2 verification allows acquirers to receive online verification of CVC 2 values from issuers when the certain conditions apply.

- The acquirer transmits the CVC 2 value that the cardholder provided to the merchant in DE 48 (Additional Data—Private Use), subelement 92 (CVC 2) of the Authorization Request/0100 message.
- The issuer provides a valid response in DE 48, subelement 87 (Card Validation Code Result) of the Authorization Request Response/0110 message to indicate that the CVC 2 value was verified (value M or N) or not processed (value P).

Participation Requirements

Participation requirements for acquirers and issuers using CVC 2 verification are listed in table format.

Acquirers

When cardholders provide merchants with the CVC 2 value for transactions, acquirers must include the CVC 2 value in DE 48, subelement 92 of the Authorization Request/0100 message.

To participate in CVC 2 verification, acquirers must be able to receive the following CVC 2 values in DE 48, subelement 87 of the Authorization Request Response/0110 message.

Subelement 87 Value	Description
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

The acquirer is responsible for ensuring that the merchant receives the CVC 2 response code provided by the issuer in DE 48, subelement 87 of the Authorization Request Response/0110 message.

Issuers

Issuers must be able to receive and to process the CVC 2 value when present in DE 48, subelement 92 of the Authorization Request/0100 message, and to provide a valid CVC 2 response in DE 48, subelement 87 of the Authorization Request Response/0110 message.

CVC 2 values M, N, and P are considered valid when used by issuers. Only Mastercard can use CVC 2 value U.

The Authorization Platform places a value of U in DE 48, subelement 87 of the Authorization Request Response/0110 message to indicate that the CVC 2 value was not verified, at the issuer's request, as the issuer was temporarily unable to receive the CVC 2 value.

Issuers should note that if an acquirer transmits both CVC 1 and CVC 2 data, CVC 1 processing takes precedence over CVC 2 processing.

WHEN the CVC 1 value is…	THEN…
Invalid	Issuers should respond with value Y (Invalid CVC 1) in DE 48, subelement 87. Issuers should not verify the CVC 2 value.
Valid	Issuers must verify the CVC 2 value and send the appropriate response to the acquirer.

Mastercard will require all issuing and acquiring processors to code, support, and integrate into their systems the data elements, subelements, and values associated with CVC2. 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.

Card Validation Code 3 (CVC 3) Verification

Card validation code 3 (CVC 3) verification provides added security to validate whether a Mastercard® contactless card or device is legitimate.

CVC 3

CVC 3 is a code algorithmically derived by a contactless card or device.

CVC 3 On-behalf Services

Mastercard provides several CVC 3 on-behalf services to support contactless products. The CVC 3 on-behalf services are available for transactions that derive from proximity chip functionality with magnetic stripe Track 1 or Track 2 data containing a CVC 3 value.

To support on-behalf processing of contactless products, the following CVC 3 on-behalf services are available:

- 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 Pre-validation Service.

Mastercard will perform the dynamic CVC 3 validation on behalf of the issuer before forwarding the Authorization Request/0100 message. If the issuer is unavailable, Mastercard will consider the results of the dynamic CVC 3 validation when the transaction is processed by the Stand-In System.

- Dynamic CVC 3 Validation in Stand-In Service—This service is mandatory for issuers with contactless-enabled authorization systems that support dynamic CVC 3 validation in order to provide dynamic CVC 3 validation when the issuer is not available and the transaction is processed by the Stand-In System.

NOTE: Effective on or before 1 April 2017 based on region specific effective dates per *Global Operations Bulletin* No. 4, 1 April 2016, Revised Standards for Validation Services During Stand-In Processing, all issuers globally that participate in Stand-In processing must have Dynamic CVC 3 Validation in Stand-In performed during Stand-In processing.

The issuer receives the following information in the Authorization Request/0100 message:

- The result of the CVC 3 validation inserted in DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 2 (OB Result 1) with one of the following values:
  - A (ATC outside allowed range) for dynamic CVC 3 pre-validation only
  - E (CVC 3 ATC Replay) for dynamic CVC 3 only
  - I (CVC 3 Invalid)
  - N (Unpredictable Number Mismatch) for dynamic CVC 3 only
  - U (Unable to process)
  - V (Valid CVC 3)
- ATC information inserted in DE 48, subelement 34 (Dynamic CVC 3 ATC Information) only for the dynamic CVC 3 services and if DE 48, subelement 71 is value V, A, or E.

Participation in any CVC 3 on-behalf service is defined by the combination of an account range and the floor expiry date. Validation is facilitated by information the issuer provides to Mastercard. Unless Mastercard arranges for devices to be sent to cardholders on behalf of issuers, issuers will be requested to provide confidential key data to Mastercard that will be critical in the validation process. For information about CVC 3 validation, issuers should reference the Key Management Services (KMS) interface section in the *On-behalf Key Management (OBKM) Procedures*, *On-behalf Key Management (OBKM) Interface Specifications*, and *Contactless On-behalf Services Guide*.

The acquirer receives the following CVC 3 data in the Authorization Request Response/0110 message containing DE 48, subelement 87 (Card Validation Code Result):

- E (Length of unpredictable number was not a valid length)
- P (Unable to process)
- Y (Invalid or ATC Outside of Allowed Range or ATC Replay)

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 receives the following information in the Authorization Advice/0120 message when the Stand-In System responded on behalf of the issuer or when the issuer requested the Optional Non-valid CVC 3 Processing:

- DE 48, subelement 71 (On-behalf Services) identifies the service performed and the result.
- DE 48 (Additional Data—Private Use), subelement 34 (Dynamic CVC 3 ATC Information) is present when the on-behalf service result in subelement 71, subfield 2 (On-behalf Result 1) was value A, E, or V.
- DE 48, subelement 87 (Card Validation Code Result) is present when the CVC 3 validation result was not valid.
- DE 60 (Advice Reason Code) identifies the specific reason for the advice message.

Optional Non–valid CVC 3 Processing

Mastercard provides issuers the option to have the Authorization Platform respond to the Authorization Request/0100 messages on their behalf when the CVC 3 value is not valid. Issuers receive an Authorization Advice/0120—System-generated message when the Authorization Platform responds.

This option only is available to issuers, which are connected to the Mastercard Network, participating in the Contactless Mapping Service or the Dynamic CVC 3 Pre-validation Service.

Overview

The Contactless Application Transaction Counter (ATC) file (MCC109) contains the most recent ATC values for cards supporting EMV Contact, EMV Contactless, and Contactless Magstripe transactions. It is used in the scope of EMV Cryptogram and CVC3 Pre-validation Services and Validation in Stand-in Services.

Issuers may need to use the MCC109 ATC file update when the ATC value of the card gets out of sync compared to the value recorded in the Mastercard MCC109 database. It allows them to cover any ATC value discrepancies that are created when transactions are not routed through the Mastercard Network.

In the context of CVC 3 pre-validation and validation in Stand-in Services, issuers must use the MCC109 ATC file update when the ATC length value in the discretionary data of the card is fewer than four digits.

Mastercard supports entry of the ATC data in DE 101 (File Name), value (MCC109) via the following methods:

- Online File Maintenance
- Bulk File Maintenance
- Mastercard eService Maintenance

MCC109 ATC maintenance requests submitted by 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 hours (St. Louis, Missouri USA time).

Alternate Processing

Mastercard considers the results of the CVC 3 validation in DE 48, subelement 71 (On-behalf Services) when responding to the Authorization Request/0100 message for issuers participating in pre-validation services or in the Stand-In validation services. If the results are invalid, Mastercard uses the issuer's instructions from the decision matrix as set in the key file.

Issuers participating in one of the CVC 3 on-behalf services should reference the KMS interface section defined in the *On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications* manuals for information about dynamic CVC 3 validation keys.

Authorization Reports

Certain reports provide information about CVC 3 on-behalf services.

- The Authorization Parameter Summary Report (SI737010-AA) lists the name of the on-behalf service in which the issuer is participating for an account range and displays the issuer selection for participating in the optional, non-valid CVC 3 processing service.
- The Daily Account File Activity Report (AM700010-DD) contains the Contactless Application Transaction Counter (ATC) File activity.

For a sample of the Authorization Parameter Summary Report (SI737010-AA), refer to Reports. For a sample of the Daily Account File Activity Report (AM700010-DD), refer to the *Account Management System User Manual*.

To Participate

CVC 3 on-behalf services are currently available to issuers that process through the Dual Message System.

For more information about CVC 3 on-behalf services and how to participate, refer to the *Contactless On-behalf Services Guide*.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Card Validation Code Verification for Emergency Card Replacements

Card validation code (CVC) for emergency card replacements is a service that provides a way for Mastercard to encode a CVC on the Emergency Card Replacement Service (ECR Service). The Mastercard Global Service Center provides this service for customers.

CVC verification for ECR Service is optional.

How to Request CVC Verification for ECR Service

Customers that use Mastercard ECR Service can request this service by completing the *CVC Verification Specification Form for Emergency Card Replacements* (Form 566/567).

NOTE: Customers that do not currently use Mastercard ECR Service can request the ECR Service by completing the Global Service questionnaire, available from the Global Customer Service team.

Use of CVC Keys

To produce ECRs with CVC technology, Mastercard either must obtain CVC keys from issuers or receive permission from issuers to use CVC keys that they provided to Mastercard for CVC verification in Stand-In processing.

To provide Mastercard with CVC keys and specifications, complete the *CVC Specification Form for Emergency Card Replacements* (Form 566/567).

Mastercard securely stores these keys and components, allowing access to the information only to generate CVC coding for the ECRs processed through the Global Service Center.

Cirrus and Maestro Transaction Processing

The Authorization Platform supports Cirrus® (CIR) and Maestro® (MSI) transaction processing.

NOTE: Applies only to the Europe region.

The Authorization Platform supports Cirrus® (CIR) and Maestro® (MSI) transaction processing. Mastercard supports both acquiring and issuing activity on the Authorization Platform for CIR and MSI card products.

Both acquiring and issuing CIR and MSI transactions are limited to Europe region acquirers and issuers that process through the Mastercard Network.

Cirrus

Cirrus (CIR), as a brand, is a Mastercard card brand designed exclusively for use at an ATM. Cirrus, as a network, is a wholly owned subsidiary of Mastercard International Incorporated that operates the international ATM sharing association known as the Mastercard® ATM Network. CIR is one of the brands accepted by the Cirrus® network.

The following transaction types can be initiated at the ATM and are indicated by the contents of DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) for CIR transactions:

- 00 (Purchase)
- 01 (Withdrawal)
- 28 (Payment Transaction)
- 30 (Balance Inquiry)
- 91 (PIN Unblock)
- 92 (PIN Change)

Although the Authorization Platform supports CIR transaction acquiring, only specified acquirers have this functionality. To ensure transactions are submitted by eligible acquirers, the

Authorization Platform verifies the acquirer parameter when an authorization transaction is branded as CIR.

Maestro

Maestro (MSI) is a Mastercard brand for debit card products that may be used both at an ATM and at a point-of-service (POS) terminal. POS transactions include face-to-face and electronic commerce (e-commerce) transactions. Following are the valid values for DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) for MSI transactions:

- 00 (Purchase)
- 01 (Withdrawal)
- 09 (Purchase with Cash Back)
- 20 (Purchase Return/Refund)
- 28 (Payment Transaction)
- 30 (Balance Inquiry)
- 91 (PIN Unblock)
- 92 (PIN Change)

For POS processing, Mastercard has defined specific POS processing criteria for MSI transactions. DE 35 (Track 2 Data) must be present in the POS transaction. For Maestro e-commerce transactions, if the acquirer could not construct DE 35, the Authorization Platform will build DE 35 using the contents of DE 2 (Primary Account Number [PAN]) and DE 14 (Date, Expiration). Although the Authorization Platform supports MSI transaction acquiring, only specified acquirers have this functionality. To ensure transactions are submitted by eligible acquirers, the Authorization Platform verifies the acquirer parameter when an authorization transaction is branded as MSI.

Alternate Processing

Alternate processing is optional for CIR and MSI transactions.

For issuers that choose to use the Stand-In System for alternate processing, Stand-In uses either the product or account range issuer-defined limits to determine how to respond to an Authorization Request/0100 message. If an issuer does not specify account range level processing, the Stand-In System uses the Mastercard defined product level defaults.

For the current definition of minimum transaction limits, refer to *Mastercard Rules* and *Transaction Processing Rules*.

WHEN…	THEN the Authorization Platform…
The issuer or the Stand-In System is not available to respond to the Authorization Request/0100 message	Returns an Authorization Request Response/0110 message where: DE 39 = 91 (Authorization System or issuer system inoperative)

CIR and MSI transactions are not processed by the X-Code System.

For More Information

Specific processing rules and Standards have been defined for CIR ATM processing and MSI ATM processing. For more information, refer to ATM Processing for Europe Region Acquirers.

Country Level Authorization

Country level authorization is an optional service that allows issuers of local-use-only cards to have the Authorization Platform automatically decline all local-use-only authorization outside of their country. The Authorization Platform compares the data in the point-of-service (POS) country code field with the issuer's country. The Authorization Platform only forwards authorizations acquired within the issuer's country to the issuer for processing. The Authorization Platform declines all other transactions.

Country Level Authorization Process

Stages of the process that the Authorization Platform follows if the issuer designates the BIN for local-use only:

1. When the acquirer MIP receives an Authorization Request/0100 message, the Authorization Platform checks whether the issuer designated the BIN for local-use-only.
2. For BINs for which the issuer designated the BIN for local-use-only, the Authorization Platform compares:
   - The issuer's country on file at Mastercard to
   - The POS Country Code, DE 61 (Point-of-Service [POS] Data), positions 14–16 of the Authorization Request/0100 message.
   - An accurate match depends on acquirers including the correct data in this field.

WHEN the issuer's country…	THEN the Authorization Platform…
Matches the POS Country Code	Continues with normal processing.
Does not match the POS Country Code	Returns a response of 62 (Restricted Card) in DE 39 (Response Code) of the Authorization Request Response/0110 message.

NOTE: Use of the Country Level Authorization service does not alter a customer's responsibility for the use of local-use-only cards outside the country of issuance, including liability for all authorized and all below-the-floor-limit transactions. In addition, Mastercard assumes no liability for improper authorizations of such transactions that may result from issuer, acquirer, or merchant errors, or from Authorization Platform or Country Level Authorization service outages.

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 following country- and currency-related data fields in the MDES pre-digitization and ASI messages according to the configurations provided by the issuer during the onboarding process:

- DE 43 (Card Acceptor Name/Location for All Transactions), subfield 5 (Card Acceptor State or Country Code)
- DE 49 (Currency Code, Transaction)
- DE 61, subfield 13 (POS Country Code)

Credential on File Transaction Processing

A Credential on File transaction is a transaction in which a cardholder has explicitly authorized a merchant or payment facilitator's sub-merchant to store the cardholder's Mastercard® or Maestro® account information (PAN and expiration date, or tokenized PAN and expiration date), and the cardholder subsequently authorizes that same merchant to bill the cardholder's stored Mastercard or Maestro account.

DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), value 10 (Credential on File) identifies Mastercard-branded Credential on File transactions submitted to the Mastercard Network.

The Credential on File indicator:

- Allows a merchant to identify a pre-existing relationship with a cardholder to the issuer, using an identifier that is common across the payments industry.
- Increases approval rates for e-commerce transactions initiated with cardholder payment credentials already stored by, or on file with, the merchant or the service provider.
- Helps to make identification of types of Credential on File transactions clearer for issuers, as there are only slight differences between Credential on File recurring payment transactions and Credential on File e-commerce transactions.

Transactions Identified as Credential on File

The following are categorized as Credential on File transactions and should be identified with the Credential on File indicator:

- Recurring payments
- Installment payments

- E-Commerce and Mail Order/Telephone Order (MO/TO) transactions for which the cardholder authorizes the merchant to use the Credential on File for payment
- Card-not-present transactions originating from a merchant's brick-and-mortar location for which the cardholder authorizes the merchant to use the Credential on File
  - Credential on File transactions are always initiated without the presence of a card; however, they can be cardholder-present transactions in which the cardholder authorizes the merchant to use card credentials stored during a previous consumer interaction. An example of such a transaction is when a consumer makes a purchase at a physical location of a pharmacy that supports both physical/retail and remote business (mail, phone, or e-commerce). The consumer may have previously interacted with the pharmacy through a remote channel using their Mastercard account number and provided permission to store the number for future use. If the consumer walks into one of the pharmacy's retail locations to pick up a prescription, the merchant may offer the consumer an option to pay using the stored credential. In this case, the transaction is cardholder-present, card-not-present, and requires the use of the Credential on File identifier.
- Account Status Inquiry (ASI) messages
  - The absence of the Credential on File value in a Purchase ASI or Recurring ASI message should indicate a one-time request to validate card status or a request to validate prior to saving as Credential on File for future purchases or recurring payments.

Cross-Border Fee Manager Service

Issuers have the option to enroll in the Cross-Border Fee Manager service, an on-behalf service that allows the application of issuer-determined cardholder fees for cross-border and currency conversion transactions.

Cross-Border Fee Manager Service Overview

The Cross-Border Fee Manager service allows issuers to have the flexibility to set markup fees for both currency-conversion and cross-border transactions, taking into account a variety of parameters.

- Account range for Mastercard, Debit Mastercard, Maestro, and Cirrus acceptance brands
- Region differentiation (for example, intraregional versus interregional)
- Processing groups (for example, point of sale [POS], ATM, Card-present, card-not-present, and so on)
- Transaction currency

In combination with the default service in Clearing, issuers can select Authorization as an option. Markup fees are added to the cardholder billing amount (DE 6) without any impact to other data fields within the authorization. The markup amount provided within Authorization serves as an estimate and may differ slightly from the amount within Clearing due to fluctuations within the currency conversion rates used to calculate the final issuer markup.

Issuers may use the Currency Conversion Method, the Cross-Border Flex Method, or both to set the markup fees for cross-border and currency conversion transactions and to 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 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.

Both of these methods are provided in the following message types:

- Authorization Request/0100
- Authorization Advice/0120—Acquirer-generated
- Authorization Advice/0120—System-generated
- Reversal Request/0400 (full and partial)
- Reversal Advice/0420—System-generated (full and partial)

Issuers can optionally set up to three different markup fee overrides based on any transaction currency at the account range level for both Authorization and Clearing. If the transaction currency matches the override currency, the markup fee override is used to calculate the markup versus the issuer's default service setting for all other currencies. Issuers may use these overrides to change the existing markup fee setup or even nullify the markup service (using a 0 percent override) for lower risk currencies, or to increase the fee for higher risk, volatile currencies.

Mastercard calculates the Currency Conversion Method and Cross-Border Flex Method amounts based on the markup services the issuer opts into and fees established by the issuer at the account range level. Mastercard incorporates these calculated amounts into DE 6 (Amount, Cardholder Billing) as described in the following table.

Method Description	Condition of Application	Markup Calculation
Currency Conversion Method	DE 49 (Currency Code, Transaction) is different from DE 51 (Currency Code, Cardholder Billing)	Percentage rate, fixed amount, or both
Cross-Border Flex Method	DE 43, subfield 6 is different from the issuer country code (defined at account range level)	Percentage rate, fixed amount, or both

NOTE: The Cross-Border Flex Method does not apply to intra-European transactions where the country codes of the merchant and the account range are both in the extended Eurozone (Euro countries plus Sweden) and the transaction currency is euros (EUR).

By participating in either of the methods (Currency Conversion Method and Cross-Border Flex Method), issuers have the option to use a combination of the following parameters at an account range level, which can be applied to the total cardholder billing amount:

- Account range for Mastercard, Debit Mastercard, Maestro, and Cirrus acceptance brands
- Region differentiation
- Processing groups (for example, point of sale [POS], ATM, Card-present, card-not-present, and so on)
- Transaction currency

For both of these methods, issuers can apply different fees for intraregional and interregional identifiers.

Cross-Border Fee Manager Service Enrollment

The *Cross Border Fee Manager Customer Form* (Form 1155d), available on Mastercard Connect™, must be completed and submitted before issuers can participate in the Currency Conversion Method, the Cross-Border Flex Method, or both, as part of the Cross-Border Fee Manager service.

This form should be submitted to the issuer's local customer delivery manager.

NOTE: Issuers may only participate in the Currency Conversion Method and the Cross-Border Flex Method where permitted by local regulations.

Mastercard allows participating issuers or issuers that plan to register for the Cross-Border Fee Manager service to select Authorization as an option, in combination with the default service in Clearing.

Currency Conversion Processing

The Authorization Platform automatically provides a currency conversion service to acquirers and issuers to allow processing of online 01xx authorization and 04xx reversal transaction messages in the customer's preferred currency.

Acquirers may submit online messages in any valid local transaction currency. Acquirers and issuers will receive amount-related data elements in the acquirer's transaction currency and 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).

Acquirers and issuers that want to change the option to receive settlement amount-related data elements must complete the *Currency Conversion Parameters—Acquirer and Issuer Usage* (Form 391).

Currency Conversion Rates

The Authorization Platform uses wholesale mid rates to perform currency conversion between two currencies. The T057 Currency Conversion Rate File provides customers with Mastercard-

Issued USD Rates and Mastercard-Issued Cross Rates, including wholesale mid rates. These wholesale mid rates are denominated against the U.S. dollar.

Currency Conversion Calculation

The Authorization Platform converts from a source currency to a destination currency using the wholesale mid rates of the two currencies.

For example:

Source currency rate vs. U.S. dollars	= 2.000000
USD rate	= 1.000000
Destination currency rate vs. U.S. dollars	= 3.000000
Source amount	= 1,000
USD amount	= 500 (1000 x 1.000000/2.000000)
Destination amount	= 1,500 (1000 x 3.000000/2.000000)

Amount-related Data Element Usage

How acquirers and issuers send and receive amount-related data elements in online messages is listed in table format.

Data Element	Acquirer Sends	Issuer Receives	Issuer Returns	Acquirer Receives
DE 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

Data Element	Acquirer Sends	Issuer Receives	Issuer Returns	Acquirer Receives
DE 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. 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	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. 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.

Data Element	Acquirer Sends	Issuer Receives	Issuer Returns	Acquirer Receives
DE 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. 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 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. 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.

Data Element	Acquirer Sends	Issuer Receives	Issuer Returns	Acquirer Receives
DE 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. 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 28	In acquirer's transaction currency	In acquirer's transaction currency	In acquirer's transaction currency (echo)	In acquirer's transaction currency
DE 49	Acquirer's transaction currency code	Acquirer's transaction currency code	Acquirer's transaction currency code (echo)	Acquirer's transaction currency code
DE 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. 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.

Data Element	Acquirer Sends	Issuer Receives	Issuer Returns	Acquirer Receives
DE 51	N/A	Issuer's cardholder billing currency code	Issuer's cardholder billing currency code (echo)	Issuer's cardholder billing currency code. 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 54	If applicable to the transaction, one occurrence of each amount type in acquirer's transaction currency	One occurrence of each amount type in acquirer's transaction currency One occurrence of each amount type in issuer's cardholder billing currency	If applicable to the transaction, one occurrence of each amount type in issuer's cardholder billing currency (not an echo of what the acquirer sent)	One occurrence of each amount type in acquirer's transaction currency One occurrence of each amount type in issuer's cardholder billing currency

Data Element	Acquirer Sends	Issuer Receives	Issuer Returns	Acquirer Receives
DE 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	Same values as received (echo)	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 in U.S. dollars if acquirer 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 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 3 in issuer's cardholder billing currency
		DE 95, subfield 4 zero-filled		DE 95, subfield 4 zero-filled

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.

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.

Currency Conversion Form

Issuers must complete the *Currency Conversion Parameters—Acquirer and Issuer Usage* (Form 391) to specify their cardholder billing currency and to indicate if they want to receive amount-related data elements in the settlement currency (U.S. dollars) in authorization and reversal messages.

Additionally, acquirers must complete the Currency Conversion Parameters—Acquirer and Issuer Usage form to indicate if they want to receive amount-related data elements in the settlement currency (U.S. dollars) in authorization and reversal messages.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Digital Secure Remote Payment

A DSRP transaction is an electronic commerce Transaction that contains cryptographic information, in the form of either full EMV chip data passed in DE 55 or a cryptographic value derived from an M/Chip cryptogram passed in the Universal Cardholder Authentication Field (UCAF). Subsequent to the initial DSRP transaction, a related transaction for a partial shipment may occur, in which case, cryptographic information is not passed. When a DSRP transaction contains tokenized account information, MDES performs token mapping and cryptographic validation services.

DSRP transactions have the capability to include dynamic data to provide evidence that cardholder verification has been performed.

DSRP transactions can be initiated from:

- Any device that can perform cardholder verification, including mobile devices and properly secured web-based implementations
- Token Requestors (such as merchants or commerce platforms) participating in MDES for Merchants and MDES for Commerce programs.

Typical scenarios for these transactions include:

- Mobile e-commerce scenarios where cardholders use either their mobile browsers or a specific merchant application to purchase goods or services
- Merchant tokenization scenarios where cardholders purchase goods or services from a merchant website that participates in MDES for merchants

The use of a mobile application also offers the potential for shopping experiences in which DSRP can be used in circumstances where traditionally a face-to-face transaction at a physical point-of-sale device would have been conducted. For example, a merchant may provide an application that allows the cardholder to use the camera on a mobile device to scan the barcodes of goods in a brick and mortar store. When the cardholder has completed shopping, rather than going to a cashier to check out and pay, the cardholder may pay using DSRP through the mobile application, and leave the store with the goods without going to a cashier to checkout.

Because DSRP enables both e-commerce and replacement of a face-to-face payment in store, the two scenarios are distinguished in the Dual Message System (Authorization) and Single Message System transactions through the use of the POS Terminal Location field.

Depending on the implementation, DSRP transactions may or may not provide fraud liability protection to the merchant. This is indicated in the Dual Message System (Authorization) and Single Message System transactions through the use of different values of Security Level Indicators (DE 48 [Additional Data—Private Use], subelement 42 [Electronic Commerce

Indicators], subfield 1 [Electronic Commerce Security Level Indicator and UCAF Collection Indicator]).

Electronic Commerce

Electronic commerce (e-commerce) transactions are non–face-to-face, online transactions that use electronic media over any public network such as the Internet, or private network such as an extranet. E-commerce processing allows transactions to be initiated from a cardholder-controlled device, such as a PC or mobile phone, for purchasing goods and services on the Internet.

Customer Requirements

To process e-commerce transactions:

- All issuers must be able to receive and process all e-commerce data present in the Authorization Request/0100 messages.
- All acquirers must properly identify e-commerce messages within the Authorization Request/0100 message. They must be able to receive and to process e-commerce Authorization Request Response/0110 messages.

For detailed transaction flows and requirements associated with participation in the Mastercard® *Identity Check* program, refer to the *Identity Check Program Guide* and *Mastercard Identity Check Program Guide*. For details about data requirements and transaction processing specifications, refer to the *Customer Interface Specification* manual.

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 presentments 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 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.

E-Commerce Split or Partial Shipments

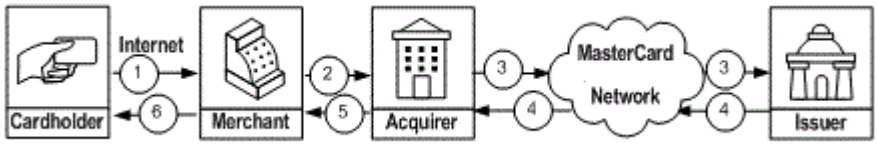
The following are options for managing e-commerce split or partial shipments.

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.

Process for an Electronic Commerce Transaction

A typical e-commerce transaction is depicted in the following graphic.

Electronic Commerce Transaction Flow



1. The cardholder accesses a merchant's website via the Internet and requests to make a purchase.
2. The merchant submits the cardholder's information to the acquirer.
3. The acquirer sends an Authorization Request/0100 message via the Mastercard Network to the issuer.
4. The issuer makes the authorization decision and replies using an Authorization Request Response/0110 message.
5. The acquirer responds to the merchant.
6. The merchant completes the transaction according to the authorization response returned.

Partial Reversal Processing—Europe Region

Since 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, a

merchant is not required to submit a partial reversal if the remaining items are processed by Mastercard clearing within 24 hours of finalization of the transaction.

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 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.

E-Commerce Split or Partial Shipments

Options for managing e-commerce split or partial shipments are listed in table format.

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.

Automated Fuel Dispenser Transactions

An automated fuel dispenser transaction identified with MCC 5542 (an AFD transaction) may occur through the use of a digital application as an "in-app" payment. Such AFD transactions must comply with all e-commerce transaction processing requirements. In addition, AFD e-commerce transactions use the same processing flow as those occurring at cardholder-activated terminals, with respect to the use of preauthorization and advice messages.

An AFD e-commerce transaction preauthorization request may be submitted for an estimated amount, followed by an advice message advising the issuer of the final transaction amount. In the Europe region, the acquirer must send an authorization advice message advising the issuer of the final transaction amount within 20 minutes of receiving the issuer's approval of the preauthorization request.

In the United States and Canada regions, the preauthorization request may be sent either for an estimated amount, or for USD 1 or CAD 1 respectively. If approved by the issuer, then within 60 minutes of the time that the authorization request message was sent, the acquirer must send an Authorization Advice/0120 message for the final transaction amount (or a Reversal Request/0400 message if the transaction will not be completed or will finalize for a lesser amount than requested). If the issuer has placed a hold on cardholder funds in excess of USD 1 or CAD 1, as applicable, then within 60 minutes of receiving the acquirer's advice message, the issuer must release any hold amount that exceeds the final transaction amount specified.

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.

NOTE: As an alternative, the Trace ID of the original preauthorization may be used for clearing presentment if that same Trace ID is included in the AFD completion advice message within DE 48, subelement 63 (Additional Data, Trace ID).

Security of Electronic Commerce Transactions

There are various methods for securing e-commerce transactions that customers may process through the Mastercard Network.

Mastercard messaging requirements regarding e-commerce may vary depending on the security protocol involved in the transactions. Security protocols may include:

- No security protocol
- Channel encryption, which is a security layer that resides between an application and its transport layers, for example, SSL (Secure Sockets Layer) and HTTPS (Hypertext Transfer Protocol Secure)
- *Identity Check* transaction using the Universal Cardholder Authentication Field (UCAF™)

If an e-commerce item that ships late is re-authorized for message reason code 4808 (Authorization-Related Chargeback) chargeback protection, this transaction will take on the security characteristics of the original authorization within a dispute resolution.

NOTE: Without UCAF data present, a re-authorized transaction must be presented within clearing for non-UCAF interchange (as applicable by region).

For more information about *Identity Check*, including detailed transaction flows and participation requirements, refer to the *Mastercard Identity Check Program Guide*.

E-Commerce Payment Transactions Using Tokens with or without Cryptographic Data

Effective 12 June 2018, Mastercard allows payment transactions to process without a cryptogram in DE 48 (Additional Data—Private Use), subelement 43 (Universal Cardholder Authentication Field [UCAF]) when they also contain DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 28 (Payment Transaction) in the Authorization Request/0100 message.

This functionality applies to the following transaction types:

- Electronic commerce (e-commerce)—Identified by DE 22 (POS Entry Mode), subfield 1 (POS Terminal PAN Entry), value 81 (PAN/Token entry via electronic commerce with optional Identity Check-AAV or DSRP cryptogram in UCAF or the Digital Payment Data Field)
- Credential on File—Identified by DE 22, subfield 1, value 10 (Credential on File)

Mastercard will reject payment transaction requests involving tokens without cryptograms that are not identified as payment transaction (DE 3, subfield 1, value 28).

Digital Secure Remote Payment with UCAF Data

Mastercard provides DSRP to enable secure mobile-originated transactions for remote payments.

DSRP authorization request messages may be transmitted either with cryptographic data within the UCAF field or the Digital Payment Data field, or with full EMV data.

For details about DSRP, including examples of process flow, refer to Digital Secure Remote Payment.

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.

Accountholder Authentication Value

The Accountholder Authentication Value (AAV) is a *Identity Check*-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. All AAVs must be generated using the Mastercard SPA algorithm. With the EMV® 3-D Secure protocol and the Mastercard Identity Check program, Mastercard has created a new SPA algorithm called SPA2. For more information about this new algorithm, refer to the *SPA2 AAV for the Mastercard Identity Check Program* manual on Mastercard Connect™.

AAV can be generated by the issuer or Mastercard and the presented to the merchant for placement in the authorization request upon successful authentication of the cardholder or attempted authentication of the cardholder. 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 during the Authorization Request/0100 messages, either through their own self-validation process or through the Mastercard ***Identity Check*** AAV Verification service.

All customers must participate in Mastercard *Identity Check* AAV Verification in Stand-In Processing if they perform self-validation during normal authorization processing.

To implement the Mastercard *Identity Check* AAV Verification service, complete the *Key Validation Service Specification Form* (Form 735).

NOTE: All issuers globally that participate in Stand-In processing must have *Identity Check* Dynamic AAV verification in Stand-In performed during Stand-In processing.

Effective on or before 1 April 2017 based on region specific effective dates per *Global Operations Bulletin* No. 4, 1 April 2016, Revised Standards for Validation Services During Stand-In Processing, all issuers globally that participate in Stand-In processing must have Dynamic CVC 3 Validation in Stand-In performed during Stand-In processing.

Effective April 2019, issuers have the option to exchange a SPA1 key or not during enroll for the AAV Validation service by completing Form 735 (Key Validation Services).

Digital Payment Data Field (DE 104)

The Digital Payment Data field enables acquirers to provide both a Digital Secure Remote Payment (DSRP) cryptogram in DE104, subelement 001 and Identity Check 3DS Accountholder Authentication Value (AAV) in the existing UCAF field (DE48, subelement 43) in a Dual Message System Authorization request transaction and a Single Message System Financial Transaction request.

Before release 19Q4 there was only one field (UCAF field) to carry the cryptography data, resulting in acquirers dropping the DSRP cryptogram and providing the 3DS AAV. The initial purpose of this field is to carry the DSRP cryptogram, but as new methods of validating digital transactions emerge, the field may be used to carry additional types of digital-related data.

Tokenized E-Commerce Transactions with Dynamic Payment Credentials

To support Digital Secure Remote Payments (DSRP) Universal Cardholder Authentication Field™ (UCAF) transactions, merchants and acquirers that participate in the Mastercard Digital Enablement Service (MDES) must make changes to their systems. Mastercard has mitigated these impacts by leveraging both a Dynamic Token Verification Code and Dynamic Expiration Date, enabling the transaction to process like a traditional e-commerce payment.

Mastercard employs this authentication option using two fields:

- Dynamic Token Verification Code—Merchants that support card validation code 2 (CVC 2) capabilities can supply the Dynamic Token Verification Code (provided by Mastercard) to the acquirer for inclusion in DE 48 (Additional Data—Private Use), subelement 92 (CVC 2).
- Dynamic Expiration Date—Along with the Dynamic Token Verification Code, the merchant provides a Dynamic Expiration Date to the acquirer for inclusion in DE 14 (Date, Expiration).

NOTE: This option uses data fields CVC 2 and Expiration Date, which already exist in Authorization Request/0100 messages. The dynamic data is used for Mastercard internal processing only and is not sent to issuers.

Mastercard also allows the processing of MDES e-commerce transactions that contain a Mastercard Identity Check merchant attempt AAV value in the UCAF field and have been successfully authenticated by the Dynamic Token Verification Code and Dynamic Expiration Date.

Mastercard *Identity Check*

Mastercard® *Identity Check*™ builds 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. In addition, the Mastercard Identity Check Authentication Program has been introduced as a global authentication program building on the best parts of *SecureCode* and focusing on consumer experience. The Mastercard Identity Check Authentication Program also supports the better methods of authentication and eliminates static passwords and activation during shopping. Mastercard *Identity Check* is the successor program to *SecureCode*, and both programs will run in parallel until *SecureCode* is phased out.

NOTE: Mastercard Identity Check will replace Mastercard *SecureCode* as the consumer-facing brand for Mastercard's Identity suite of authentication solutions by December 2019. For more information, refer to *Global Security Bulletin* No. 6, 15 June 2017 or the *Mastercard Identity Check Program Guide*.

Mastercard *Identity Check* AAV Verification Service

Mastercard offers a Mastercard® *Identity Check*™ AAV verification service on every authorization transaction that contains the Universal Cardholder Authentication Field (UCAF™) data regardless of whether the issuer's host system is available or unavailable to respond to the Authorization Request/0100 message.

Effective 21 April 2017, participation in the Mastercard *Identity Check* AAV Verification service on every authorization transaction is mandatory for all issuers. Issuer self-validation is an implementation option.

For more information about using the Mastercard *Identity Check* AAV Verification service, refer to the *Customer Interface Specification* manual.

NOTE: Mastercard Identity Check will replace Mastercard® *SecureCode*™ as the consumer-facing brand for Mastercard's Identity suite of authentication solutions by December 2019. For more information, refer to *Global Security Bulletin* No. 6, 15 June 2017 or the *Mastercard Identity Check Program Guide*.

Mastercard *Identity Check* AAV Verification in Stand-In Processing

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.

NOTE: All issuers globally that participate in Stand-In processing must have *Identity Check* AAV Verification in Stand-In performed during Stand-In processing.

Effective on or before 1 April 2017 based on region specific effective dates per *Global Operations Bulletin* No. 4, 1 April 2016, Revised Standards for Validation Services During Stand-In Processing, all issuers globally that participate in Stand-In processing must have Dynamic CVC 3 Validation in Stand-In performed during Stand-In processing.

For more information about using the Mastercard *Identity Check* AAV Verification in Stand-In Processing service, refer to the *Customer Interface Specification* manual.

NOTE: Mastercard Identity Check will replace Mastercard® *SecureCode*™ as the consumer-facing brand for Mastercard's Identity suite of authentication solutions by December 2019. For more information, refer to *Global Security Bulletin* No. 6, 15 June 2017 or the *Mastercard Identity Check Program Guide*.

Mastercard Attempts and Smart Authentication AAV Service

The Attempts Service for Mastercard *Identity Check* will provide an Attempts AAV indicating the merchant attempted contact with the Mastercard Directory Server. When a merchant contacts the Mastercard Directory Server and either the PAN's BIN or the PAN is not enrolled in Mastercard *Identity Check*, Mastercard will provide an Attempts AAV to show that the merchant attempted authentication. The AAV must be present when an Attempts transaction is submitted in authorization.

The Smart Authentication service is a stand-in authentication service implemented for the EMV 3DS Identity Check platform. Smart Authentication adds intelligence to Attempts Processing from the legacy Identity Check Platform. The intelligence is a risk-based authentication (RBA) model managed by Mastercard, leveraging data from all Mastercard sources of authentication, authorization, fraud, SafteyNet, and other services. This model allows Mastercard to provide stand-in authentication services by fully authenticating low-risk authentications, as well as merchant-only attempts to authenticate non-low-risk authentications. This enhances the Attempts Processing service from the legacy platform to inform issuers of risk rather than merchant-only authentication attempts.

The new Attempts and Smart Authentication processing service will now provide an AAV under three scenarios:

- For stand-in when the issuer Access Control Server is unavailable.
- The account range is enrolled in Mastercard *Identity Check*, but the cardholder is not enrolled in Mastercard *Identity Check*.
- The issuer account range is not participating in Mastercard *Identity Check*.

Identity Check Authentication Platforms

Mastercard Identity Check Authentication Program was introduced in 2017 as a successor program to Mastercard *SecureCode*. Mastercard Identity Check uses the best features of *SecureCode*, including the liability shift protection and interchange programs, and places focus on the consumer experience. Mastercard Identity Check will no longer support the static

password or activation during shopping, which has been associated with cardholder abandonment. Mastercard Identity Check will support risk-based decision-making, biometrics and one time use codes and will integrate the latest version of 3DS protocol to support in application payments and non-browser authentication.

All Mastercard acquirers and issuers currently participating in *SecureCode* must be compliant with using the Mastercard Identity Check by December 2019. Program enrollment is required for the Mastercard Identity Check Authentication Program.

Licensing *Identity Check* Specifications

The design specifications associated with Mastercard *SecureCode*/Mastercard Identity Check are based on Mastercard intellectual property. Mastercard licenses the specification to technology vendors and customers to integrate into their current authentication security solutions and platforms.

Technology vendors that want to integrate Mastercard *Identity Check* functionality into current or future products first must establish licensing agreements with Mastercard.

NOTE: Mastercard Identity Check will replace Mastercard® *SecureCode*™ as the consumer-facing brand for Mastercard's Identity suite of authentication solutions by December 2019. For more information, refer to *Global Security Bulletin* No. 6, 15 June 2017 or the *Mastercard Identity Check Program Guide*.

For More Information

For more information about Mastercard *Identity Check*, including detailed transaction flows and participation requirements, see the *SecureCode Implementation Guides* and *Mastercard Identity Check Authentication Program Guide—U.S. Region* available for acquirers and issuers.

For additional information about the data elements required to support the use of UCAF™, refer to the *Customer Interface Specification* manual.

Mastercard Utility Payment Program

The Mastercard Utility Payment Program is a specific utility/bill payment program that leverages the Maestro® Recurring Payments Program.

The Mastercard Utility Payment Program is maintained as a separate program to address potential differences associated with bill payments in areas such as fraud risk and registration requirements. The technical and implementation requirements for the Mastercard Utility Payment Program are consistent with the Maestro® Recurring Payments Program.

This program is available for registered billers and restricted to the following utility and bill payment card acceptor business codes (MCCs):

- MCC 4814, MCC 4816, MCC 4899 (Telecommunication, Internet Access, Cable and Satellite television services)
- MCC 4900 (Utilities)
- MCC 6300 (Insurances)
- MCC 6050 (Quasi Cash—Member Financial Institution)
- MCC 6051 (Quasi Cash Merchant)

Program Details

The Mastercard Utility Payment Program offers enrolled billers:

- Recurring card payments for automating bill payments—The cardholder establishes a relationship with a merchant to receive ongoing services and gives permission to the merchant to bill his or her account on a recurring basis. The merchant periodically initiates transactions that may be a fixed amount or may vary with each billing.
- E-billing integration, optimizing the payment experience of electronically presented bills—Billers can optimize the payment experience of electronic bills by integrating a card based payment option. The program enables billers to add a payment button to the electronic invoice providing cardholders with a one-click bill payment experience. The biller provides an environment where the electronic bill will be presented and invites the consumer to register. The consumer registers a Maestro card number and credentials allowing cardholder authentication.

Implementation Requirements

For recurring payments, the first transaction can either be a face-to-face transaction at a point-of-sale (POS) terminal (where PIN is required) or an online e-commerce transaction (requiring Mastercard® *Identity Check*™). If the first payment from the cardholder is authorized by the issuer, the biller can submit subsequent payments by the same cardholder using the same card account without the use of Mastercard *Identity Check*.

For e-billing integration, the first transaction must be submitted as an e-commerce transaction and the biller must request Mastercard *Identity Check* authentication. If the first payment from the cardholder is authorized by the issuer, the biller can submit subsequent payments by the same cardholder using the same card account without the use of Mastercard *Identity Check*.

All payments under the Mastercard Utility Payment Program are identified by a specific Accountholder Authentication Value (AAV) in DE 48 (Additional Data—Private Use), subelement 43 (Universal Cardholder Authentication Field [UCAF]) in the Authorization Request/0100 message:

5MUPPPROGRAM9999999999999999

Enrolled billers receive a Mastercard Assigned ID and are allowed to process Maestro® transactions without the use of Mastercard *Identity Check* once an initial transaction is successfully verified with either Mastercard *Identity Check* or PIN.

Where a transaction is submitted with a static AAV, the issuer will have a chargeback right for reasons of fraud, which would be resolved via standard procedures.

To Participate

Participants need to demonstrate bill payment activity and must guarantee minimum security requirements. To enroll billers in this program, the acquirer must complete a participation request form, available in the e-Commerce section (under e-Business on the main menu) and on the Publications page on Mastercard Connect™.

Maestro Low Risk Merchant Program for E-Commerce Transactions

Mastercard provides a new European program to enable Maestro® e-commerce transactions to be conducted using a risk-based approach to customer authentication for pre-identified categories of low-risk transactions.

NOTE: Applies only to the Europe region.

Background

The European Banking Authority (EBA) has produced a set of guidelines that addresses the security of Internet transactions, including strong authentication requirements for Internet payments.

In most European Economic Area (EEA) countries, Mastercard expects an increase in Mastercard® *Identity Check*™ adoption by merchants and an increase in Maestro® e-commerce acceptance.

The EBA Guidelines allow also for merchants to undertake a risk-based approach to authentication. In particular, the EBA Guidelines allow alternative authentication measures for low-risk payments to balance security with consumer convenience during the online transaction authentication process.

Benefits

Recognizing the EBA Guidelines, the purpose of the new Maestro Low Risk Merchant Program for e-commerce transactions is:

- To reduce fraud in online payments
- To encourage merchants to implement *Identity Check*
- To promote a risk-based approach to *Identity Check* authentication
- To promote an enhanced checkout experience for Maestro cardholders

The Maestro Low Risk Merchant Program will enable low-risk, high-volume e-commerce merchants to conduct Maestro e-commerce transactions using a risk-based approach to *Identity Check* authentication, as long as this is effective in maintaining fraud at a level within the 10 basis points program threshold as defined in the following sections Eligibility Requirements and Operations Requirements.

The new program allows approved e-commerce merchants to use alternative authentication measures for pre-identified categories of Maestro low-risk transactions on the condition that the Maestro issuer bank identification number (BIN; account range) is enrolled in the program. The definition of low-risk transaction is a responsibility of the approved merchant.

As a result of a merchant-led risk assessment, approved e-commerce merchants may accept Maestro transactions without having to attempt strong *Identity Check* authentication in every instance.

However, approved merchants must obtain *Identity Check* strong authentication from the Maestro issuer on registration of card payment data with the merchant account and on high-risk transactions. The definition of high risk is the responsibility of the approved merchant.

For the Maestro issuer BINs not enrolled in the program, approved merchants must attempt *Identity Check* strong authentication on all Maestro e-commerce transactions irrespective of low-risk or high-risk definition.

Program Participants

The Maestro Low Risk Merchant Program is a Europe region program and applies to acquirers of Maestro e-commerce merchants in the Europe region and to issuers of Maestro cards supporting e-commerce in the Europe region.

Eligible acquirers shall have a licensed area of use in the Europe region. Eligible merchants shall be in the acquirer's licensed area of use. They must be low-risk, high-volume e-commerce merchants. The request to participate into the program shall be submitted by the merchant and its acquirer.

The new program is designed for e-commerce merchants that store consumers' payment details on file so that they recognize the consumer when that person returns and makes a subsequent payment. Merchants' participation in the program is optional.

All issuers of Maestro cards supporting e-commerce in the Europe region will be by default enrolled at program set-up and deemed to be supportive of merchant-led risk-based assessment. The account ranges of enrolled issuers will be communicated to the approved merchants.

For the avoidance of doubt, issuers in the Europe region that do not support Maestro e-commerce are out of scope and Europe region-issued Mastercard cards are out of scope.

Eligibility Requirements

For each merchant, the acquirer will complete a participation request form. Mastercard staff will review the participation request form, and notify the acquirer if the merchant has been enrolled in the Program.

Merchant participation in the Maestro Low Risk Merchant Program is subject to an eligibility check process to verify that the e-commerce merchant fulfills the following program requirements:

- Acquired volume exceeding 100,000 EUR per month for the last 12 months
- Fraud rates of less than or equal to 10 basis points for the two consecutive quarters preceding the application. If the e-commerce merchant has two or more acquiring Interbank Card Association (ICA) numbers then the fraud basis points will be calculated for each acquirer ICA number.
- Merchant support of *Identity Check* to enable strong authentication performed by the issuer
- Merchant to use *Identity Check* as per Operations Requirements described in the following section
- Agree to a Global Risk Management Program Review as part of the Maestro Low Risk Merchant Program process. Merchants will undergo the Global Risk Management Program Review on sign-up. The objective of the review is to validate the merchant eligibility requirements and make sure that the merchant has solid risk management processes. As

outlined in the *Mastercard Consolidated Billing System* manual, there will be a service fee for the Global Risk Management Program Review and it will be invoiced to the acquirer or to the acquirers.

For approved e-commerce merchants to meet the program criteria, cardholders must be able to:

- Register on the e-commerce merchant's website
- Create an account with log-in credentials
- Add the Maestro card number for use in e-commerce transactions

If all of the above eligibility requirements are met, then the merchant will receive a Mastercard-assigned ID and a Static Accountholder Authentication Value (AAV). The merchant acquirer is required to uniquely identify approved merchants within the transaction message through the Mastercard-assigned ID.

Operations Requirements

An approved merchant will obtain strong authentication from the issuer through *Identity Check* at the time of registration of Maestro card payment data with the merchant account and on high-risk Maestro e-commerce transactions. The definition of high risk is the responsibility of the approved merchant.

If the *Identity Check* authentication does not occur when the card is added to the merchant's card-on-file system, then the participating merchant must obtain a *Identity Check* authentication for the first Maestro e-commerce transaction, prior to submitting the authorization.

For subsequent transactions with the same Maestro card, the merchant is allowed to skip the *Identity Check* authentication on the condition that it is a pre-defined low-risk transaction and that the card issuer is supportive of a risk-based approach to *Identity Check* authentication. The definition of low-risk transaction is the responsibility of the approved merchant.

Participating e-commerce merchants will receive a list of Maestro issuer account ranges (Europe region-issued) that are supportive of merchant-led risk-based assessment. Approved merchants may skip the *Identity Check* authentication on these issuer account ranges on the condition that it is a low-risk transaction and the *Identity Check* authentication was obtained at the time of the card add or at first transaction.

On subsequent transactions approved merchants will use:

- DE 48 (Additional Data—Private Use), subelement 32 (Mastercard Assigned ID) in the Authorization Request/0100 message with a Mastercard-assigned ID
- DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]) in the Authorization Request/0100 message with the Mastercard-assigned Static Account Authentication Value (AAV) 5MARPPROGRAM9999999999999999 (28 positions)
- DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator) in the Authorization Request/0100 message must have the value 213 in positions 1, 2, and 3.

- PDS 0052 (Electronic Commerce Security Level Indicator), subfield 3 (UCAF Collection Indicator) in the clearing record submitted to the Global Clearing Management System (GCMS) for processing with a value of 3
- PDS 0176 (Mastercard Assigned ID) in the clearing record submitted to GCMS for processing with a Mastercard-assigned ID

Approved merchant fraud levels will be measured by acquirer ICA on a quarterly basis. Should the fraud threshold of 10 basis points be exceeded in any single quarter, the acquirer and the merchant will receive an advisory letter from Mastercard. Should fraud levels exceed 10 basis points for two consecutive quarters, the acquirer and the merchant will receive a second warning letter and will be required to support a further Global Risk Management Program review.

The objective of the review is to agree on a plan to bring the fraud basis points below the threshold level. Should the fraud basis points fail to go down to the threshold level, merchant participation in the program will be re-assessed. There will be a fee for the Global Risk Management Program review.

Mastercard reserves the right to lower the Program fraud threshold in the future.

Issuers' participation to the program is optional. Issuers that want to opt out of the program will have to express their withdrawal in writing to their Mastercard Account manager. For these Maestro issuer account ranges, approved merchants must accept the Maestro card and attempt a *Identity Check* authentication as these issuers will want to retain control of the risk decision.

Liability

When an approved merchant does not authenticate the cardholder using *Identity Check*, and submits a transaction under the Maestro Low Risk Merchant Program with a *Identity Check* level indicator of 3, the issuer will have the right to charge back the transaction for reason of fraud if the cardholder states that they did not authorize the transaction.

The issuer is otherwise responsible for fraud in connection with any Maestro e-commerce transaction that the issuer has approved, unless it can be proved that the merchant and/or acquirer participated in the fraud or the merchant website does not support the passing of UCAF data.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

E-Commerce Fraud Alerts for Issuers

E-commerce Fraud Alerts for Issuers requires acquirers to inform issuers when a merchant or acquirer has decided not to complete an approved card-not-present (CNP) transaction because of high-fraud risk. This information will enable issuers to appropriately monitor or block those cards to prevent future fraud.

This service will be required for CNP transactions, including e-commerce, mail order/telephone order (MOTO), and recurring payment transactions.

Benefits

E-commerce Fraud Alerts for Issuers provides the following benefits:

- Provides issuers with a very predictive indicator about cards that need to be monitored due to suspicious behavior
- Allows issuers, acquirers, and merchants to reduce fraud losses, chargebacks, and associated costs by enabling issuers to intervene early on alerted card accounts
- Enables increased collaboration and communications between merchants and issuers to take fraud out of the system and ultimately increase cardholder confidence in the system

How It Works

When an acquirer or merchant has decided not to complete an approved CNP transaction because of high-fraud risk, the acquirer must send the Authorization Platform a Reversal Request/0400 message containing DE 39 (Response Code), value 34 (Suspect Fraud).

The issuer must be prepared to receive DE 39 (Response Code), value 34 (Suspect Fraud) in Reversal Request/0400 or Reversal Advice/0420 messages and generate appropriate Reversal Request Response/0410 or Reversal Advice Response/0430 messages. Issuers must release any hold placed on the cardholder's account for the amount of the original, approved Authorization Request/0100 message.

Fees

Refer to the *Mastercard Consolidated Billing System* manual for fees and billing information.

Reports

The Issuer Authorization Detail report (AB201010-A2) will be used to support analysis of the reversal messages containing the new code. The Stand-In Detail Authorization report (AB111010–AA) will also be modified to support the new reason code value in DE 39. Refer to the *Mastercard Consolidated Billing System* manual for samples of these reports.

An issuer E-commerce Fraud Alerts for Issuers report will be available for Dual Message System transactions that contains detail transaction information. This report can be requested through PortfolioAnalytics.

Comparison of Security Protocols

A comparison of security protocols is listed in table format.

	Type of Security Protocol		
Feature	**None**	**Channel Encryption**	***Identity Check* (using UCAF; dynamic AAV)**
Protection of information over the Internet	Unprotected	Protected	Protected
Protection of information at the merchant site	Payment information unprotected. (Merchant sees all cardholder information.)	Payment information unprotected (Merchant sees all cardholder information).	Payment information unprotected unless used in conjunction with pseudo-account number solution (Merchant sees all cardholder information. Merchant should encrypt all sensitive data behind a firewall in compliance with the Payment Card Industry (PCI) Data Security Standard).
Authentication of Acquirer	No authentication	No authentication	No authentication
Authentication of Merchant for payment	No authentication	No authentication	No authentication
Authentication of Cardholder for payment	No authentication	No authentication	Reliable authentication provided by the Mastercard issuer or by Mastercard on-behalf of the issuer

Expert Monitoring for Merchants

Expert Monitoring for Merchants provides participating acquirers and merchants 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:

- Increases accuracy in fraud detection by leveraging comprehensive cardholder account transaction history to identify unusual activity.
- Lowers false positive rates and customer inconvenience by reducing investigation of transactions that appear to be fraudulent but prove to be legitimate.
- Improves order acceptance rates by maximizing revenues from legitimate orders and reducing fraud and manual review costs from fraudulent ones.
- Reduces fraud-related chargeback rates with a highly predictive fraud score that provides incremental lift in fraud detection.

How It Works

Using state-of-the-art predictive modeling technology, Expert Monitoring for Merchants provides merchants with a fraud risk score on CNP transactions at the time of transaction authorization. The score indicates the likelihood that the transaction on the associated card account is fraudulent.

Mastercard scores CNP transactions for merchants by using a CNP fraud detection model and evaluating the current CNP transaction against a comprehensive view of the cardholder's transaction behavior history.

The fraud score, which is prompted for in the authorization request message and provided within the authorization response message, is a three-digit number ranging from 001 to 998. The higher the score, the more likely it is that the transaction is fraudulent.

The fraud score can be used as a highly predictive data point and integrated into a merchant's fraud screening process.

Authorization Processing

The following stages describe the merchant fraud scoring process:

1. At the time of the transaction request, the merchant prompts the acquirer to request the merchant fraud score.
2. The acquirer requests the fraud score in the Authorization Request/0100 message and sends it to the Authorization Platform.
3. The Authorization Platform forwards the Authorization Request/0100 message to the Expert Monitoring for Merchants.
4. The Expert Monitoring for Merchants scores the transaction, using a CNP fraud detection model, generates the scores, and then provides the score to the Authorization Platform.
5. The Authorization Platform forwards the merchant fraud score results to the acquirer in the Authorization Request Response/0110 message, along with the issuer's approval/decline.
6. The acquirer sends a response containing the merchant fraud score results to the merchant.

Mastercard uses the following values in DE 48 (Additional Data—Private Use), subelement 51 (Merchant On-behalf [OB] Services), subelement 55 (Merchant Fraud Scoring Data), subelement 57 (Security Services Additional Data for Acquirers), subelement 71 (On-behalf Services), and subelement 75 (Fraud Scoring Data) of Authorization Request/0100 and

Authorization Advice/0120—System-generated messages to support transactions that qualify for fraud scoring.

The Authorization Platform inserts subelement 75 when Expert Monitoring is performed or when both Expert Monitoring for issuers and Fraud Rule Manager services are performed on the transaction. When a rule adjusted score is provided in subfield 3, at least one or more rule reason code values will be provided in subfields 4–5. However, rule reason code values may be provided in subfields 4 or 5 with or without a rule adjusted score in subfield 3.

- Subelement 51 (Merchant On-behalf [OB] Services):
  - Subfield 1 (Merchant On-behalf [OB] Service)
  - Subfield 2 (Merchant On-behalf [OB] Result 1)
  - Subfield 3 (Additional Information)
- Subelement 55 (Merchant Fraud Scoring Data):
  - Subfield 1 (Merchant Fraud Score)
  - Subfield 2 (Merchant Score Reason Code)
- Subelement 57 (Security Services Additional Data for Acquirers):
  - Subfield 1 (Security Services Indicator)
  - Subfield 2 (Security Services Data)
- Subelement 71 (On-behalf Services):
  - Subfield 1 (On-behalf [OB] Service), value 18 (Fraud Scoring Service)
  - Subfield 2 (On-behalf [OB] Result 1), value C (Successful) and U (Unable)

  Subelement 75 will not be populated when U (Unable) is the result.
- Subelement 75 (Fraud Scoring Data):
  - Subfield 1 (Fraud Score)
  - Subfield 2 (Score Reason Code)
  - Subfield 3 (Rules Adjusted Score)
  - Subfield 4 (Rules Reason Code 1)
  - Subfield 5 (Rules Reason Code 2)

NOTE: Participating acquirers may contact the Mastercard Risk Solutions Team for a list of the specific score reason codes and rule reason codes that apply to their institution.

To Participate

Acquirers and merchants that want to participate in Expert Monitoring for Merchants must complete a contract and registration form. For information about this service, acquirers should contact their Mastercard representative.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Expired Card Override

Overriding expired card tests allows issuers to override possible expiration date keying errors, to support reissued cards, and to identify transactions they may otherwise approve.

Issuers will receive all Authorization Request/0100 and Reversal Request/0400 messages containing expired expiration dates. Issuers will have the opportunity to review each transaction, and subsequently approve or decline each transaction.

NOTE: Mastercard automatically enables issuers for Expired Card Override. Issuers that want Mastercard to reject Mastercard Authorization Request/0100 and Reversal Request/0400 messages containing expired expiration dates must complete the *Expiration Date Test Form* (Form 379).

System Definition of an Expired Card

The Authorization Platform defines an expired card as a card with an expiration date that meets one of certain criteria.

- Earlier than the current processing year and month
- 20 years later than the current processing year

Customers can locate the expiration date in DE 14 (Date, Expiration), and from the magnetic stripe track, in DE 45 (Track 1 Data), or DE 35 (Track 2 Data).

Expired Card Tests

The expired card tests occur at the acquirer MIP.

The following table provides examples of Mastercard expired card test logic.

Transaction Date	Card Expiration Date (MM/YY)	Authorization Request Expiration Date (YY/MM)	Authorization Platform Response	Explanation of Logic
0910 (September 2010)	1010 (October 2010)	1010 (October 2010)	Accept	October 2010 is later than the current processing year and month. The system accepts the date as valid.
0910 (September 2010)	0209 (February 2009)	0902 (February 2009)	Decline	February 2009 is earlier than the current processing year and month. The system declines the date as expired.

Transaction Date	Card Expiration Date (MM/YY)	Authorization Request Expiration Date (YY/MM)	Authorization Platform Response	Explanation of Logic
0910 (September 2010)	0830 (August 2030)	3008 (August 2030)	Accept	August 2030 is less than 20 years from September 2010. The system accepts the date as valid, because 2030 is still within 20 years from 2010.
0910 (September 2010)	0131 (January 2031)	3001 (January 2031)	Decline	January 2031 is 20 years and four months from September 2010. The system declines the dates as expired, because 2031 is more than 20 years from 2010.

NOTE: The Authorization Platform uses DE 14 (Date, Expiration), if present, for the expired card test; otherwise, DE 35 (Track 2 Data), if available; otherwise, DE 45 (Track 1 Data), if available. If both DE 14 and track data are present, the Authorization Platform uses DE 14 only.

Issuer is Enabled for Expired Card Override

When a transaction fails the expired card tests and the issuer is enabled for Expired Card Override, the Authorization Platform forwards the Authorization Request/0100 or Reversal Request/0400 message to the issuer for processing.

Issuer is Not Enabled for Expired Card Override

If the issuer is not enabled for Expired Card Override and the transaction fails the expired card test, the Authorization Platform generates an expired card authorization response 54 (Expired Card) in DE 39 (Response Code) of the Authorization Request Response/0110 or Reversal Request Response/0410 message sent to the acquirer.

Potential Inappropriate Declines

If the issuer is not enabled for Expired Card Override, the Authorization Platform may decline cardholder transactions that the issuer would have approved if the Authorization Request/0100 and Reversal Request/0400 messages were sent to the issuer.

Expired Data Errors

Expired card tests at the acquirer MIP assume that the expiration date in the authorization message is correct. However, improper keying, misunderstanding of the date, or other human error can cause the expiration date listed in the authorization message to be incorrect.

The following table provides an example of a reason a merchant might receive an incorrect expired card authorization response.

Transaction Date	Card Expiration Date (MM/YY)	Authorization Request Expiration Date (YY/MM)	Authorization Platform Response	Explanation of Error
0910 (September 2010)	05/31/11	3105 (merchant entered 0531 instead of 0511)	Decline	May 2011 is eight months from September 2010. However, the merchant entered the month (05) and the day (31), but not the year (11). The Authorization Platform reads the expiration date as May 2031.

The system declines the date as expired, because 2031 is more than 20 years from 2010. However, the expiration date is valid, and perhaps the issuer would have accepted the transaction.

Alternate Processing

If the issuer is enabled for Expired Card Override and is unavailable, the Authorization Platform performs the expired card tests, either in Stand-In processing or during X-Code processing.

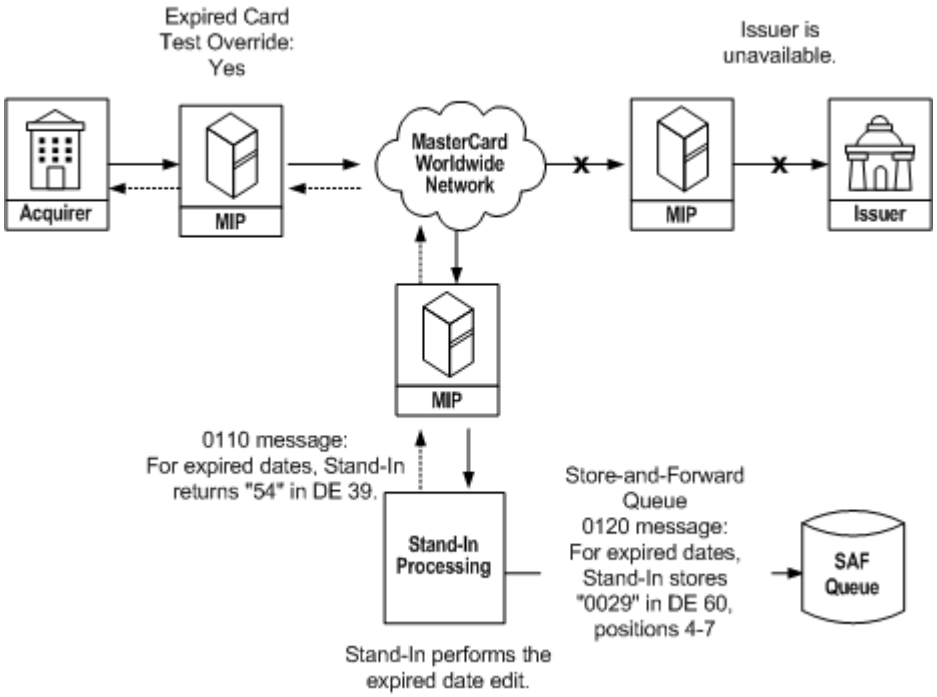
Stand-In Processing

Stand-In performs an expired card test. For transactions that fail the expired card test, Stand-In processing:

- Returns to the acquirer code 54 (Expired card) in DE 39 (Response Code) of the Authorization Request Response/0110 message.
- Stores the transaction in the Store-and-Forward queue with value code 0029 in DE 60, subfield 2 of the Authorization Advice/0120 message, available for issuer retrieval (Code 0029 indicates that Stand-In processing returned code 54 in the Authorization Request Response/0110 message).
- Identifies transactions with code 54 in the RESPONSE column or code 0029 in the FAIL RSN column on the following reports:
  - AB201010-AA (Authorization Detail)
  - AB111010-AA (Stand-In Detail Authorization)
  - AB517010-AA (Issuer Call Referral Tiered Detail)

Refer to the *Mastercard Consolidated Billing System* manual for samples of these reports.

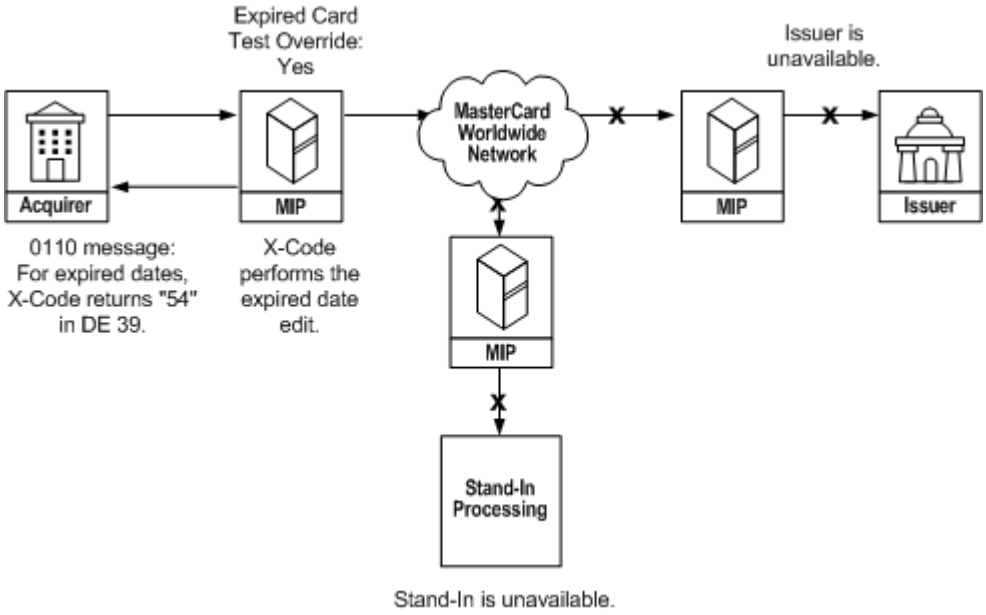
Expired Card Override—Stand-In Processing Flow



X-Code Processing

X-Code processing performs an expired card test. For transactions that fail the expired card test, X-Code processing returns to the acquirer code 54 in DE 39 of the Authorization Request Response/0110, and sends an Authorization Advice/0120 to the issuer.

Expired Card Override—X-Code Processing Flow



Fleet Card Transactions

The Mastercard Corporate Fleet Card® is designed to monitor and control fuel and maintenance expenses. A Mastercard Corporate Fleet Card program can be assigned to an individual employee or to a vehicle.

Mastercard Corporate Fleet Card transactions are identified with the following card acceptor business codes (MCCs): MCC 4468, 5499, 5541, 5542, 5983, or 7511. For more information about MCCs, refer to the *Quick Reference Booklet*.

NOTE: MCC 7511 is being life cycled and replaced with MCC 5541 (Service Stations [with or without Ancillary Services]).

Incentive Interchange Rates

Acquirers receive incentive interchange rates for transactions that support the data collection requirements of Mastercard Corporate Fleet Card® transactions.

To receive the incentive interchange rates for Fleet Card transactions, acquirers must capture specific data to support submission requirements for clearing records.

For clearing record requirements, refer to the *GCMS Reference Manual*.

Transmitting Fleet Card Data in Authorization Request/0100 Messages

To support Fleet Card transactions, acquirers must include specific data in Authorization Request/0100 messages.

To determine which data to include, the merchant terminal must recognize the Product Type Code on the magnetic stripe. The Product Type Code determines the:

- Terminal prompt at the POI location
- Data that the acquirer must include in the DE 48 (Additional Data—Private Use) field of the Authorization Request/0100 message

Terminal Prompt at the POI Location

When the merchant terminal reads the Product Type Code, the terminal responds by prompting for certain information.

Product Type Code Value	Terminal Prompt—Acquirer May Receive from Merchant
1	ID Number and Odometer
2	Vehicle Number and Odometer
3	Driver Number and Odometer
4	Odometer Only
5	No Prompt

Data in the Authorization Request/0100 Message

When the acquirer receives the Fleet Card data from the merchant, the acquirer must include some of the data in the DE 48 (Additional Data—Private Use) field of the Authorization Request/0100 message.

Product Type Code Value	Acquirer Must Include in the 0100 Message	Position in the Authorization Request/0100 Message
1	ID Number	DE 48, subelement 98
2	Vehicle Number	DE 48, subelement 99
3	Driver Number	DE 48, subelement 98
4	None	None
5	None	None

Fleet Card Authorization Response

Acquirers that support the Fleet Card program must also be able to interpret the additional data provided by the issuer in DE 44 of the Authorization Request Response/0110 message.

If the issuer declines a transaction because of an invalid driver, ID, or vehicle number, the issuer returns an Authorization Request Response/0110 message with value 12 in DE 39. The issuer will return additional data in DE 44 that explains the reason for the decline. The terminal at the point-of-interaction must display this additional data.

Initiating Fleet Card Support

To learn more about supporting the Fleet Card program, contact the Global Customer Service team.

Gambling Transaction Processing

U.S. region Mastercard and Maestro issuers must block online gambling transactions in accordance with the Standards and applicable U.S. law. Such potentially illegal online gambling transactions are declined during Stand-In System processing.

The Authorization Platform 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 Authorization Platform also supports Gaming Payment Transaction processing for the Mastercard and Maestro brands in the United States Region to transfer lottery winnings to a card.

Internet Gambling Transactions in the U.S. Region

Internet gambling transactions are identified in Authorization Request/0100 messages by these values.

- DE 18 (Merchant Type), MCC 7995 (Gambling Transactions)
- DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level Indicator), value 6 (Authorized Level 6 CAT: Electronic commerce)

The presence of both these values in an Authorization Request/0100 message indicates that the acquirer has coded the transaction as an Internet gambling transaction, and possibly a restricted transaction (that is, a payment in connection with a gambling transaction that is illegal in the U.S region).

U.S. region Mastercard and Maestro issuers must use a method of transaction blocking or decline all such transactions on an individual basis.

Issuers may approve, on an individual basis, any Internet gambling transaction authorization requests identified with MCC 9754 (Gambling—Horse Racing, Dog Racing, Non-Sports Intrastate Internet Gambling) that involve a U.S. region cardholder. In using MCC 9754, the acquirer asserts that the transaction involves gambling activity deemed by the acquirer to be legal in the U.S. region.

Issuers are not required to validate the transaction category code (TCC) value for this purpose.

Specific processing rules and Standards for Internet gambling transactions have been defined in Rule 3.7, Integrity of Brand and Network of the *Mastercard Rules*.

Stand-In System Processing

The Stand-In System limits of zero will apply for the following parameter combinations:

- MCC 7995 (Gambling Transactions)
- Cardholder-activated terminal (CAT) level 6 (Electronic Commerce Transaction)

If this parameter combination is sent to the Stand-In System for processing, the Stand-In System will reject the Authorization Request/0100 message by returning DE 39 (Response Code), value 57 (Transaction not permitted to issuer/cardholder).

These blocking parameters are also established for account range setup.

Gaming Payment Transaction Processing in the Europe and Middle East/Africa Regions

The Authorization Platform 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 (POS Terminal PAN Entry Mode):
  - Value 10 (Credential on File) and DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence), value 5 (Cardholder not present [Electronic order]), or
  - 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).

Acquirer Implementation

Acquirers must complete an implementation project to submit Payment Transactions for gaming winnings. For more information about registering for this service, contact your Mastercard regional representative or your Customer Implementation Services (CIS) Implementation Project Manager.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual and *Mastercard Rules*.

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).

Global Automated Referral Service

The Global Automated Referral Service (GARS) is a service that streamlines the process of responding to call referrals for both acquirers and issuers.

GARS is mandatory in the U.S. region and optional for customers outside the U.S. region.

Benefits

GARS reduces the processing time for call referrals from an average of 20 minutes to an average of five minutes or less.

It includes the following features:

- A toll-free phone number connecting acquirers to issuers worldwide. Routing is based on the card account number entered by the acquirer (For the toll-free phone number that applies to your area, contact the Global Customer Service team).
- Issuer response time parameters to support the timely provision of authorization responses
- Stand-In processing for calls not answered within the required time frame or for issuers not registered for GARS, to guarantee a timely response to the acquirer
- Tracking and reporting of issuer and acquirer performance
- Performance monitoring and pricing that motivate call referral completion and eliminate unnecessary issuance of call referrals

GARS Process

When the merchant receives a refer to card issuer authorization response, the merchant calls the acquirer.

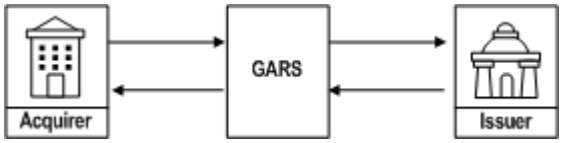
The acquirer calls GARS, which uses one of the following paths to obtain an authorization response:

- GARS connects the acquirer to the issuer

- GARS connects the acquirer to Stand-In processing

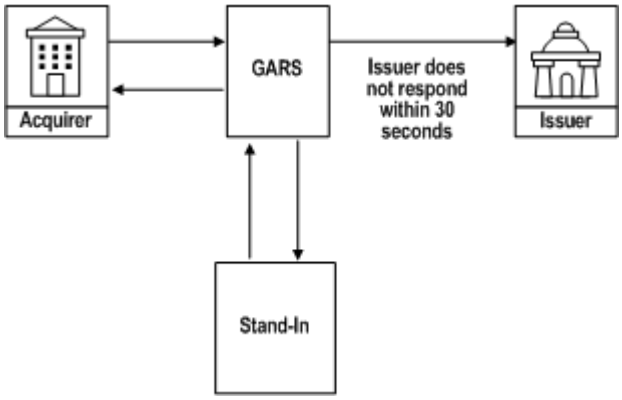
GARS Connects Acquirer to Issuer Flow

GARS connects the acquirer to the issuer. The acquirer receives the authorization response from the issuer and relays the response to the merchant.



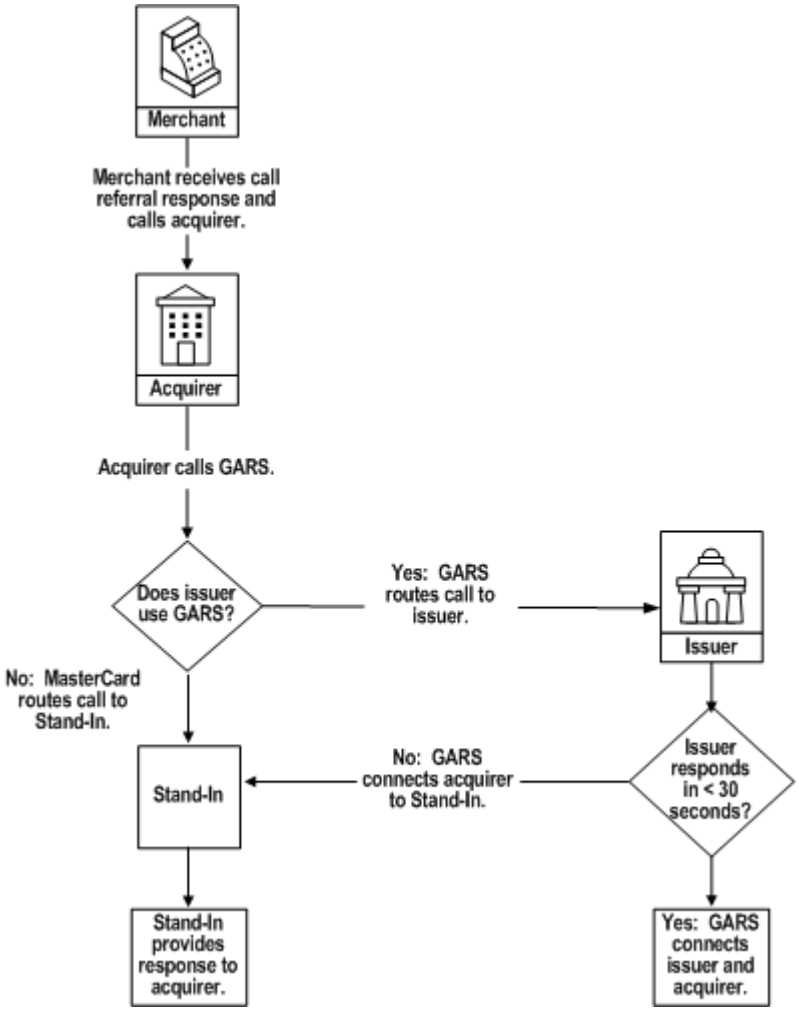
GARS Connects Acquirer to Stand-In Processing Flow

If the issuer does not respond to the phone call within 30 seconds or for issuers not registered for GARS, GARS connects the acquirer to Mastercard Stand-In processing. The acquirer receives the authorization response from Mastercard Stand-In processing. The acquirer relays the response to the merchant.



GARS Process Flow

The following diagram illustrates the entire GARS process.



Acquirer Use of GARS

GARS helps acquirers to more quickly receive a response to a call referral from issuers.

Acquirer Procedures

Acquirers receiving a refer to card issuer authorization response should use the following procedure to receive an authorization decision from the issuer.

IF…	THEN…
You receive an authorization response of refer to card issuer.	Dial the GARS phone number for your country (provided when you sign up for GARS) after issuance of the refer to card issuer message.

IF…	THEN…
GARS says, "Welcome to the Mastercard Global Automated Referral Service. If you make an error entry at any time, press the star key. Please enter the Acquiring ICA number followed by the pound sign."	Enter your six-digit billing ICA number, followed by the pound/hash sign (#).
GARS says, "The ICA number entered is XXXXXX. If correct, press one. If not correct, press two."	Press either the one (1) or two (2) key.
GARS says, "Please enter the Mastercard account number followed by the pound sign."	Enter the 16-digit Mastercard cardholder account number followed by the pound/hash sign (#).
GARS validates the Mastercard account number, dials the issuer, and the issuer comes on the line.	Discuss the authorization transaction.
The issuer provides you with an authorization response.	Provide the merchant with the issuer's authorization response.

Stand-In Processing Procedures

If the issuer does not connect with the call within 30 seconds, GARS connects you to Stand-In processing. Use the following procedure to receive an authorization decision from Stand-In processing.

IF…	THEN you should…
GARS says, "We appreciate your patience. The issuer is not available at this time. Your call will now be serviced by Mastercard Stand-In processing."	Follow the instructions given by GARS.
GARS says "Please enter the MCC number, followed by the pound sign."	Enter the MCC number and the pound/hash sign (#).
GARS says "Please enter the merchant number, followed by the pound sign."	Enter the merchant number and the pound/hash sign.
GARS says "Please enter the four digit expiration date in MM/YY format, followed by the pound sign."	Enter the four-digit expiration date in MM/YY format and the pound/hash sign.

IF…	THEN you should…
GARS says "Please enter the transaction amount in U.S. dollars and cents, followed by the pound sign."	Enter the transaction amount in U.S. dollars and cents and the pound/hash sign.
GARS says, "You entered X dollars and X cents. If correct, press 1. If not correct, press 2."	Press 2 to repeat this step.
GARS says "Please choose one of the following transaction types: • For retail, press 1. • For phone, mail order, or electronic commerce, press 2. • For cash advance, press 3. • For travel, press 4. • For all other transaction types, press 5."	Enter the number for the transaction type of this transaction.
If 5 is entered in the previous step, GARS will offer additional options: • "For automobiles, press 1. • For food, press 2. • For hotel, press 3. • For tuition or hospital, press 4. • For unique, press 5. • For payment, press 6."	Enter the number for the transaction type of this transaction.
GARS provides one of the following authorization responses: • "The approval code is XXXXXX. To repeat the approval code, press 1. To end this call, press 2." • "This transaction has been declined. Thank you for calling Mastercard International. Goodbye."	Provide the merchant with Stand-In processing's authorization response.

Acquirer Best Practices

Mastercard recommends that acquirers promote efficient and accurate processing of call referrals by using the following practices when talking to issuers' agents:

- Be prepared to provide the following authorization request information to the issuer's agent:

  - Card account number
  - Expiration date
  - Card acceptor business code (MCC)
  - Transaction amount in U.S. dollars

    If the acquirer chooses to receive DE 5 (Amount, Settlement) in the Authorization Request Response/0110 message, the acquirer may use that amount, which is stated in U.S. dollars; or the acquirer may determine the USD amount in DE 4 (Amount, Transaction) or DE 6 (Amount, Cardholder Billing). If the USD amount is not provided, the acquirer must perform currency conversion to U.S. dollars.
  - Acquirer ICA number
- Initiate the conversation with slow, distinct pronunciation. Be aware that the issuer's agent might not be comfortable with the acquirer's primary language.
- Request clarification when uncertain of the communication.

If the issuer or its agent cannot respond to the call referral in a timely manner, GARS routes the call referral to the Mastercard Stand-In processing. Acquirers should allow additional time to complete the call and be prepared to provide additional authorization information, as required by Stand-In processing.

Acquirers should monitor call referral response rates to identify merchants that do not comply with the call referral process.

Acquirers receive reimbursement automatically when they use GARS in response to a refer to card issuer authorization response.

NOTE: Reimbursement to acquirers using GARS is automatic. If acquirers use non-GARS methods of communication, they must request reimbursement through the 667 record (usage code 100).

Methods Acquirers Can Use to Improve GARS Performance

The acquirer can improve GARS performance and ensure that it qualifies for reimbursement by doing the following:

- Test your phone system to ensure that it generates true touch-tones on outbound calls. The GARS connection to the issuer is dependent on touch-tones.
- Communicate the GARS procedures to your agents. Mastercard is available to assist you in your training efforts.
- Consider adding a conference call feature to your phone system so that you, your merchant, the cardholder, and the issuer can interact directly.
- Consider adding speed dialing to your phone system to save time when calling GARS.
- Communicate the GARS procedures and the importance of GARS to your merchants. Encourage them to call you (rather than request another form of payment) when a call referral message appears on their POI devices.

Issuer Use of GARS

GARS helps issuers because it provides them with a method to more quickly respond to acquirers requesting authorizations for call referral responses.

Issuer Procedures

When you issue a response of refer to card issuer and the acquirer contacts you via GARS, use the following procedure.

IF…	THEN you should…
GARS says, "Incoming Mastercard referral call. Press the zero key and the pound key now."	Press the required zero (0) and pound (#) keys within 30 seconds. If you do not enter 0# within 30 seconds, GARS connects the acquirer to Stand-In processing for the authorization response.
GARS connects you with the acquirer to discuss the transaction.	Obtain the necessary authorization information from the acquirer and communicate your authorization response to the acquirer.

Issuer Best Practices

Mastercard recommends that issuers promote efficient and accurate processing of call referrals by using the following practices when talking to acquirers' agents:

- Initiate the conversation with slow, distinct pronunciation. Be aware that the acquirer's agent might not be comfortable with the issuer's primary language.
- Request clarification when uncertain of the communication.

To improve their call referral processes, issuers should monitor:

- The number of call referrals they generate in response to Authorization Request/0100 messages. Issuers should use call referrals only for high-risk situations because call referrals result in an expensive and time-consuming process, which can be detrimental to cardholder relationships.
- The rate of call referrals going to Stand-In processing. Issuers should ensure that they have sufficient call center staff and a stable telecommunications infrastructure to be able to support the number of call referrals they generate. Mastercard strongly urges issuers to register for GARS. Acquirer GARS calls will be routed to the Stand-In System for issuers not registered.
- The average duration of call referrals. Issuers should try to meet the goal of keeping call referrals to five minutes or less. Short call durations result in reduced transaction times, improve the call referral process for merchants and cardholders, and provide the best use of resources.

Issuers should establish Stand-In processing transaction limits that are specific to transactions approved through GARS call referrals. The Mastercard Stand-In processing facility ensures a timely authorization decision when the issuer is not available.

Mastercard suggests that GARS issuers establish two phone numbers for GARS call referral processing. Issuers can have all intracountry call referrals routed to one phone number and all intercountry call referrals routed to another phone number. Issuers can better anticipate potential language differences and offer enhanced services to cardholders traveling outside of their countries.

Charges to the issuer apply for issuing each call referral and for completed GARS calls initiated by the acquirer. Issuers also pay a noncompliance assessment for Stand-In processing if they fail to answer a GARS call within 30 seconds.

Methods Issuers Can Use to Improve GARS Performance

Issuers can use the following methods to improve GARS performance:

- Ensure that your phone system can generate true touch-tone signals. If you use an automated system such as a Voice Response Unit to answer incoming calls, be sure the system responds with a zero key followed by a pound key (0, #). This allows the acquirer's agent to hear the instruction of your automated system to expedite your call referral response.
- Ensure that your system is prepared to answer phone calls within 30 seconds. Calls not answered within these time frames will be routed to the Stand-In System.
- Determine whether to establish specific Stand-In transaction limits for GARS. Complete the *GARS Initiation and Change Form* (Form 334) to establish specific limits.
- Determine whether to establish one phone number for all incoming GARS calls or two phone numbers: one for GARS requests from acquirers located outside of the issuer country and one for domestic GARS requests. Indicate the phone numbers on the *GARS Initiation and Change Form* (Form 334).
- Review the information you provided to Stand-In processing either online or on the Stand-In Processing Worksheet. In particular, check the following:
  - Referral phone number provided. GARS uses this number to route calls to you.
  - Stand-In processing parameters

Submit any changes to your customer representative at least 15 days before using a new phone number or new parameters:

- Determine your ability to handle the volume of completed call referrals using GARS. Because GARS call referrals are fast and easy, there may be an increase in the ratio of calls completed to referrals issued. You may want to consider adjusting staffing and equipment levels to ensure higher control and risk reduction and avoid excessive Stand-In processing fees.
- Communicate to your employees the importance of answering GARS calls quickly to avoid additional Stand-In processing fees. Mastercard is available to assist you in your training efforts.

Monitoring Call Referral Activity

The minimum response and talk-time standards apply to all call referrals—domestic and international—whether processed through GARS or direct customer-to-customer communications.

Issuer and Acquirer Performance Reports

Issuers and acquirers can monitor call referrals completed through GARS using the following reports:

- Issuer Authorization Detail Report and Issuer Call Referral Detail Report—shows issuer charges for call referrals
- Acquirer Authorization Detail Report and Acquirer Call Referral Detail Report—shows acquirer reimbursement for completed call referrals
- Call Referral Summary Report—shows tiered pricing for excessive issuer call referral activity
- Guaranteed Issuer Availability Report

Samples of these reports showing charges or reimbursements associated with GARS appear in the *Mastercard Consolidated Billing System* manual.

Store and Forward Messages

Issuers also can monitor call referrals completed through GARS via store-and-forward (SAF) messages. Mastercard generates Authorization Advice/0120 messages for GARS transactions that Stand-In processes. Mastercard uses a promotion code of MCGARS to identify GARS Stand-In activity.

Requesting GARS or Changing GARS Parameters

To begin to use GARS or to change GARS parameters, complete the *GARS Initiation and Change Form* (Form 334).

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 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.

Incremental Preauthorization Transaction Processing

Issuers must manage the data in incremental preauthorization messages to release holds on cardholder accounts that can occur as a result of transactions.

The acquirer must use the Trace ID as a unique identifier from the original approved preauthorization in any incremental preauthorizations in connection with the same

transaction. The unique identifier, Trace ID, must also be included in the transaction clearing record.

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 DE 63 (Network Data) and DE 15 (Date, Settlement) information from the original Authorization 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 use the Trace ID to match the original and any approved incremental preauthorization to the transaction and release holds created by all authorizations properly related to the original preauthorization.

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 the same transaction on later dates. Incremental preauthorizations for an additional amount are 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 are used to extend only the chargeback protection period associated with the original preauthorization.

When the chargeback protection period of a preauthorization is extended as a result of an incremental preauthorization, it is extended for 30 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 that 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. If the issuer declines the chargeback extension request and the original extension subsequently expires, the acquirer must request a new authorization.

NOTE: Each approved preauthorization has an extended payment guarantee period of 30 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 days for Mastercard authorizations properly coded as preauthorizations and is seven days for all other Mastercard authorizations and for all Maestro and Cirrus authorizations and preauthorizations.

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. For the Europe region effective 5 November 2013 and for all other regions effective 21 April 2017, the payment guarantee period of the aggregate transaction is 30 days from the date of the last incremental preauthorization. Transactions that have incremental preauthorizations must originally be submitted as preauthorizations. Any transaction submitted as a final authorization or undefined 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 have incremental preauthorizations must originally be submitted as preauthorizations. Incremental preauthorizations must be coded as preauthorizations.

Typical Usage Scenario

The following table depicts the flow of a typical incremental preauthorization. The merchant successfully completes an original authorization for 100, followed by an incremental preauthorization of 50. This total amount is then processed as a first presentment.

Message Type	DE 61 (Point-of-Service), subfield 7 (POS Transaction Status)	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)[a]	4	MCC123ABC	1105	N/A	100
Incremental Preauthorization (0100/0110)[a]	4	MCC456ABC	1106	MCC123ABC1105	50
First Presentment (1240-200)		N/A	N/A	MCC123ABC1105	150

a	The Authorization Request/0100 message to issuer, the Authorization Response/0110 message to acquirer.

Incremental Preauthorization Reversals

Acquirers must ensure their merchants must send a full or partial reversal within 30 calendar days of the original preauthorization for Mastercard® or Debit Mastercard® transactions if the merchant will not submit all or part of a transaction for clearing.

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 below.

In the following scenario, the merchant successfully completes an original preauthorization for 100, followed by an incremental preauthorization of 50, but then wishes 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)[a]	MCC123ABC	1105	N/A	100	N/A
Incremental Preauthorization (0100/0110)[a]	MCC456ABC	1106	MCC123ABC1105	50	N/A
Reversal (0400/0410)[b]	MCC789ABC	1106	MCC123ABC1105	150	0

a	The Authorization Request/0100 message to issuer, the Authorization Response/0110 message to acquirer.
b	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.

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) (Clearing—DE 63, subfield 2)	DE 4 (Amount, Transaction)	DE 95 (Replacement Amount)
Original Preauthorization (0100/0110)[a]	MCC123ABC	1105	N/A	100	N/A
Incremental Preauthorization (0100/0110)[a]	MCC456ABC	1106	MCC123ABC1105	50	N/A
Reversal (0400/0410)[b]	MCC789ABC	1106	MCC123ABC1105	150	140
Clearing (1240-200)	N/A	N/A	MCC123ABC1105	140	N/A

a	The Authorization Request/0100 message to issuer, the Authorization Response/0110 message to acquirer.
b	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 (DE4) is recommended to contain 150, while the Replacement Amount (DE95) is recommended to contain 140.

Merchants 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.

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 nights lodging if they so choose. Any amount above that would be a violation of Mastercard rules and be at risk for a chargeback.

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 the same transaction on later dates. Incremental preauthorizations for an additional amount are 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 are used to extend only the chargeback protection period associated with the original preauthorization.

When the chargeback protection period of a preauthorization is extended as a result of an incremental preauthorization, it is extended for 30 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 life cycle expires before the transaction is finalized:

- Submit a new preauthorization within 30 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 days before).
- Use the Advance Resort Deposit process as described in section D.2 of 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 life cycle, an incremental preauthorization is recommended. As noted earlier in this document, the authorization life cycle is based on the date of the latest incremental preauthorization.

Extending Security Features

Mastercard® *Identity Check*™ 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.

Issuer Security Solutions

Mastercard offers best-in-class fraud management solutions to help issuers tackle fraud from every angle. These solutions were developed to control the cost of fraud, protect cardholders, and minimize potential damage to issuer reputations. Mastercard addresses multi-channel fraud by layering security strategies, policies, and technologies at each stage of the payment life cycle.

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 enables smarter decisioning, giving issuers a multi-dimensional authorization tool to assess both the risk and rewards of every transaction, so they can

enhance the consumer experience by approving more genuine transactions without increasing risk. Decision Intelligence evaluates information about consumers, merchants, and issuers during the shopping experience to help issuers decide whether a transaction makes sense and if it should be approved or declined for a particular consumer.

Mastercard will require all issuing and acquiring processors to code, support, and integrate into their systems the data elements, subelements, and values associated with Decision Intelligence. 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.

Benefits to Issuers

Decision Intelligence enriches and simplifies the decision management process with insights across multiple key dimensions that can help issuers deepen cardholder loyalty, gain incremental business and revenue, and reduce operational expenses.

Protect Cardholder Loyalty

- Deepen consumer relationships through a more consistent and satisfying shopping experience.
- Reduce cardholder inconvenience from erroneous declines.

Grow Business and Revenue

- Increase approvals of genuine online transactions without increasing risk exposure.
- Grow share-of-wallet by becoming the go-to payment choice for online shopping.

Reduce Operational Expenses

- Reduce false positive/erroneous declines of genuine transactions.
- Lessen revenue lost from fraud and chargebacks.
- Improve productivity and operational efficiency in fraud management.
- Decrease customer service costs due to more approved transactions.

Ease of Implementation

- Simplify decisions with a single transaction score on a risk–reward continuum.
- Integrate decision score easily into issuer's authorization decision processes and cardholder strategies.

- Lower time, effort and development costs by outsourcing advanced decisioning technologies through Mastercard's established, scalable platform.

How It Works

Decision Intelligence evaluates authorization and cardholder criteria, applying sophisticated modeling algorithms and enhanced data insights not typically available during authorization, into a single transaction decision score delivered to issuers in the real-time authorization message.

Additional data from Authorization IQ and Digital Transaction Insights, account data compromise events, and new variables focused issuer declines expands the focus of analysis from fraud detection to a more holistic view of the entire cardholder experience.

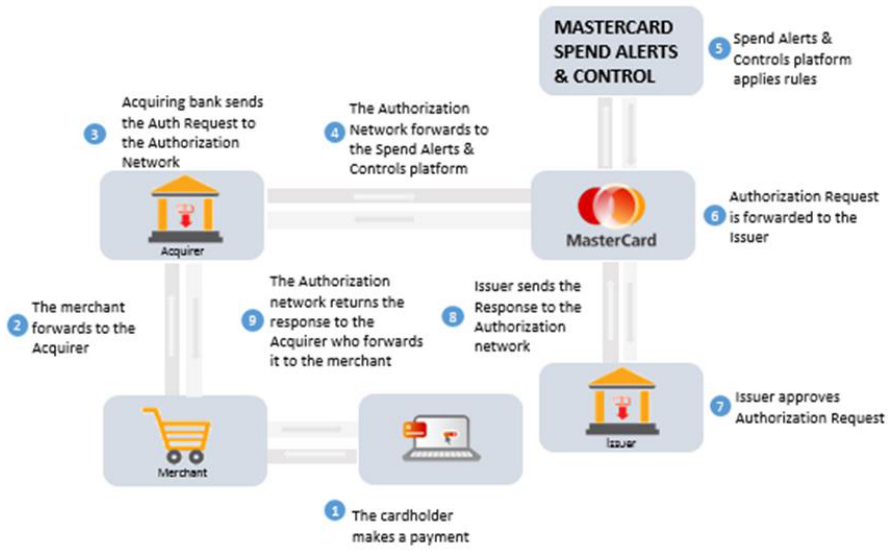
For each transaction, Decision Intelligence assesses:

Consumer transaction attributes based on consumer account and device information	Consumer transaction attributes assessment leverages the Mastercard Network to facilitate the globally interoperable exchange of information between merchants and issuers in digital, card-not-present (CNP) environments. It consolidates, normalizes, and assesses consumer account and device data provided by participating merchants, helping to inform issuers' real-time authorization decisions by giving them a level of assurance that the consumer's attributes they use to transact with the merchant are genuine.
Transaction security based on widespread fraud monitoring, fraud rules, transaction fraud models, and profiles	Fraud monitoring helps take action against and helps prevent further fraud from large-scale network-level fraud attacks on one or more payment channels (such as ATM and electronic commerce [e-commerce]) due to unforeseen circumstances such as a system breach. Security rule management enables issuers to establish and implement precise business rules using data elements within the authorization message as well as Mastercard-defined variables to score the security of their cardholder's transactions and dynamically perform actions appropriate for the individual's cardholder's segment and transaction attributes. Security scoring uses finely tuned decisioning models to generate a predictive security score in real-time.

Cardholder segmentation based on insights into account spending that help define the value and engagement of the cardholder with their issuer	Cardholder segmentation assessment leverages enhanced analytics to properly identify and understand activity of high-spending cardholders at a transactional level in real-time during authorization.

This produces a single transaction decision score delivered to issuers in the real-time authorization message. The decision score shows the transaction on a risk–reward continuum (with a value from 0 to 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 and cardholder strategies.

Transaction Flow



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 about data requirements, refer to the *Customer Interface Specification* manual.

Decision Intelligence—Authorization IQ Feature

In an overall effort to reduce and prevent fraud, Mastercard provides Authorization IQ, an actively managed segmentation feature of the Decision Intelligence service that can help

issuers increase approvals and ensure a more satisfying consumer experience without incurring greater risk.

Authorization IQ gives issuers targeted, real-time segmentation insights to help them identify best-spending or most frequent-spending cardholders who show the greatest revenue opportunity at the time of card usage. The service adds a critical dimension to decision management strategies—supplementing and expanding fraud detection—by providing tangible data points to enable data-driven authorization strategies.

Mastercard will require all issuing and acquiring processors to code, support, and integrate into their systems the data elements, subelements, and values associated with Authorization IQ. 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.

About Authorization IQ

Authorization IQ is an actively managed, network-based, segmentation feature of the Decision Intelligence service that provides issuers with real-time data insights that complement their segmentation solutions and drive their authorization strategies.

Authorization IQ allows issuers targeted, real-time segmentation insights to help them identify best-spending or most frequent-spending cardholders who show the greatest revenue opportunity at the time of card usage. The service adds a critical dimension to decision management strategies, supplementing and expanding fraud detection, by providing, tangible data points to enable data-driven authorization strategies.

In addition to assessing authorization decisions based on the risk profile of how the cardholder originated the transactions, such as magstripe, EMV2, or, tokenization), Mastercard Authorization IQ provides a complementary set of data points that help bring focus to the importance of the individual cardholder at the time of the transaction.

Benefits

Mastercard designed this feature to help participating issuers drive:

- Higher approval rates without increasing risk by providing card and transaction level insights
- Higher revenue via increased approval rates

- Greater visibility into more profitable and sensitive transactions, such as cross-border or frequent travelers
- Reduced operational and customer service costs due to lower decline volume

How It Works

The Authorization IQ feature of the Decision Intelligence service leverages a rolling 12 months of account spend to provide issuers with real-time actionable intelligence relevant to that specific account and transaction. The insights are designed to help issuers target authorization strategies via analysis across three key dimensions.

Overall Account Spending Insights

With a large percentage of spend typically concentrated across a small number of cards, pinpointing cardholders with the greatest opportunity is critical to drive meaningful results. This dimension looks at 12 months of cleared, non-fraudulent spend, treating current spend as more relevant (for example, USD 1,000 spent this week is more relevant than USD 1,000 spent four weeks ago). The transaction spend is ranked by country/product such as U.S. region/debit or U.S. region/credit) to determine spend ranking across one of the following categories:

- High (Top 10 percent)
- Med-1 (Top 30 percent)
- Med-2 (Top 50 percent)
- Med-3 (Top 75 percent)
- Low
- New (Card activity on the network less than 60 days old)

For example, high spenders are the top 10 percent of accounts for the country, not just within the issuer, and provide an opportunity to identify the best of the best spenders in the market. These cardholders are highly coveted and quickly reach for another card if declined at the point of sale.

Channel Spending Insights

Frequency of behavior is a key component to the overall cardholder experience. This dimension looks at 12 months of cleared, non-fraudulent spend across designed channels including card-present/card-not-present (CNP) and domestic/cross-border combinations. The transaction spend is ranked by activity across the issuer portfolio into one of the following categories:

- High (Top 10 percent)
- Med-1 (Top 30 percent)
- Med-2 (Top 50 percent)
- Med-3 (Top 75 percent)
- Low
- New (Card activity on the network less than 60 days old)
- None (No network activity in the last 12 months)
- Dormant (Previously active card with no network activity in the last 120 days)

Transactions are qualified into specific segments. Refer to the Segment Definitions table in the *Customer Interface Specification* manual. Each segment is assigned to a specific qualifying channel.

Account Transactional Insights

Frequency of behavior is a key component to the overall cardholder experience. This dimension looks at 12 months of cleared, non-fraudulent spend across a number of predefined segments (such as retail, travel, and gaming). Transaction spend is ranked against the qualifying segment for the issuer portfolio into one of the following categories:

- High (Top 10 percent)
- Med-1 (Top 30 percent)
- Med-2 (Top 50 percent)
- Med-3 (Top 75 percent)
- Low
- New (Card activity on the network less than 60 days old)
- None (No network activity in the last 12 months)
- Dormant (Previously active card with no network activity in the last 120 days)

Transactions are qualified into specific segments. Refer to the Segment Definitions table in the *Customer Interface Specification* manual.

Service Deliverables

The Authorization IQ feature of the Decision Intelligence service provides two key deliverables for issuers:

- Real-time data enrichment of authorization messages enabled by the dimension analysis:

  The outcome from the dimension analysis is placed into the authorization messages for all enrolled bank identification number (BIN) ranges.
- An issuer opportunity matrix dashboard that provides a way to visualize and better assess the service impact in conjunction with, and outside of, any ongoing authorization strategy changes.

  The dashboard is made available to all service customers upon enrollment and provides specific portfolio assessment by card product group and segmentation categories. Use of the dashboard is not dependent on the completion of any authorization coding changes.

Fees

Refer to the *Mastercard Consolidated Billing System* manual for fees and billing information.

Message Specification Requirements

The following are detailed message specifications for issuers that want to participate in the Authorization IQ feature of the Decision Intelligence service.

Fields

Issuers should refer to the *Customer Interface Specification* or *Single Message System Specifications* manuals for detailed field information.

NOTE: Testing for support of these fields is required.

Issuers participating in the Authorization IQ feature of the Decision Intelligence service must support the following fields:

- On-behalf Service (OBS)—DE 48 (Additional Data—Private Use), Subelement 71 (On-behalf Services):
  - Subfield 1 (On-behalf [OB] Service) with a value of 18 (Fraud Scoring Service)
  - Subfield 2 (On-behalf [OB] Result 1) with a value of C (Expert Monitoring Fraud Scoring Service was performed successfully)
- Fraud Scoring Data—DE 48, Subelement 75 (Fraud Scoring Data):
  - Subfield 1 (Fraud Score)
  - Subfield 2 (Score Reason Code)
  - Subfield 3 (Rules Score)
  - Subfield 4 (Rules Reason Code 1)
  - Subfield 5 (Rules Reason Code 2)
- Security Services—DE 48, 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 Authorization IQ should contact their Mastercard Account Representative.

For More Information

For details about data requirements, including Service Data Content and Segment Definitions, refer to the *Customer Interface Specification* manual.

Decision Intelligence—Digital Transaction Insights Feature

Through the Decision Intelligence service, Mastercard provides Digital Transaction Insights, an information exchange framework that enables merchants to share electronic commerce (e-commerce) data with issuers in card-not-present (CNP) environments.

The Digital Transaction Insights feature of the Decision Intelligence service facilitates the exchange and normalization of consumer account and device data provided by participating merchants to help give issuers a level of assurance that consumers are transacting using attributes that are typically associated with them.

About Digital Transaction Insights

With the growth of e-commerce has come an increase in digital fraud. Although ways have been developed to combat this fraud, false-positive declines are detrimental and costly.

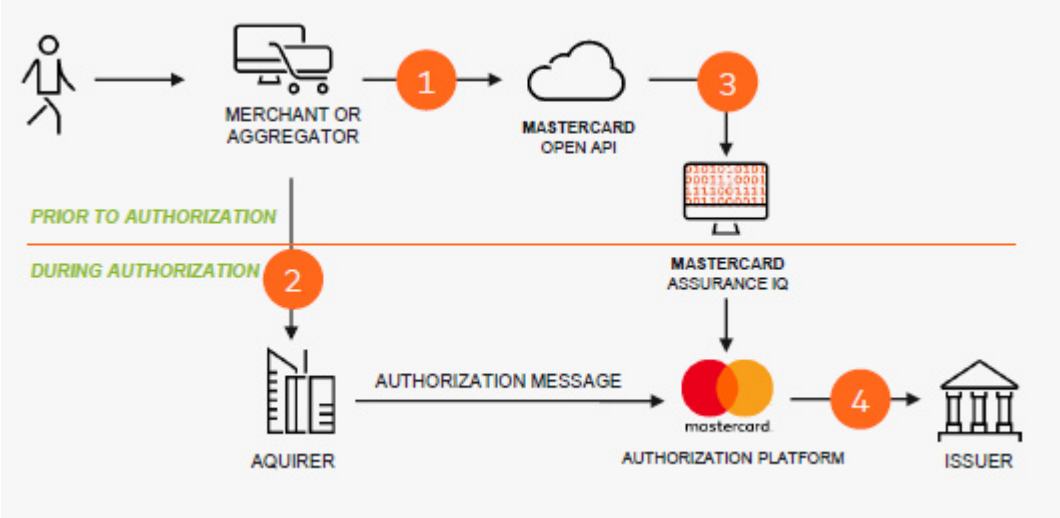
Consumers who experience a declined card can abandon or reduce their spending on the card or even consider changing cards or banks.

The Digital Transaction Insights feature of the Decision Intelligence service helps to close the information gap, enabling e-commerce merchants to share CNP transaction data with issuers that was not previously available to them. Digital Transaction Insights facilitates the exchange and normalization of consumer account and device data provided by participating merchants to help give issuers a level of assurance that consumers are transacting using attributes that are typically associated with them.

Digital Transaction Insights supports all Mastercard brands (Mastercard®, Maestro®, and Cirrus®), segments (consumer, commercial), and products (credit, debit, prepaid). While the service is available for single and dual message transactions, it is only applicable to CNP transactions.

How it Works

The Digital Transaction Insights feature of the Decision Intelligence service leverages the Mastercard Network to facilitate the globally interoperable exchange of information between merchants and issuers in digital environments. It assesses consumer account and device data provided by participating merchants, helping to inform issuers' real-time authorization decisions by giving them a level of assurance that the consumer's attributes used to transact with the merchant are genuine.



Digital Transaction Insights follows these general processing steps:

1. Prior to authorization, participating e-commerce merchants use the Mastercard Application Program Interface (API) to pass hashed consumer account and device information captured at the point-of-interaction (POI) to Mastercard. The type of data merchants might provide to Mastercard includes:
   - Account information (such as billing and shipping addresses)

- Device information
- A non-hashed merchant-determined assurance level assessment via the API

Merchants can participate in the Digital Transaction Insights feature of the Decision Intelligence service by sending one of the following three types of requests to Mastercard via the API:

a. Scoring Request
b. Notification Request
c. SendConfidence Request

2. Merchant submits the authorization request to the acquirer.
3. Digital Transaction Insights consolidates, normalizes, and assesses the merchants' hashed data to provide an assurance level to issuers.
4. Issuers receive a risk-level assessment and two reason codes that describe the assessment in the real-time authorization message:

a. Risk Level—provides a risk-based authentication assessment.
b. Reason Code 1—supports the Mastercard-determined risk-level assessment.
c. Reason Code 2—supports the merchant-determined transaction assessment.
d. The following applies to both reason codes:

- A—Normal Activity for Account Relationship; Known Device/Account Relationship
- B—Established Account Relationship
- C—Strong Authentication History; Established Account Relationship
- D—Valid Device/PAN Pairing; Established Account Relationship
- E—Risk Event—Suspicious Account Activity
- F—Risk Event—Unknown Device/Account Relationship
- G—Risk Event—Device or Profile Information associated with fraud event
- H—Risk Event—Recent change to Device or Profile Information
- I—Risk Event—Recent High Risk Change to Device or Profile Information
- J—Risk Event—PAN associated with fraud event
- K–Y—Reserved for future use
- Z—New Account or Insufficient Data

Benefits to Issuers and Merchants

The power of the Digital Transaction Insights feature of the Decision Intelligence service is in the network effect, which symbiotically benefits both issuers and merchants.

Digital Transaction Insights helps issuers:

- Improve revenues by increasing approvals and reducing false declines of genuine e-commerce transactions without increasing their risk exposure.
- Deepen and retain valued consumer relationships with a more consistent, satisfying experience across shopping choices.
- Reduce financial losses and associated costs from fraud and chargebacks.
- Decrease customer service costs due to more approved transactions.

- Lower operational costs in capital, information technology (IT) development, and customer service by outsourcing a trusted data exchange framework through the Mastercard-established, globally interoperable, scalable platform.

Using Digital Transaction Insights, merchants can:

- Lower decline rates to help preserve revenue and relationships with their valued customers.
- Obtain greater influence over the consumer experience and transaction decisioning by providing better real-time insights beyond what issuers have today.
- Reduce decisioning latency by leveraging a real-time assurance level of consumer attributes that influences issuer transaction decisions at the most critical time during authorization.
- Increase savings and efficiency in managing the consumer experience by leveraging an assurance level of consumer attributes to avoid full consumer verification of every transaction.

Fees

At this time, there are no fees required for issuers or merchants to participate in the Digital Transaction Insights feature of the Decision Intelligence service; however, for an issuer to participate in Digital Transaction Insights, the BIN must be enrolled in one Category 1 fraud service including Safety Net, Prepaid Monitoring, Fraud Rule Manager, Expert Monitoring, and/or Network Defense to be eligible to participate in Digital Transaction Insights. Issuers that use a Category 1 Security Service are not charged an additional fee for Digital Transaction Insights.

Message Specification Requirements

Mastercard requires all acquiring and issuing processors to code for, support, and integrate into their systems the data elements, subelements, and values associated with Address Verification Service (AVS).

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

For additional information about this requirement, refer to the Global Safety and Security Standards Roadmap.

NOTE: Mastercard does not require acquirers or issuers to enroll in these optional products and services, unless Participation Requirements state otherwise. Acquirers and issuers 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.

To Participate

Issuers interested in participating in the Digital Transaction Insights feature of the Decision Intelligence service 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.

Participating merchants must also complete a Service Agreement indicating their agreement to provide CNP data to Mastercard.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

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 provides two scoring solutions: 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.

Fraud Rule Manager

As an integral part of a rules-based authorization strategy, Fraud Rule Manager enables issuers to automate precise, highly variable fraud decisions during authorization in order to quickly and easily respond to evolving fraud trends.

Mastercard will require all issuing and acquiring processors to code, support, and integrate into their systems the data elements, subelements, and values associated with Fraud Rule Manager. 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.

Fraud Rule Manager 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.

Fraud Rule Manager provides the flexibility issuers need to identify the precise actions that address ever-changing fraud trends. Issuers can establish business rules using:

- More than 70 authorization fields which provide billions of rule decision combinations.
- Mastercard-derived data which enables rule development using Business Rule Velocity, ADC Events, Expert Monitoring, IQ Series, Decision Intelligence, and more.
- Custom-defined rule reason codes which notify you when fraud is detected and/or when to perform appropriate actions based on your specifications.
- Custom-defined velocity parameters which evaluate prior authorizations occurring over a specific time period before interpreting the current authorization.
- Custom-defined lists which simplify management of large and/or highly variable data values without affecting rules.

Fraud Rule Manager delivers the agility that issuers need to quickly manage rules in response to the dynamics of fraud. Issuers can use business rules using:

- Globally hosted service, which enables issuers to stay focused on their fraud strategy without the distraction of operational, IT, resource, and training concerns.
- Real-time fraud prevention using rules during authorization to enable immediate action against suspect transactions.
- Standalone fraud detection or seamless integration with other Mastercard management data such as Expert Monitoring, IQ Series, and more.
- Self-service utilities, which provide issuers with flexibility to manage and view rules and resulting actions how and hwn they want.
- On-demand deployment times available, which places issuers in control of when business rules are in active production.
- Experienced rule experts that can help oversee the implementation and deployment of issuer fraud rules.

Benefits

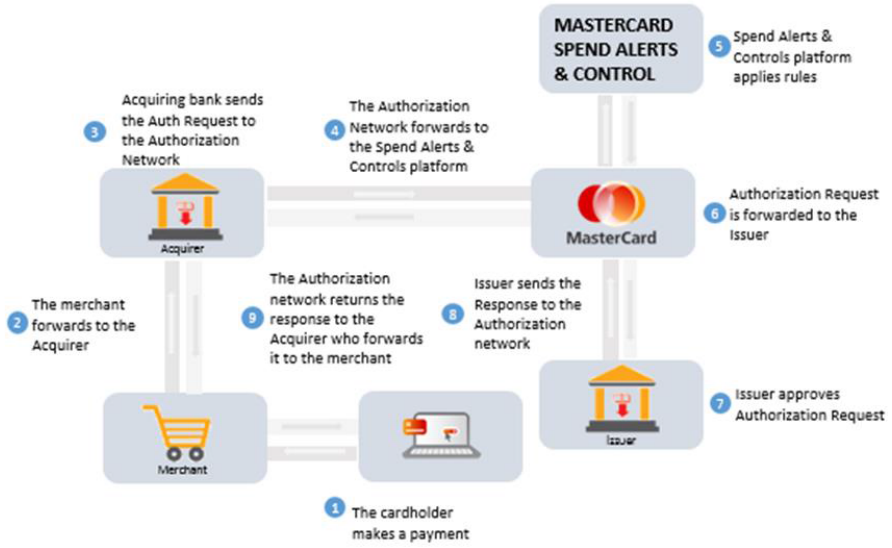
When targeting known fraud scenarios specific to their business, issuers need to pinpoint fraud using precise business rules that enable them to quickly and flexibly tailor their fraud decisions. Fraud Rule Manager simplifies and streamlines rules management, helping issuers to improve their agility in response to fraud trends.

- Decrease implementation cycle time to market from days/weeks to hours by minimizing time spent on IT development, operational, resource, and training concerns.
- Enable fraud analysts to quickly perform their fraud strategy by tuning fraud scores and reason codes to specific fraud patterns for issuer portfolios.
- Reduce their investment in fraud detection.
- Increase cost certainty by shifting to a more predictable operational cost structure for business rules management.
- Minimize costs and resources required for IT development, operations and expansion of their fraud detection capabilities.
- Enhance their quality in fraud detection.
- Enable fraud analysts to manage rules in a few simple steps to reduce the chance for human error.
- Validate business rules by enabling fraud analysts to test the effect of rules prior to implementation.
- Boost the effectiveness of fraud detection models by tailoring fraud scores to their unique business needs.

How It Works

Issuers may establish fraud rules via the Rules Management Utility in the Fraud Center of Mastercard Connect for simple rules management or consult with Mastercard experts for more complex rules. Mastercard may take up to 5 days to process and implement rule requests.

Fraud Rule Manager evaluates all transactions in real time and delivers fraud rules output and/or incorporate derived data (such as the Expert Monitoring fraud score) in the authorization message or the Case Management utility in the Fraud Center or both.



1. The Authorization Request message is received by the Authorization Platform for transaction processing.
2. The Authorization Request message is routed to Fraud Rule Manager.
3. Fraud Rule Manager identifies details associated with the authorization message. Fraud Rule Manager will evaluate the authorization against the issuer's rules, assign a score and reason code, and return the results to the issuer either in the authorization message or to the Case Management utility tool for further review.
4. Issuers that are unable to receive fraud rules output and/or additional derived data into the real-time authorization message may use a turnkey configuration option available via Case Management. This utility notifies issuers of fraud, enabling them to view alerts of approved or declined transactions and track any subsequent investigation. Case Management retains fraud events and transactions for up to 90 days once they are closed.

NOTE: In addition to Case Management, List Management, Transaction Views, and Rules Management, self-service utilities available at no charge to assist participating issuers in managing fraud-related information. Customers can request access to these utilities available on the Fraud Center through Mastercard Connect.

To Participate

Issuers that want to participate in these services must complete a contract and registration form. Issuers interested in registering for these services should contact their Mastercard representative or the Mastercard Risk Solutions Team at risksolutions@Mastercard.com.

For More Information

For additional detail on data values used in the authorization service, refer to the *Customer Interface Specification* manual.

Issuer Security Solutions Product Specifications and Data Usage

Mastercard uses the following values in DE 48 (Additional Data—Private Use), subelement 56 (Security Services Additional Data for Issuers), subelement 71 (On-behalf Services), and subelement 75 (Fraud Scoring Data) of Authorization Request/0100 and Authorization Advice/0120—System-generated messages to support fraud scoring service transactions.

Authorization Processing

The Authorization Platform inserts subelement 75 when Expert Monitoring for Issuers is performed or when both Expert Monitoring for Issuers and Fraud Rule Manager services are performed on the transaction. When a rule adjusted score is provided in subfield 3, at least one or more rule reason code values will be provided in subfields 4–5. However, rule reason code values may be provided in subfields 4 or 5 with or without a rule adjusted score in subfield 3.

- Subelement 56 (Security Services Additional Data for Issuers):
  - Subfield 1 (Security Services Indicator)
  - Subfield 2 (Security Services Data)
- Subelement 71 (On-behalf Services):
  - Subfield 1 (On-behalf [OB] Service), value 18 (Fraud Scoring Service)
  - Subfield 2 (On-behalf [OB] Result 1), value C (Successful) and U (Unable)

  Subelement 75 will not be populated when U (Unable) is the result.
- Subelement 75 (Fraud Scoring Data):
  - Subfield 1 (Fraud Score)
  - Subfield 2 (Score Reason Code)
  - Subfield 3 (Rules Adjusted Score)
  - Subfield 4 (Rules Reason Code 1)
  - Subfield 5 (Rules Reason Code 2)

For More Information

For more information about these services, refer to the *Customer Interface Specification* manual.

M/Chip Processing Services

Mastercard provides M/Chip processing services to help issuers that want to migrate to Mastercard M/Chip technology without having to make an initial investment to completely upgrade their host systems for M/Chip processing.

The M/Chip processing services support issuers using M/Chip technology by performing all or part of the M/Chip-related authorization processing on behalf of the issuer for a designated account range.

The M/Chip processing services are available to all brands—Mastercard, Maestro, Cirrus, and Debit Mastercard. There are three M/Chip processing services:

- Chip to Magnetic Stripe Conversion
- M/Chip Cryptogram Pre-validation
- M/Chip Cryptogram Validation in Stand-In Processing

NOTE: All issuers globally that participate in Stand-In processing must have M/Chip Cryptogram Validation in Stand-In Processing performed during Stand-In processing.

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 an issuer is not able to respond to an authorization request.

In addition to these three services, issuers can combine the M/Chip Cryptogram Pre-validation Service and the Chip to Magnetic Stripe Conversion Service (referred to as the Combined Service Option).

Issuers that participate in the M/Chip Cryptogram Pre-validation service, the M/Chip Cryptogram Validation in Stand-In Processing service, or the Combined Service Option may optionally support *M/Chip Advance*.

For more detailed information about these M/Chip processing services, including information about the Chip Processing Services Member Requirements and Parameters Form, refer to the *M/Chip Processing Services—Service Description* guide. For supporting data requirements, refer to the *Customer Interface Specification* manual.

Chip to Magnetic Stripe Conversion

Mastercard provides Chip to Magnetic Stripe Conversion to issuers by performing all or part of the M/Chip-related authorization processing on behalf of the issuer for a designated account range.

Mastercard removes designated M/Chip-related data elements and alters others before forwarding the transaction to the issuer. Mastercard notifies the issuer that the transaction was an M/Chip transaction and that Mastercard altered the transaction information before sending it to the issuer.

When the Chip to Magnetic Stripe Conversion service processing is performed on a transaction, the original method used to enter the primary account number (PAN) in the Authorization Platform is indicated in DE 48 (Additional Data—Private Use), subelement 71 (On-behalf [OB] Services), subfield 2 (On-behalf Result 1) before sending Authorization Request/0100, Authorization Advice/0120, and Reversal Request/0400 messages to the issuer for processing.

The source of the track data provided is from Track 2 Equivalent Data (tag 57). Issuers should be aware that the CVC value contained therein is the Chip CVC and not CVC 1; therefore, will impact any CVC validation that an issuer performs.

Providing this information allows the issuer to make the authorization decision based on information remaining in the authorization request, without having to reject the transaction because it does not currently process M/Chip transactions. For issuers that participate in the

Chip to Magnetic Stripe Conversion service and do not want to receive the service results, refer to U.S. Chip-Enabled Travel Card Program.

The Chip to Magnetic Stripe Conversion service is optional.

NOTE: The Global Clearing Management System (GCMS) also offers the Chip to Magnetic Stripe Conversion service. For information about this optional service, issuers should reference the *GCMS Reference Manual*.

Chip CVC to CVC 1 Conversion Service

The Chip CVC to CVC 1 Conversion service offers issuers the option of having Mastercard pre-validate the Chip CVC value and, when valid, replace it with the appropriate CVC 1 value before delivering the authorization request message to the issuer during normal authorization processing.

Pre-validation is performed to ensure that a CVC 1 value is generated only for transactions containing a valid Chip CVC. The Chip CVC to CVC 1 conversion service validates the Chip CVC value and, if valid, replaces it with the appropriate CVC 1 value before delivering the authorization request message to the issuer during normal authorization processing.

The Chip CVC to CVC 1 Conversion service is optional.

Service Options

Two service options are available to issuers:

- Single key and decision matrix for both CVC 1 and Chip CVC
- Different keys and decision matrices for CVC 1 versus Chip CVC

The service first attempts to validate the Chip CVC value using issuer-provided keys (validation is performed to help ensure that only transactions containing a valid Chip CVC are serviced). If the validation is successful, the service uses issuer-provided keys to calculate the CVC 1 value and replace the Chip CVC with the CVC 1 value.

Regardless of the Chip CVC validation result (successful or unsuccessful), the service always attempts to send the authorization request message to the issuer for an authorization decision (if the issuer is unavailable and Stand-In processing is enabled for the account range, the Stand-In System will make the authorization decision). The service does not offer an option to decline on behalf of the issuer.

The service supports issuers with authorization host systems that do not support Chip CVC validation. Issuers may choose to use the service as part of their magnetic-stripe to chip technology migration path, or as a component of their long-term chip issuance strategy.

The service, in conjunction with the other Mastercard Chip on-behalf services, assists issuers in minimizing or eliminating host system impact from a migration to chip technology.

NOTE: Issuers that use the service must ensure CVC 1 and Chip CVC are located in the same positions of the Track 2 data, in the physical magnetic stripe Track 2 and in the Track 2 equivalent data encoded in the chip.

Validation of Chip CVC Using Issuer-Provided Keys

Before generating CVC 1, the service will first attempt to validate the Chip CVC using issuer-provided keys.

WHEN...	THEN...
Validation is successful	The service will generate CVC 1, which will replace the Chip CVC in the Track 1 DE 45 or Track 2 DE 35 data as applicable.
Validation is unsuccessful	The service will not generate CVC 1, and the Chip CVC will remain in the Track 1 DE 45 or Track 2 DE 35 data as applicable. Mastercard recommends that issuers include DE 48, subelement 87 (CVC Result) value "Y" (Invalid CVC 1) in the authorization response message whenever CVC 1 is determined to be invalid.

The appropriate On-behalf service IDs and service result code will be added to the message in DE 48, subelement 71.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

U.S. Chip-Enabled Travel Card Program

The U.S. Chip-Enabled Travel Card program leverages the functionality of the Chip to Magnetic Stripe Conversion service, and allows issuers that participate in the Chip to Magnetic Stripe Conversion service the option not to receive notification that the conversion has taken place (service results) in authorization and financial request messages.

Benefits

The U.S. Chip-Enabled Travel Card program benefits include the following:

- Creates new revenue streams and greater operational efficiency
- Provides the opportunity to capture more payments in new markets, displacing many cash purchases made around the world
- Promotes the globalization of EMV chip technology

How It Works

Issuers have the option not to receive notification that the Chip to Magnetic Stripe Conversion has taken place, removing the impact to their authorization and clearing systems when implementing chip. Existing functionality of the Chip to Magnetic Stripe Conversion service, as

well as the Combined Service Option (Chip to Magnetic Stripe Conversion and M/Chip Cryptogram Pre-validation services) are not affected. Service results are retained by Mastercard for billing and reporting purposes.

Transactions are tracked at the account range. The source of the track data provided is from Track 2 Equivalent Data (tag 57). Issuers should be aware that the CVC value contained therein is the Chip CVC and not CVC 1; therefore, it will impact any CVC validation that an issuer performs.

For a chip transaction received for an account within the account range, the chip transaction is converted to the magnetic stripe equivalent. Although participation is set at the account range, instead of at the specific account, other accounts that the issuer does not want to participate will not be chip enabled.

Chip-enabled U.S. travel cards include a hybrid chip and magnetic stripe card with signature, as the card verification method and online PIN capabilities. Chip-enabled U.S. Travel cards allow chip acceptance and continue to function similar to existing issuer magnetic stripe cards.

Authorization Processing

The following information describes the Authorization Platform of U.S. chip-enabled travel cards transaction processing.

WHEN...	THEN the Authorization Platform...
The Chip to Magnetic Stripe Conversion Service is requested for a transaction	Verifies whether the issuer wants to receive Chip to Magnetic Stripe Conversion Service results in Authorization Request/0100, Authorization Advice/0120, and Reversal Request/0400 messages for an account range that is eligible to participate in the service.
The issuer for the account range does not want to receive the Chip to Magnetic Stripe Conversion Service results in the Authorization Request/0100 message	Removes the Chip to Magnetic Stripe Conversion Service results contained in DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services [OBS]), subfield 1 (On-behalf [OB] Service) and subfield 2 (On-behalf Result 1) from the Authorization Request/0100, Authorization Advice/0120, or Reversal Request/0400 message. The Chip to Magnetic Stripe Conversion service removes chip-related data in DE 55 (Integrated Circuit Card [ICC] System-Related Data) and DE 23 (Card Sequence Number) if present when DE 14 (Date Expiration) is greater than or equal to the floor expiration date.

WHEN...	THEN the Authorization Platform...
The issuer for the account range wants to receive the Chip to Magnetic Stripe Conversion Service results in the Authorization Request/0100 message	Follows business-as-usual processing by providing the Chip to Magnetic Stripe Conversion Service results in the Authorization Request/0100, Authorization Advice/0120, or Reversal Request/0400 message.

To Participate

Issuers that want to participate in the U.S. chip-enabled travel card program must register for the Chip to Magnetic Stripe Conversion Service. In addition, issuers must contact their regional Mastercard representative to request this service and identify the account range for which the Chip to Magnetic Stripe Conversion service will support.

M/Chip Cryptogram Pre-validation Service

The M/Chip Cryptogram Pre-validation service is for issuers that use the M/Chip Select 2.0, M/Chip Lite 2.1, M/Chip 4.0 (Mastercard, EMV CSK, and EMV2000 session key derivation methods), *M/Chip™ Advance*, and EMV CCD-compliant chip cards.

This service:

- Validates the Authorization Request Cryptogram (ARQC) and Transaction Certificate Cryptogram (TC), and generates the Authorization Response Cryptogram (ARPC) on behalf of an issuer.
- Validates critical chip information included in the Card Verification Results (CVR) and Terminal Verification Results (TVR).

After performing this service, Mastercard notifies issuers of the results of the cryptogram validation. Issuers may use these results in the authorization approval process.

For more information about using the M/Chip Cryptogram Pre-validation service, refer to the *Customer Interface Specification* manual.

The M/Chip Cryptogram Pre-validation service is mandatory.

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.

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

M/Chip Cryptogram Validation in Stand-In Processing is available for issuers that use the M/Chip Select 2.0, M/Chip Lite 2.1, and M/Chip 4.0 (Mastercard, EMV CSK, and EMV2000 session key derivation methods), *M/Chip Advance*, and EMV CCD-compliant chip cards.

NOTE: All issuers globally that participate in Stand-In processing must have M/Chip Cryptogram Validation in Stand-In Processing performed during Stand-In processing.

This service authorizes M/Chip transactions within Stand-In processing when an issuer host is not available. When Stand-In processing authorizes M/Chip transactions, Mastercard validates the ARQC, TC, and critical (CVR and TVR) chip information, processes the authorization request based on the issuer's Stand-In parameters, and generates the ARPC.

M/Chip Cryptogram Validation in Stand-In Processing is mandatory for all chip card issuers.

Issuers should consider participating in PIN Validation services for successful Stand-In processing of chip transactions with online PIN.

M/Chip Advance

Mastercard® *M/Chip*™ *Advance* is a dual interface chip card specification for credit, debit, prepaid, and Mastercard® contactless programs.

M/Chip Advance:

- Integrates contactless products—Fully integrates contact and contactless cards and simplifies the adoption and implementation of contactless products.
- Provides enhanced on-card risk management—Increases the volume of approved transactions with more informed card risk management decision making.
- Supports new third-party transit, loyalty, voucher programs, and ticketing (for example, music concerts, cinema, theatre, or sports events)—Provides the functionality to extend card payment services into new markets.

- Provides enhanced payment features. M/Chip 2 and M/Chip 4 have a single set of counters to manage the risk of all offline transactions. This means that the risk management functionality of the application is not able to differentiate between CVM and no-CVM transactions or contact and contactless transactions.
- Provides backwards compatibility with existing M/Chip platforms—Facilitates the migration from M/Chip 2 and M/Chip 4 to *M/Chip Advance*.

The *M/Chip Advance* card application specification is available to card developers under a specific Mastercard development agreement.

With *M/Chip Advance*, DE 55 (Integrated Circuit Card [ICC] System-Related Data), subelement 9F10 (Issuer Application Data [IAD]) contains expanded counters. These expanded counters are used in the ARQC when the value of the right-most bit of the CVN is 1. The IAD can be configured to include accumulators, counters, or both, in plain text or encrypted. The value of an accumulator or counter included in the IAD may be either its absolute value (for example, Accumulator Amount or Counter Number) or the value of their balance. If so, the IAD is extended with one or two, 8 byte fields.

M/Chip issuers may optionally choose to support *M/Chip Advance* but are not required to migrate to *M/Chip Advance* specifications to continue using these services.

Issuers that participate in the M/Chip Cryptogram Pre-validation service, the M/Chip Cryptogram Validation in Stand-In Processing service, or the Combined Service Option may optionally support *M/Chip Advance*.

Maestro Preauthorized Transaction Processing

Maestro preauthorized transaction processing is explained here.

NOTE: Applies only to the Europe region.

The Authorization Platform allows Europe region acquirers to request preauthorization on transactions for which the final transaction amount is not yet determined. For automated fuel dispenser (AFD) transactions, once the issuer approves the preauthorization request and after the transaction completes at the point-of-interaction and the final amount is determined, the acquirer sends an authorization advice message to the issuer. For card-not-present (CNP) and post-authorized aggregated Maestro contactless transit transactions, if the final amount is not equal to the preauthorized amount, a partial reversal is required and clearing must be submitted for the new amount identified in the partial reversal.

The Clearing message must contain the final amount, which is equal to the amount contained the authorization advice message or in the new amount of a partial reversal message.

Preauthorization on Maestro transactions is permitted only at unattended point-of-sale (POS) terminals at petrol stations (MCC 5542, Fuel Dispenser, Automated). Preauthorization on Maestro transactions is also permitted for CNP transactions and for post-authorized aggregated Maestro transactions. Preauthorizations must not be used in any other acceptance environment.

Acquirers must ensure that an authorization request for an amount greater than zero is properly identified as a preauthorization when a CNP transaction might not be completed for reasons other than technical failure or lack of full issuer approval. For example, the transaction might not be completed when the cardholder will be offered the choice at a later time to complete the transaction with another payment means, or when the goods ordered by the cardholder might be later found to be out of stock. The risk of technical failures such as telecommunications failure or POI terminal failure should not be taken into account to determine if an authorization must be coded as a preauthorization.

For a CNP transaction, the transaction amount must equal the preauthorized amount. Preauthorizations for an estimated amount are only permitted for unattended petrol terminal (MCC 5542) transactions.

How It Works

Maestro preauthorized transaction processing works as follows:

- The acquirer submits an Authorization Request/0100 (preauthorization format) message containing the maximum amount determined by the acquirer or the merchant where DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains value 4 (Preauthorized request). Each approved preauthorization has a payment guarantee period of seven calendar days from the authorization approval date.
- The issuer generates an Authorization Request Response/0110 message for the full amount of the preauthorization or for a lesser amount, as determined by the issuer, if the merchant's terminal supports partial approval. The transaction is guaranteed up to the amount authorized by the issuer.
- The acquirer must send Authorization Advice/0120—Acquirer-generated messages containing DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code), value 191 (Acquirer Processing System [APS] Completed Authorization Transaction) at the completion of Maestro CAT Level 1 petrol transactions.
- The issuer acknowledges the transaction using an Authorization Advice Response/0130 message.
- The acquirer must send Reversal Request/0400 messages containing DE 4 (Amount, Transaction) from the Authorization Request/0100 message or DE 4 from the Authorization Request Response/0110 message if a partial approval response and DE 95 (Replacement Amounts) that contains the actual amount subfield necessary to perform a partial reversal if the final amount is less than the preauthorized amount for card-not-present (CNP) and post-authorized aggregated Maestro contactless transit transactions.
- If any transaction is terminated after the preauthorization, the acquirer must send the issuer a Reversal Request/0400 message containing DE 4 (Amount, Transaction) from the Authorization Request/0100 message or DE 4 from the Authorization Request Response/0110 message if a partial approval response.
- The issuer acknowledges full and partial reversal requests using a Reversal Request Response/0410 message.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Mastercard ATM Cash Pick-Up Service

The Mastercard ATM Cash Pick-Up service allows money to be sent to individual recipients who obtain their funds from an ATM which has been upgraded with the ATM Cash Pick-Up software.

The service recipients receive a code (via, for example, a Short Message Service [SMS] text message) that they can enter into the ATM; therefore, they do not need a debit card or relationship with a bank to receive funds.

The Mastercard ATM Cash Pick-Up service provides the following use cases for customers engaging in the service:

- Relief Fund Disbursement
- Emergency Cash Assistance
- Cash Rewards
- Person to Person Payments
- Small Insurance Claims
- Government Aid Payments/Social Benefits
- Compensation

To Participate

To participate in the Mastercard ATM Cash Pick-Up service, acquirers and issuers must contact their Mastercard Implementation Representative.

Mastercard ATM Network

The Mastercard® ATM Network provides cash access around the world to credit and ATM debit cardholders by accepting cards bearing the Mastercard, Maestro, and Cirrus logos.

All Mastercard issuers must participate in the Mastercard ATM Network to provide cash access to their cardholders. For more information about ATM participation, refer to the *Security Rules and Procedures*.

Where permitted, issuers may provide to their cardholders the option of conducting various transactions, such as balance inquiries and merchandise purchases, using the Mastercard ATM Network.

The Mastercard ATM Network is the world's largest global ATM network. It has more ATMs, in more countries, accessed by more cardholders, conducting the most transactions than any other ATM network. The Mastercard ATM Network and processors continue to provide a superior percentage of completed transactions. Cardholders using Mastercard®, Maestro®, and Cirrus® cards know that they can expect to receive the cash they requested.

For information about ATM transaction processing capabilities for Europe region acquirers that process through the Mastercard Network, refer to ATM Processing for Europe Region Acquirers.

Data Security

Evaluation of a number of possible security schemes, such as Internet Protocol Security (IPSec), Secure Sockets Layer (SSL) or Transport Layer Security (TLS) shows that these introduce too great a timing overhead on transactions for the transit environment.

Accordingly, an alternative security scheme should be used to overcome these time issues. The scheme should take into consideration whether the terminal can support software or hardware encryption.

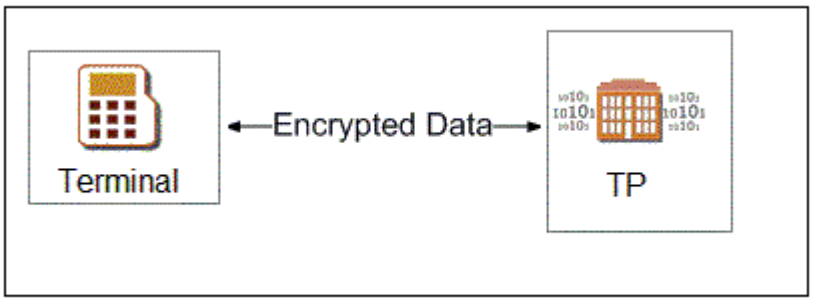
If software encryption is supported, the use of the Advanced Encryption Standard (AES) and symmetric session keys is recommended to encrypt and decrypt data.

If hardware encryption is supported, AES may be slower and 3-key Triple DES (3DES) and symmetric session keys may be an alternative viable option to encrypt and decrypt data. 3-key 3DES is preferable over 2-key 3DES.

Both methods have the advantage of introducing almost no time overhead.

Each session key is associated with a session key ID to uniquely identify the key which has been used in securing the data.

The session keys and corresponding key IDs shall be loaded securely into the terminal in a secure loading area and should be changed periodically and securely through a Maintenance Management System The terminal should therefore allow for the remote distribution of key files.



Global ATM Locator

The Mastercard Global ATM Locator is a set of websites and toll-free automated voice recognition systems that cardholders use to search for ATMs.

Cardholders access the Mastercard Global ATM Locator using:

- The Internet
- Mobile phones
- Personal digital assistants
- Voice response telephone numbers

- Onboard vehicle navigation systems
- Bank websites

Maps and directions to ATMs are available in many countries.

Location Administration Tool

The Location Administration Tool enables customers and processors to efficiently manage and market their ATM location information and service-related terminal attributes to help drive transaction volume and increase revenue at the point-of-interaction. Services include ATMs, Mastercard® contactless terminals, Pre-Paid Travel, and Mastercard® *rePower*™.

Benefits

The Mastercard ATM Network provides numerous benefits to cardholders, acquirers, and issuers.

- Cardholders benefit from the Mastercard ATM Network because the network provides:
  - Worldwide access to cash 24 hours a day, seven days a week
  - No need to carry large sums of cash
  - Favorable currency conversion exchange rate
- Acquirers benefit from the Mastercard ATM Network because the network provides:
  - Interchange income each time a Mastercard or Cirrus cardholder uses an ATM owned by that acquirer that displays the Mastercard and Cirrus logos
  - Competitive advantage by accepting Mastercard, Maestro, and Cirrus cards having worldwide recognition and acceptance
  - More transactions from more cardholders, lowering the cost per transaction
- Issuers benefit from the Mastercard ATM Network because the network provides:
  - Competitive advantage by offering Mastercard®, Maestro®, and Cirrus® cards having worldwide recognition and acceptance
  - Fee revenue opportunities

Supported Transactions

The Mastercard ATM Network supports a variety of transactions.

- Cash withdrawal from debit accounts
- Cash disbursement from credit accounts
- Account balance inquiry from debit accounts
- Available balance inquiry from credit accounts
- Tokenized transactions at contactless ATMs initiated by Near Field Communications (NFC)-enabled devices and wallets
- Chip PIN management transactions (PIN Change and PIN Unblock for Chip cards)
- Magnetic Stripe PIN management (PIN Change only) transactions
- Merchandise purchase from debit accounts for items, such as postage stamps and other items approved by Mastercard.

Acquirers must successfully complete testing for ATM merchandise transaction before submitting merchandise purchase transactions to Mastercard.

- Mastercard® MoneySend™ transactions.
- ATM Bill Payment is allowed for domestic transactions only when the service is offered domestically. When ATM Bill Payment is not allowed, acquirers will receive a response of Transaction not permitted to acquirer/terminal.
- Credit Card Cash Advance in Installments transactions at the ATM are allowed when the service is offered domestically.

Restrict Cash Access and ATM Balance Inquiry Transactions

Issuers can restrict cash access at the ATM to align the processing systems with Mastercard product rules. When the issuer has restricted cash access, acquirers receive DE 39 (Response Code), value 57 (Transaction not permitted to issuer/cardholder) in the Authorization Request Response/0110 message.

In addition to cash access restrictions, Mastercard allows issuers to restrict ATM balance inquiry transactions. When the issuer has restricted ATM balance inquiries, acquirers receive DE 39, value 57 in the Authorization Request Response/0110 message.

Interfaces to the Mastercard ATM Network

Mastercard issuers can choose either of the following options to receive authorization requests for ATM transactions.

- A direct interface to the Mastercard ATM Network
- An interface via the Mastercard Network to the Mastercard ATM Network

Direct Interface

Issuers that choose to interface directly with the Mastercard ATM Network receive ATM transactions via a Financial Transaction Request/0200 message.

For a description of the 0200 messages, refer to the *Single Message System Specifications* manual, the *Mastercard Rules*, and the *Transaction Processing Rules*.

Interface via the Mastercard Network

If the issuer chooses to receive ATM transactions via the Mastercard Network, the issuer receives ATM transactions in an Authorization Request/0100 message.

Choosing to receive ATM transactions via the Mastercard Network in Authorization Request/0100 messages gives issuers the following additional options:

- Mastercard validation of the PIN
- Application of Mastercard Stand-In processing when the issuer is unavailable (only if Mastercard also validates the PIN)

PIN Validation

Issuers can choose to have Mastercard validate the PINs or to validate the PINs themselves.

WHEN…	THEN…
Mastercard validates the PIN	Mastercard performs this service before forwarding the Authorization Request/0100 message to the issuer.
The issuer validates the PIN	Mastercard forwards the PIN to the issuer with the Authorization Request/0100 message.

Issuers that validate their own PINs must send to Mastercard the encryption key to translate encrypted PINs in the online request message.

Issuers that choose to have Mastercard validate PINs for ATM transactions must complete the *PIN Processing Profile* (Form 269) and must provide PIN verification keys by completing the *Hard Copy Key Exchange* (Form 723).

Stand-In Processing

Issuers can choose whether to have Stand-In processing process online request ATM transactions when they are not available. Issuers may choose whether to allow transactions with unverified PINs to be processed in the Stand-In System or to have Mastercard validate a PIN if a PIN is present in an online request message when the issuer is unavailable.

WHEN the issuer requests that…	THEN Mastercard…
Mastercard allow transactions with an unverified PIN in Stand-In processing	Processes the online request message.
Mastercard perform Stand-In processing and PIN validation	Processes the online request message and validates the PIN.
Mastercard not allow transactions with unverified PINs and not perform PIN validation during Stand-In processing	Returns a response of decline when the issuer is unavailable.

ATM Processing for Europe Region Acquirers

Mastercard provides ATM transaction processing capabilities for Europe region acquirers that process through the Mastercard Network.

NOTE: Applies only to the Europe region.

Acquirers using the Mastercard Network submit transactions using Customer Interface Specification (CIS), which is a dual message format. This processing only allows Europe region acquirers to submit ATM transactions via their dual message connection to the Mastercard Network.

ATM transactions are identified by:

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) containing one of the following values:
  - 00 (Purchase)
  - 01 (Withdrawal)
  - 30 (Balance Inquiry)
  - 91 (PIN Unblock)
  - 92 (PIN Change)
- DE 48 (Additional Data—Private Use), position 1 (Transaction Category Code [TCC]) containing value Z (ATM Cash Disbursement)

Only specified acquirers have this functionality. To ensure the transactions are submitted by eligible acquirers, the Authorization Platform verifies the acquirer parameter when an Authorization Request/0100 transaction is determined to originate from an ATM. ATM transactions provided by eligible acquirers are forwarded to the issuer. The Authorization Platform will respond to all other requests with an Authorization Request Response/0110 message containing DE 39 (Response Code), value 58 (Transaction not permitted to acquirer/terminal).

ATM Access Fee

Acquirers in approved Europe region countries may optionally apply an ATM access fee to domestic cash withdrawal transactions. Acquirers may charge ATM access fees on Mastercard, Maestro, or Cirrus cross-border transactions, as long as the access fee charged on those transactions is not higher than the access fee charged in connection with a transaction of any network accepted at that ATM. If another network accepted at the ATM prohibits the acquirer from charging an ATM access fee on cross-border ATM transactions, the acquirer must not charge an ATM access fee on Mastercard, Maestro or Cirrus cross-border transactions at the ATM. If all other networks accepted at the ATM permit the acquirer to charge access fees on cross-border ATM transactions, the acquirer will be permitted to charge an ATM access fee on cross-border Mastercard, Maestro, and Cirrus ATM transactions.

Acquirers include the transaction amount and access fee in DE 4 (Amount, Transaction) and the access fee amount (if applicable) in DE 28 (Amount, Transaction Fee) of Authorization Request/0100 and Reversal Request/0400 messages.

Mastercard Cardless ATM Program

The Mastercard Cardless ATM Program enables cardholders to initiate cash withdrawals using an issuer's mobile banking application (app) and to complete the transaction at an enabled ATM without the use of their physical card.

NOTE: Effective 11 June 2019 with Release 19.Q2, Mastercard will launch the Mastercard Cardless ATM Program and implement switching enhancements to support the program.

Mastercard enables an issuer and ATM operator to allow cardholders to view the fee of an ATM cash withdrawal in advance of conducting the transaction from an enabled ATM using

their mobile banking app. Cardholders may initiate the withdrawal using their mobile banking app after their arrival at the ATM or any time in advance of the withdrawal. At the ATM, cardholders will scan a Quick Response (QR) code or manually enter a code displayed on the ATM. After viewing any transaction fees in their mobile banking app, cardholders will authenticate the withdrawal using their mobile device. Mastercard will pass the token and details of the withdrawal to the ATM operator about the authorization request. If the transaction is approved by the issuer, the ATM will dispense cash to cardholders.

The Mastercard Cardless ATM Program supports cardless cash withdrawals initiated on the Mastercard Network or those received from alternate networks via the Mastercard Direct Services Access (MDSA) or Alternative Network Routing Solution (ANRS) protocols.

NOTE: Mastercard does not enable Visa tokenized accounts carrying a Mastercard ATM brand.

Benefits

The Mastercard Cardless ATM Program is a digital ATM solution that provides improved security, convenience, and transparency to consumers, drives engagement in the mobile banking app, and reduces time and cost of teller service cash disbursements for issuers. The Mastercard Cardless ATM Program allows ATM acquirers to meet the increased security expectations of issuers and consumers and leverages the use of existing network capabilities for authorization, settlement, and reconciliation.

To Participate

Customer participation in the Mastercard Cardless ATM Program is on an opt-in basis. Acquirers and issuers that want to participate in the Mastercard Cardless ATM Program must contact their Mastercard Implementation Representative.

Mastercard Contactless Mapping Service

Mastercard® contactless cards and devices that contain a proximity chip offer consumers a fast and convenient way to pay.

Using proximity chip payment technology, consumers can pay for their purchases at the point of sale by simply tapping their contactless card or device on a contactless terminal. The contactless card or device transmits the card information to the terminal. The contactless terminal interacts with existing authorization mechanisms to initiate and complete the authorization. The increased speed and convenience make contactless an attractive way to pay, especially in high-traffic environments such as mass transit stations, movie theaters, and fast food restaurants.

The Contactless Mapping Service is not available to issuers that support the use of online PIN with a card or device product. If PAN mapping is performed in a transaction using online PIN, the PIN validation will fail.

Contactless Mapping Service Description

Mastercard recommends that a unique account number be used for contactless transactions. This added layer of security protects issuers and cardholders against the risk of fraudulent acquisitions and use of a contactless account number.

One cardholder account is assigned two numbers:

- A primary account number (PAN), which is encoded on the magnetic stripe and embossed on the front of the card.
- A different contactless account number, which is personalized on the contactless chip of the same card or on a companion contactless device.

Implementation of a separate contactless account number requires the issuer to:

- Allocate a contactless account number to provide Contactless Mapping functionality for an existing PAN.
- Establish and maintain a cross-reference or mapping database between the PAN and the contactless account number.
- Upgrade the issuer host system to recognize that both account numbers must debit the same cardholder account and that:
  - The contactless account number must be accepted only when the transaction is originated at a contactless terminal.
  - The PAN must be accepted only when the card is swiped or when the PAN is provided by manual entry on a POS, on the Internet, or over the phone.

A contactless account number is a unique number encoded on the proximity chip of a contactless card or device that the Contactless Mapping Service associates to a PAN. A primary account number (PAN) is the number that is embossed, encoded, or both, on a Mastercard card that identifies the issuer and the particular cardholder account.

Mastercard recognizes that the use of a separate contactless account number for some issuers may not be viable. For this reason, Mastercard offers the Contactless Mapping Service—an optional service that helps issuers process contactless transactions by translating contactless account numbers into primary account numbers that issuers can process with minimal impact.

Mastercard offers two participating options for the Contactless Mapping Service:

- Processing-only Participation Only—At setup, the participating issuer provides Mastercard with a mapping file of PANs and contactless account numbers that it created and personalized on contactless cards or devices.
- Processing and Contactless Mobile Over-the-Air Provisioning—Mastercard offers secure web services that allow issuers to request both the contactless personalization of a near-field communication (NFC) mobile phone and its activation. Through the activation process, the registered PAN and contactless account number are mapped together.

Processing that is common to both participation options consists of the Authorization Platform translating contactless authorization requests into messages that the issuers' non–contactless-enabled authorization systems can understand and process.

Contactless Mapping Service Availability

Contactless Mapping Service availability varies.

- Processing Only—Available to contactless magnetic stripe-only cards or devices and contactless M/Chip and contact M/Chip devices (and cards under certain conditions).
- Processing and Contactless Mobile Over-the-Air Provisioning—Available depending on the issuer market.

Contactless Mapping Service Components

The Contactless Mapping Service consists of certain Authorization Platform components.

- PAN Mapping File (MCC106)
- Processing of contactless account number
- Transaction history

NOTE: Dynamic CVC 3 pre-validation is used when the Contactless Mapping Service is performed on contactless magnetic stripe transactions.

PAN Mapping File (MCC106)

The Contactless Mapping Service leverages the PAN Mapping File (MCC106). MCC106 contains the service-eligible contactless account number and the associated cardholder PAN. Each contactless account number is unique and several contactless account numbers can be associated to a single PAN (a family with the same PAN can have multiple contactless cards or devices).

Mastercard supports listing accounts for MCC106 with the Account Management System (AMS) via the following methods:

- Online File Maintenance
- Mastercard eService
- Mastercard File Express
- Mastercard Web services

MCC106 maintenance requests submitted via the online Issuer File Update Request/0302 message, Mastercard eService, or Mastercard web services are applied immediately. Maintenance requests submitted by bulk file are applied two times per day at 08:00 and 18:00 hours (St. Louis time).

Contactless Account Number

After performing a few edits, the Authorization Platform maps the contactless account number to the cardholder's PAN if indicated for the service-eligible contactless account range.

The following information provides the Authorization Platform processing details when the contactless account number is in a Contactless Mapping Service-eligible account range and listed or not listed in the PAN Mapping File (MCC106).

When the PAN Mapping File (MCC106) Contains a Contactless Account Number

If the contactless account number is found in the PAN Mapping File (MCC106), the Authorization Platform performs the following actions on Authorization Request/0100, Authorization Advice/0120, Reversal Request/0400, and Reversal Advice/0420 messages forwarded to the issuer, the Stand-In System, or the X-Code System:

- Inserts the cardholder's PAN in DE 2 (Primary Account Number [PAN])
- Inserts the PAN card expiration date in DE 14 (Date, Expiration) if available; otherwise, DE 14 is not present
- Performs dynamic CVC 3 pre-validation using CVC 3 validation key and algorithm only on the Authorization Request/0100 message where DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) contains value 91 (PAN auto entry via contactless magnetic stripe)
- Performs Chip Cryptogram pre-validation (if the issuer is signed up for it) on the Authorization Request/0100 message where DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) contains value 07 (PAN auto entry via contactless M/Chip)
- Inserts the result of the CVC 3 validation in DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services) if DE 22, subfield 1 contains value 91 or, if applicable, the result of the Chip Cryptogram if DE 22, subfield 1 contains value 07
- If DE 22, subfield 1 contains value 91, inserts DE 48, subelement 34 (Dynamic CVC 3 ATC Information) when the CVC 3 validation result was value V (Valid), A (ATC outside allowed range), or E (CVC 3 ATC Replay)
- Changes DE 22, subfield 1, value 91 (PAN auto entry via contactless magnetic stripe) to value 92 (Contactless input, Contactless Mapping Service applied when acquirer DE 22, subfield 1 = 91); or value 07 (PAN auto-entry via contactless M/Chip) to value 08 (PAN auto-entry via contactless M/Chip Contactless Mapping Service applied)
- Removes DE 35 (Track 2 Data) or DE 45 (Track 1 Data) or both
- Inserts DE 48, subelement 71 (On-behalf Services) results for Contactless Mapping Service

NOTE: In the contactless magnetic stripe Authorization Request/0100 message to the issuer, DE 48, subelement 71 contains two occurrences: one for the Dynamic CVC 3 Pre-validation service and one for the Contactless Mapping Service.

For Authorization Request Response/0110, Authorization Advice Response/0130, and Reversal Request Response/0410 messages forwarded to acquirers, the Authorization Platform:

- Inserts DE 48, subelement 33 (PAN Mapping File Information)
- Inserts DE 48, subelement 87 (Card Validation Code Result) only in the contactless magnetic stripe Authorization Request Response/0110 response if there were issues with the validation of the CVC 3

Acquirer response messages contain the same DE 2 value that was submitted by the acquirer.

When the PAN Mapping File (MCC106) Does Not Contain a Contactless Account Number

If the contactless account number is not found in the PAN Mapping File (MCC106), the Authorization Platform:

- Rejects the acquirer message and sends the acquirer the response in Authorization Request Response/0110, Authorization Advice Response/0130, and Reversal Request Response/0410 messages with DE 39 (Response Code), value 14 (Invalid card number)
- Creates an Authorization Advice/0120 message with DE 60 (Advice Reason Code), value 140 (Unable to Convert Contactless Account Number) and sends to the issuer

Alternate Processing

When applied to contactless magnetic stripe or contactless M/Chip transactions, the Contactless Mapping Service is performed before any alternate routing to the Stand-In System or the X-Code System.

Mastercard supports issuers that are not available to respond to the Authorization Request/0100 message by considering the results of the CVC 3 or Chip Cryptogram validation in DE 48, subelement 71 when the Stand-In System responds to the Authorization Request/0100 message. The options available for Stand-In System processing of CVC 3 results are detailed in the *On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications* manuals.

If the Stand-In System rejects a contactless magnetic stripe Authorization Request/0100 message because of issuer instructions based on CVC 3 validation results, Stand-In includes in the contactless magnetic stripe Authorization Advice/0120 message sent to the issuer the following values in DE 60, subfield 2:

- 0042 (CVC 3 Unable to Process)
- 0043 (CVC 3 ATC outside allowed range)
- 0044 (CVC 3 Invalid)
- 0045 (CVC 3 Unpredictable number mismatch)
- 0046 (CVC 3 ATC Replay)

In addition, the contactless magnetic stripe Authorization Advice/0120 message will include:

- DE 48, subelement 71
- DE 48, subelement 34, if DE 48, subelement 71 contains value V, A, or E
- DE 48, subelement 33
- DE 48, subelement 87, if there was a problem with the CVC validation

For more information about additional values sent if the Stand-In System rejects a contactless M/Chip Authorization Request/0100 message because of issuer instructions based on the Chip Cryptogram validation results, refer to the *M/Chip Processing Services—Service Description* guide.

Mastercard will not consider the CVC 3 or Chip Cryptogram validation results in X-Code processing and may approve an authorization request with an invalid CVC 3 or Chip Cryptogram.

Authorization Reports

Certain reports provide information that supports the Contactless Mapping Service.

- The Authorization Parameter Summary Report (SI737010-AA) provides an indicator in the Global Parameters section to identify the account ranges that are participating in the Contactless Mapping Service. Additionally, the On-behalf Services section lists the Dynamic CVC 3 Pre-validation Service for the participating Contactless Mapping Service account ranges and one of the Chip Cryptogram Validation Services if the issuer is signed up for one of these services.
- The Daily Account File Activity Report (AM700010-DD) contains the PAN Mapping File activity.

For a sample of the Authorization Parameter Summary Report (SI737010-AA), refer to Reports. For a sample of the Daily Account File Activity Report (AM700010-DD), refer to the *Account Management System User Manual*.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Mastercard Digital Enablement Service

The Mastercard Digital Enablement Service (MDES) is a secure, globally-scalable digitization platform for the management, generation, and provisioning of digital payment credentials onto mobile devices, PCs, servers, and other form factors. This provides simpler, more secure digital payment experiences.

MDES was developed to facilitate the financial industry transition from consumer account credentials stored on payment cards to digital credentials provisioned into mobile devices. These digitized credentials enable consumers to perform:

- Payments via existing contactless POS, other POS systems, and newer remote payment methods, such as in-app payments.
- Cash withdrawals or other financial transactions occurring at contactless ATMs with the use of Near Field Communications (NFC)-enabled devices and wallets.

MDES technology has been enhanced to allow the digitization of cardholder credentials stored on servers, facilitating more secure browser-based electronic commerce (e-commerce) and in-app transactions.

How It Works

MDES generates a token (formerly referenced as device account number) and provisions it to the secure element of the smart device, for example, or to secure cloud server solution. When a cardholder initiates a contactless or Digital Secure Remote Payment (DSRP) transaction using the token, the service validates the accompanying chip or dynamic CVC 3 data and maps the token to the cardholder's PAN.

Mastercard has also expanded POS entry modes applicable to MDES to support devices that are able to leverage a point-of-sale terminal magnetic stripe reader to pass dynamic transaction data.

MDES supports tokenization and digitization for Mastercard® cards, Debit Mastercard® cards, Maestro® cards, Maestro Prepaid, Mastercard branded Consumer Prepaid, and Debit Mastercard branded Consumer Prepaid cards.

What is a Token?

A token is a numeric value that does certain specific things.

- Acts as a surrogate for the primary account number (PAN) used by a payment card issuer to identify a payment card account.
- Issued in compliance with the EMV Payment Tokenization Specification Technical Framework.
- Passes the basic validation rules for a PAN, including the Luhn Formula for Computing Modulus 10 Check Digit.

A Mastercard Token is allocated from a BIN range designated by Mastercard to an issuer for a particular token implementation. Each Mastercard Token corresponds to a Mastercard account issued by an issuer using a Bank Identification Number (BIN) in the range reserved for Mastercard by the International Organization for Standardization (ISO). The range of PANs from which Mastercard Tokens are assigned will have the same attributes on Mastercard routing tables (for example, the same card product identifier) as the corresponding range of account PANs. Mastercard exclusively owns all right, title and interest in any Mastercard Token.

Token Types

Following are the MDES token types that can be contained in DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 1 (Account Number Indicator), which indicates the type of PAN mapping account:

- C = Mastercard Digital Enablement Service Secure Element Device Token
- F = Mastercard Digital Enablement Service Card on File Token
- H = Mastercard Digital Enablement Service Cloud-Based Payments Device Token

Following are the MDES token types that can be contained in the following data elements:

- DE 124 (Member-defined Data—General Use) subfields in Authorization Request/0100—Tokenization Eligibility
  - C = Mastercard Cloud-Based Payments
  - F = Card on File
  - S = Embedded Secure Element
- DE 124 subfields in Authorization Request/0100—Tokenization Authorization
  - C = Mastercard Cloud-Based Payments
  - F = Card on File
  - S = Embedded Secure Element

- DE 124 subfields in Authorization Request/0100—Tokenization Complete Notification
  - C = Mastercard Cloud-Based Payments
  - F = Card on File
  - S = Embedded Secure Element
- DE 120 (Record Data) layout for Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Complete Notification
  - C = Mastercard Cloud-Based Payments
  - F = Card on File
  - S = Embedded Secure Element

Authorization Processing Flow

For details about data requirements, refer to the *Customer Interface Specification* manual, or the MDES Information Center on Mastercard Connect™.

Suspended or Deactivated Tokens

When a token has been suspended or deactivated from use and an authorization request is received for that token, Mastercard will decline the transaction on behalf of the issuer and return DE 39 = 62 (Restricted card) to the acquirer. DE 48, subelement 33 will not be present with the cardholder's primary account number. Mastercard will send the issuer an authorization advice message with DE 60, subfield 1 = 141 and subfield 2 = 0202 (Reject: Token in suspended status) or 0203 (Reject: Token deactivated).

Authorization Reports

Certain reports contain information about MDES.

- The Authorization Parameter Summary Report (SI737010-AA) includes a MDES participant parameter in the Global Parameters section.
- The Daily Account File Activity Report (AM700010–AA) includes activity for the MDES within AM700010-CC.
- The Detail Account Report (AM730010-AA) includes a section for MDES accounts.

NOTE: Tokenized device account listings are now listed on the Detail Account Report – Mastercard Digital Enablement Service Device Tokens (AM730010-BB). Refer to the following section.

For a sample of the Authorization Parameter Summary Report (SI737010-AA), refer to Reports. For samples of the Daily Account File Activity Report (AM700010-CC) and Detail Account Report (AM730010-AA), refer to the *Account Management System User Manual*.

Detail Account Report – Mastercard Digital Enablement Service Device Tokens (AM730010-BB)

The Detail Account Report – Mastercard Digital Enablement Service Device Tokens (AM730010-BB) contains all tokenized device account listings for a customer. This report

shows device tokens currently on file with the digitization service and their associated status (active, suspended, or deactivated).

The Detail Account Report – Mastercard Digital Enablement Service Device Tokens (AM730010-BB) separates all tokenized device account listings from the Detail Account Report (AM730010-AA). This allows customers to view device tokens alone in one report every month, if they opt to receive it. This report eliminates the need to scan through the list of all types of accounts (including non-tokens) to check a specific device token.

The Detail Account Report – Mastercard Digital Enablement Service Device Tokens (AM730010-BB) uses the same structure as the Detail Account Report (AM730010-AA).

NOTE: Tokenized account listings are no longer located on the Detail Account Report (AM730010-AA).

The Detail Account Report – Mastercard Digital Enablement Service Device Tokens (AM730010-BB) contains the following sections:

- Secure Element Tokens
- Mastercard Cloud-Based Payments Tokens

These two sections identify the type of device token provisioned via the MDES.

The Secure Element Tokens section is present when Mastercard has one or more secure element tokens on file for the issuer in the Account Management System.

The Mastercard Cloud-Based Payments Tokens section is present when Mastercard has one or more Mastercard Cloud-Based Payments tokens on file for the issuer in the Account Management System.

The Detail Account Report – Mastercard Digital Enablement Service Device Tokens (AM730010-BB) is provided monthly via the T318 bulk file or eService OnLine Reports.

For a sample of the Detail Account Report – Mastercard Digital Enablement Service Device Tokens (AM730010-BB), refer to the *Account Management System User Manual*.

Becoming a Token Issuer

Before a Mastercard issuer may participate in MDES as a Token Issuer, the issuer must use the MDES Portal to register and establish a Token Issuer account with Mastercard.

Token Issuer Requirements

In addition to complying with section 6.1.4, Tokenization of Accounts, in the *Mastercard Rules*, a Token Issuer must complete certain steps.

- Support real-time Mastercard Token authorization request messages, and either support pre-Digitization messages for purposes of ID&V, or set ID&V Default Rules so that Mastercard may perform this function on its behalf
- Upload Digital Card Images that correspond to Accounts in the Mastercard Token Account Range to the MDES Portal, and grant the right for the appropriate Digital Card Image to be transmitted to the Token Requestor

- To participate in a particular Token Implementation, opt in to that Token Implementation and set ID&V Default Rules based on the ID&V Parameters of the relevant Token Implementation Plan
- Delete immediately, and not store for any period of time, any consumer data made available by a Wallet Token Requestor to the Token Issuer pursuant to a Cardholder's request for the Tokenization of an Account

Issuers have the option to receive activation code notification, tokenization complete notification, and tokenization event notification messages as well as send Account Management System online or bulk files to update, suspend, resume, or deactivate tokens.

An Issuer's MDES participation automatically terminates upon the termination of its participation with Mastercard.

Refer to the *Mastercard Digital Enablement Service Issuer Implementation Guide* for more information about issuer participation in MDES.

Becoming a Wallet Token Requestor

Before a Digital Wallet Operator (DWO) may participate in MDES as a Wallet Token Requestor, the DWO, or its sponsoring Customer must use the MDES Portal to register with Mastercard. The proposed Wallet Token Requestor must establish a Wallet Token Requestor account and be approved by Mastercard to participate in MDES.

Upon completion of the DWO's registration as a Wallet Token Requestor, Mastercard will assign a Token Requestor ID (TRID) to the DWO.

Wallet Token Requestor Requirements

A Wallet Token Requestor must comply with certain requirements.

- Unless the Wallet Token Requestor is an Issuer, contact Mastercard via e-mail at sdp@Mastercard.com to validate its compliance with the Payment Card Industry Data Security Standard by certifying the successful completion of an annual onsite assessment by a Payment Card Industry (PCI) Security Standards Council (SSC) approved Qualified Security Assessor (QSA) and quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV), as set forth in section 10.3.2 of the Security Rules and Procedures manual.
- Before participation begins and on an ongoing basis thereafter, perform testing and obtain any necessary certifications of its equipment, procedures, and systems as Mastercard may require to ensure compatibility with its technical specifications then in effect, and ensure its capability to transmit all required Mastercard Token authorization request message data.
- Register to use the Mastercard Open API at the following site: https://developer.Mastercard.com/portal/display/api/API/registration/process.
- Establish a Token Implementation Plan that is acceptable to Mastercard and complies with MDES Specifications.
- For each Mastercard Token implementation, use ID&V Parameters that are equivalent to those set forth in the Token Implementation Plan, regardless of whether MDES will Digitize the Accounts or the Mastercard Token Vault will perform PAN mapping and cryptography validation of the Mastercard Tokens.

- Support the display of a Digital Card Image and any terms and conditions supplied by the Token Issuer on the Mobile Payment Device. Mastercard and Maestro branding on a Mobile Payment Device must be approved by Mastercard prior to implementation, as described in the Contactless Branding in Mobile Applications section of the Mastercard Contactless Branding Standards document.

Mastercard reserves the right to approve, refuse to approve, require the modification of, or withdraw the approval of a Token Implementation Plan, and to suspend, either temporarily or permanently, a Wallet Token Requestor's MDES participation. A Customer may submit a written request that Mastercard's Chief Franchise Integrity Officer review such action, provided the request is postmarked within 30 days of the date on which notice of the action was received, and is signed by the Customer's principal contact. Any decision by the Chief Franchise Integrity Officer is final and not subject to further review or other action.

Wallet Token Requestor Obligations

A Wallet Token Requestor must avoid certain criteria.

- Disparage Mastercard or any of Mastercard's products, programs, services, networks, or systems.
- Inhibit or prevent a Mastercard account provisioned onto a Mobile Payment Device from being used to make in-application purchases at a merchant capable of processing DSRP Transactions.
- Obscure or misuse any Mastercard Mark, Issuer's logo, or Digital Card Image.
- Present Mastercard as a payment option in terms that are less favorable than those offered with respect to other payment options.
- Provide incentives with the intent of encouraging consumers to cease using a Mastercard or Maestro Account as the default payment option in its Digital Wallet, including but not limited to offering a direct or indirect reward or benefit to doing so.

Notwithstanding the foregoing, and for the avoidance of doubt, a merchant located in the United States Region or a U.S. Territory may take any action set forth in section 5.11.1, Discrimination, of the *Mastercard Rules*.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Mastercard In Control Services

The Mastercard In Control™ platform provides for a number of advanced authorization, transaction routing, and alert notification capabilities designed to assist issuers in creating new and enhanced payment products for their consumer and commercial cardholders.

Mastercard In Control fully integrates patented payment technologies with unparalleled global processing capabilities. With the integration of this capability into Mastercard core processing, issuers can benefit from cost efficiencies and speed to market for new product development.

Participation in Mastercard In Control is optional.

Mastercard In Control Purchase Controls

The Mastercard In Control™ Purchase Controls service platform 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.

Benefits

The Mastercard In Control Purchase Controls service platform allows issuers to leverage off-the-shelf solutions and create customized offerings depending on the needs of their customers.

The commercialization of the Mastercard In Control services platform offers issuers the following features to support their commercial card portfolios:

- 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.

NOTE: Purchase Controls is the first application that is specific for commercial cards, featuring virtual card numbers (VCNs) and usage controls. Additional applications will be added in the future.

Authorization Processing

Mastercard In Control platform leverages the same authorization and clearing data elements for mapping virtual card numbers and real card numbers.

For a Mastercard In Control authorization transaction that was successfully mapped and met control specifications:

1. The acquirer sends the Dual Message System an Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or a Reversal Request/0400 message 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 (PAN).
3. The Authorization Platform sends the Authorization Request/0100 message and performs mapping via the 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) contain 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), subfield 1 (On-behalf Services) = value 17 (In Control Virtual Card Service) and 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. 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).
7. If Mastercard 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).

Exception Processing

For a Mastercard In Control authorization transaction that was declined by In Control processing:

1. The acquirer sends the Dual Message System an Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, or a Reversal Request/0400 message 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 PAN.
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 containing DE 39 (Response Code), value 14 (Invalid card number).
4. If PAN mapping of the transaction is successful, but the transaction fails spend control rules, the Authorization Platform sends an Authorization Advice/0120—System-generated message to the issuer containing:

   - DE 2 (Primary Account Number [PAN])
   - DE 39 (Response Code) with a value other than 00 (Approved or completed successfully)

- 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) where:
  - Subfield 1 (Advice Reason Code) = 200 (In Control Processing Advice to Issuer)
  - Subfield 2 (Advice Detail Code) = appropriate advice reason code

Authorization Reports

The following reports provide information about the Mastercard In Control service:

- The Authorization Parameter Summary Report (SI737010-AA) includes a Mastercard In Control Mapping participant parameter in the Global Parameters section.
- The Daily Account File Activity Report includes a separate report for the Mastercard In Control service. The Daily Account File Activity Report (AM700010-EE) displays activity associated with Mastercard In Control.
- The Detail Account Report (AM730010-AA) displays Mastercard In Control accounts.

For a sample of the Authorization Parameter Summary Report (SI737010-AA), refer to Reports. For a sample of the Daily Account File Activity Report (AM700010-EE) and Detail Account Report (AM730010-AA), refer to the *Account Management System User Manual*.

To Participate

Issuers that want to participate in the Mastercard In Control Purchase Controls initiative can contact the Global Customer Service team for more information.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Mastercard In Control Real Card Spend Control Services

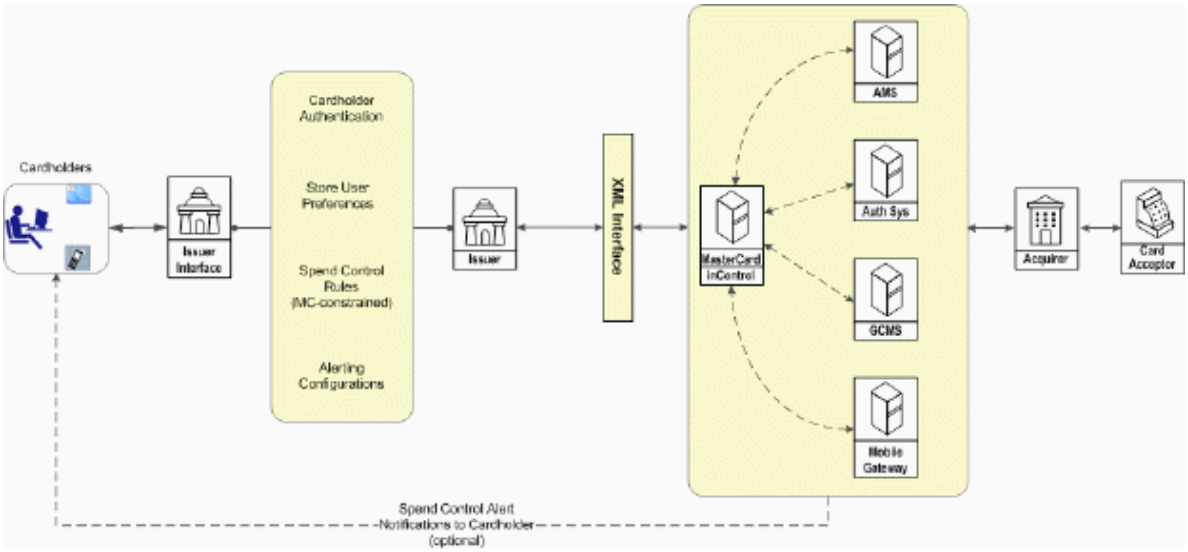
The Mastercard In Control™ Real Card Spend Control service targets the consumer cardholder segment and offers a broad suite of authorization control categories that provide increased security and budgetary monitoring capabilities coupled with an optional Short Message Service (SMS) alerting service.

Benefits

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.

How It Works

The following illustration provides a high-level overview of the Mastercard In Control Real Card Spend Control services registration process.



1. Participating issuers create a website that provides a secure interface to Mastercard In Control and enables cardholders to register for one of the real card spend control services.
2. The issuer's website passes account information, associated spend control rules, and accompanying actions such as decline instructions and alert notifications to Mastercard In Control.
3. The Mastercard In Control service submits a real-time registration request to the Account Management System. Activation of the initial registration of the first card within an eligible account range may take up to 48 hours; activation of subsequent accounts will occur within 24 hours.
4. The Account Management System sends a confirmation message to Mastercard In Control.
5. Mastercard In Control notifies the issuer website that the cardholder controls have been established.
6. The issuer notifies the cardholder that their spend control rules have been set up.
7. Cardholders can revisit their issuer's website to modify or delete their spend control rules.

Authorization Processing

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.

1. 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 Dual Message System.

2. The Authorization Platform sends the transaction to Mastercard In Control for verification against the cardholder's registered spend control rules.

WHEN the transaction...	THEN Mastercard In Control...
Meets 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).
Does not meet 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: – DE 48, subelement 71: – Subfield 1 contains value 20 – Subfield 2 contains the spend control rule that failed – DE 60 (Advice Reason Code): – Subfield 1 (Advice Reason Code) contains value 200 (In Control Processing Advice to issuer) – Subfield 2 (Advice Detail Code) contains a valid advice reason code and Sends the cardholder an alert notification indicating rule failure.
Does not meet 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, 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 Reports

The following reports provide information about the Mastercard In Control Real Card Spend Control service:

- The Global Parameters section of the Authorization Parameter Summary Report (SI737010-AA) includes a Mastercard In Control Real Card Spend Control participant parameter to indicate issuer account range participation in Mastercard In Control Real Card Spend Control services.
- The Daily Account File Activity Report (AM700010-EE) includes activity associated with the Mastercard In Control Real Card Spend Control service.

For a sample of the Authorization Parameter Summary Report (SI737010-AA), refer to Reports. For a sample of the Daily Account File Activity Report (AM700010-EE) and Detail Account Report (AM730010-AA), refer to the *Account Management System User Manual*.

To Participate

Issuers that want to participate in the Mastercard In Control Real Card Spend Control service can contact their Account Management team for more information.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Mastercard In Control Virtual Card Mapping and Spend Control Service

The Mastercard In Control™ Virtual Card Mapping and Spend Control Service is for consumer cardholders to request a virtual card number, and optionally establish spend controls on that virtual card, and receive alerts.

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.

Mastercard In Control Virtual Card Mapping and Spend Control Service authorization transactions are identified by:

- DE 2 (Primary Account Number [PAN]) contains the real card number
- DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information) contains the virtual account data
- DE 48, subelement 71 (On-Behalf Services) contains the on-behalf service performed on the transaction

The following information describes exception processing for a Mastercard In Control Virtual Card Mapping and Spend Control Service authorization transaction that was declined by In Control processing. Other possible scenarios for a virtual card number and virtual card number with spend controls are also described.

Virtual Card Number Scenarios

WHEN the...	THEN the Authorization Platform...
Virtual card number successfully mapped and a valid expiration date and CVC 2 are included	Forwards the Authorization Request/0100 message to the issuer.
Virtual card number was not successfully mapped	Rejects the Authorization Request/0100 message sent by the acquirer, and then sends an Authorization Advice/0120—System-generated message to the issuer.
Virtual card number successfully mapped, but contains an invalid expiration date or invalid CVC 2	Rejects the Authorization Request/0100 message sent by the acquirer, and then sends an Authorization Advice/0120—System-generated message to the issuer.

Virtual Card Number with Spend Controls Scenarios

WHEN the...	THEN the Authorization Platform...
Virtual card number successfully mapped, valid expiration date and CVC 2 are included, and the transaction passes spend controls	Forwards the Authorization Request/0100 message to the issuer.

WHEN the...	THEN the Authorization Platform...
Virtual card number was not successfully mapped	Rejects the Authorization Request/0100 message sent by the acquirer, and sends an Authorization Advice/0120—System-generated message to the issuer.
Virtual card number successfully mapped, but contains an invalid expiration date or CVC 2 And The cardholder wants optional alerts	Rejects the Authorization Request/0100 message sent by the acquirer, sends an Authorization Advice/0120—System-generated message to the issuer, and then sends an optional alert to the cardholder.
Virtual card number successfully mapped, valid expiration date and CVC 2 are included, but the transaction fails spend controls And The cardholder wants optional alerts, but does not want the transaction rejected	Forwards the Authorization Request/0100 message to the issuer, and then sends an optional alert to the cardholder.
Virtual card number successfully mapped, valid expiration date and CVC 2 are included, but the transaction fails spend controls And The cardholder wants optional alerts, but wants the transaction rejected	Rejects the Authorization Request/0100 message sent by the acquirer, sends an Authorization Advice/0120—System-generated message to the issuer, and then sends an optional alert to the cardholder.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Mastercard Consumer Controls

This section introduces Consumer Controls for issuers on the Dual Message System.

Product Overview

Consumer Controls enables issuers to meet popular transaction alerts and control cardholders' needs.

Issuers can offer available alerts and controls to their cardholders, based on the following:

- Transaction amount
- Channel (for example, ATM or online)
- Country in which a transaction originates (as in, cardholders may opt-in to alerts and controls for cross-border transactions)

- Static geographic location (include/exclude specific countries)
- Card acceptor business code (MCC) (single MCC or multiple MCCs)
- Budget limits
- Travel (included and excluded countries between valid to and valid from dates)

Also, cardholders can easily:

- Opt-in to receiving alerts for all transactions.
- Disable their card to temporarily stop (decline) all payments or transactions—excluding recurring payments.
- Set decline controls based on any combination of transaction amount, channel, country in which a transaction originates, static geolocation, or MCCs.

This robust feature set allows issuers to quickly implement a program to provide their cardholders with the most desirable alerts and controls.

By means of the Mastercard Authorization Network (the Mastercard global payment processing network), Consumer Controls supports value-added features for transactions. Consumer Controls complies with existing authorization message types and data element (DE) specifications. Transactions must authorize online to the Mastercard Authorization Network or route to Mastercard through Mastercard Direct Services Access (DSA) for non-Mastercard transactions for processing by the Consumer Controls application.

DSA provides issuers, acquirers, third-party processors (TPPs), or payment networks that do not switch their transaction activity on the Mastercard Network the ability to provide certain Mastercard value-added services to their customers. DSA enables customers and their authorized agents to access the Mastercard Network to apply certain services to their transactions using a Mastercard interface processor (MIP) that hosts the Direct Services Interface.

Consumer Controls features are applied in real time, based on data received as part of authorization request messages. In addition, the Consumer Controls platform is designed for global use and supports multiple currencies to meet the needs of Mastercard customers.

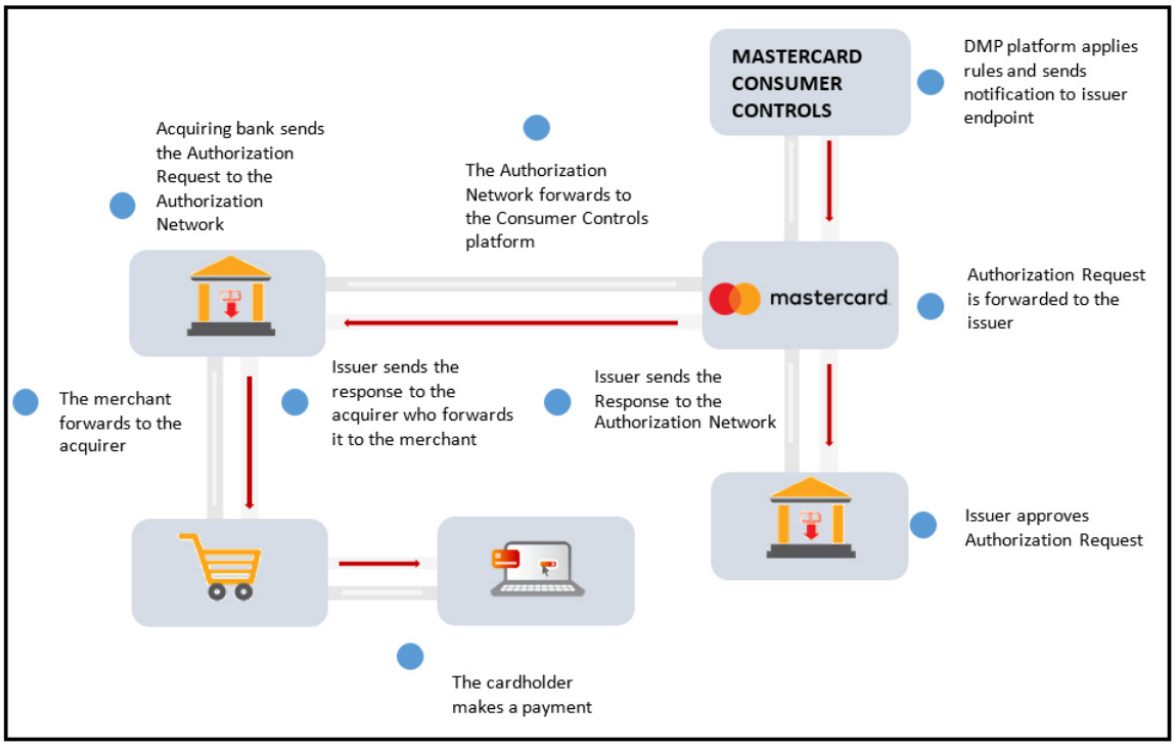
In summary, Mastercard Consumer Controls offers the following set of features:

- Alerts only for:
  - All transactions
  - Transaction amount (for example, decline and alert for transactions with a total value greater than USD 50.00)
  - Channel (for example, alert for internet transactions)
  - Transactions originating outside of a cardholder's home country (as in, cross-border transactions)
- Card On/Off:
  - Transaction declines for all transactions or for all transactions except recurring payments (for example, turn my card off temporarily)
- Controls (transaction declines and alerts):

- Based on transaction amount (for example, decline and alert for transactions with a total value greater than USD 50.00)
- Based on channel (for example, decline and alert for internet transactions)
- Based on country in which a transaction originates (for example, decline and alert for cross-border transactions)
- Based on static geolocation (for example, decline and alert for transactions originating inside or outside the United States and Canada)
- For MCCs (for example, decline and alert for transactions in electronic stores or decline and alert for transactions with an MCC in the travel category)
- For a combination of controls (for example, decline and alert for transactions in electronic stores of a total value greater than USD 1,000.00)
- Based on spending limits in an hourly or daily period (for example, alert when spending exceeds the limit set for an hourly or daily time interval)
- Based on static location(s) during a given time period (for example, alert for transactions in included and excluded countries between valid to and valid from dates with a user selected alias description)

Content, method (email, text, mobile), and delivery of alerts to cardholders is an issuer responsibility and is achieved based on the notification XML messages that Mastercard provides to an issuer during authorization processing when an alert triggers. The notification messages generated for alerts are delivered to the issuer in near real time.

The following diagram illustrates the typical transaction processing flow for a Mastercard transaction that is subject to Consumer Controls value-added features.



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 Consumer Controls. The Global Safety and Security Standards effective dates by region and territory are as follows:

- United States—21 April 2017
- Europe—13 October 2017
- Latin America and the Caribbean—13 October 2017
- Middle East/Africa—13 October 2017
- Ukraine—1 April 2018
- Asia/Pacific—13 April 2018
- Canada—13 April 2018

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.

To Participate

Issuers that want to participate in the Consumer Controls should contact their Account Management team.

For More Information

For more information on Consumer Controls, refer to the *Consumer Controls Program Guide* or the *Consumer Controls Product Application Specifications Guide*, available on the Mastercard In Control™ and Consumer Controls Information Center located on Publications via Mastercard Connect™.

From the Mastercard Connect home page, select **Library/Publications**. From the Publications page, select the drop down for **Information Centers**, then select **Mastercard In Control™ and Consumer Controls Information Center**.

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 following implementation guides, available on Mastercard Connect™.

- *Mastercard Installment Payment Service—Installment Calculation and Posting: Implementation Guide*
- *Mastercard Installment Payment Service—Point-of-Interaction Eligibility and Enablement: Implementation Guide*
- *Mastercard Installment Payment Service—Application Programming Interface: Implementation Guide*
- *Mastercard Installment Payment Service User Guide*

Mastercard MoneySend

Mastercard® MoneySend® is a set of Mastercard Network transactions that facilitate both domestic and cross-border funds transfer to and from Mastercard®, Maestro®, and Cirrus® branded Consumer Card Card and Eligible Small Business Commercial Card accounts, excluding anonymous prepaid and gift card accounts.

Receiving payment inflows to a Mastercard card account is considered a core product capability and fundamental to any financial account. The MoneySend Payment Transaction continues to enable funds to be transferred from cash or any approved account by an Originating Institution (OI) to any Mastercard®, Debit Mastercard®, Cirrus®, or Maestro® Card account held at a Receiving Institution (RI).

The MoneySend service also allows use of multiple channels to initiate transactions such as an ATM, a bank branch, a stand-alone kiosk, mobile, or over the Internet.

Financial institutions offering the MoneySend service may need to engage in two transactions to accommodate the funds transfer between the sender and the recipient:

- The MoneySend Funding Transaction is a purchase transaction that secures the sending consumer's funds, and moves them into an account at the OI. The OI has the option to enable the sender to provide funds through various channels:
  - An Internet banking site
  - A mobile device solution using either text messages or an application installed on the mobile device
  - An ATM
  - A kiosk
  - A bank branch
  - An agent location
  - A phone banking application
- The MoneySend Payment Transaction moves the principal amount designated in the Funding Transaction from the OI, via the Mastercard Network, to a Mastercard account at the RI.
- The second transaction, referred to as the Payment Transaction, moves funds from the OI, via the Mastercard Network, to the recipient of the funds and into a Mastercard®, Debit Mastercard®, Maestro®, or Cirrus® account (the Receiving Account) at the RI.

NOTE: Receiving Institutions who issue Debit and Prepaid cards must make the transferred funds available to the cardholder within 30 minutes of approval of the authorization request. Receiving Institutions who issue Credit cards must show the payment as a pending transaction in the Recipient's account within 30 minutes of authorization, so the cardholder knows it has been received and is being processed. The RI must post the transferred funds to the Recipient's Credit account within 24 hours (excluding non-processing days which vary by market—example: Sundays or holidays).

For participation requirements or for more information about this optional service, refer to the *MoneySend Program Guide*.

Mastercard MoneySend Funding Transactions

Mastercard® MoneySend™ Funding Transactions are identified in Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, Reversal Request/0400 messages by certain values.

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 00 (Purchase Transaction)
- DE 4 (Amount, Transaction) (For transaction-value limits, refer to the *MoneySend Program Guide*.)

NOTE: The MoneySend transaction amount is less than or equal to the maximum amount for the particular MoneySend funding transaction type. The Authorization Platform validates the Authorization Request/0100 message against the MoneySend maximum transaction amount limit for that transaction type. Currency conversion on the MoneySend transaction will be completed before comparing it to the maximum transaction amount limit.

- DE 18 (Merchant Type), MCC 6538 (MoneySend Funding Transaction) to identify a MoneySend Funding Transaction
- DE 48 (Additional Data—Private Use), transaction category code (TCC), value R (Retail Sale) or T (Phone, Mail, or Electronic Commerce Order) as appropriate to the transaction environment
- Appropriate MoneySend value from DE 48, subelement 77 (Funding/Payment Transaction Type Indicator)

OFIs may optionally send DE 108 (MoneySend Reference Data) and/or DE 124 (Member-defined Data) when submitting a MoneySend Funding Transaction.

Mastercard requires originating financial institution (OFI) participation when submitting a MoneySend Funding Transaction.

Mastercard MoneySend Payment Transactions

The MoneySend Payment Transaction provides a unique message to facilitate remittances between two parties: a sender (person, business, government, or non-government entity) using the services of a financial institution acting on the sender's behalf, referred to as the originating financial institution (OFI)—the Payment Transaction acquirer—and the recipient who receives the funds when they are deposited into his or her Mastercard or Maestro account at another financial institution, referred to as the receiving financial institution (RFI)—the recipient's card issuer.

Mastercard requires that OFIs register in the MoneySend service to participate. OFI registration in the MoneySend service helps to ensure that only institutions, which have been approved for these types of money transfers, are attempting to process them. OFI registration also helps to protect RFIs from receiving these types of transactions from merchants and OFIs that do not meet the MoneySend program guidelines.

If an OFI attempts to submit a MoneySend transaction, but has not registered for the MoneySend service, the Authorization Platform 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).

Mastercard MoneySend Transaction Criteria

Mastercard® MoneySend™ Payment Transactions must meet certain criteria.

- The originating financial institution must be a registered participant.
- The Authorization Request/0100 or Reversal Request/0400 message must contain:
  - DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 28 (Payment Transaction)

– DE 4 (Amount, Transaction) (For transaction-value limits, refer to the *MoneySend Program Guide*.)

  NOTE: The MoneySend transaction amount is less than or equal to the maximum amount for the particular MoneySend payment transaction type. The Authorization Platform validates the Authorization Request/0100 message against the MoneySend maximum transaction amount limit for that transaction type. Currency conversion on the MoneySend transaction will be completed before comparing it to the maximum transaction amount limit.

– DE 18 (Merchant Type), MCC 6536 (MoneySend Intracountry) or MCC 6537 (MoneySend Intercountry)
– Appropriate MoneySend value from DE 48 (Additional Data—Private Use), subelement 77 (Funding/Payment Transaction Type Indicator)
– DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level) contains one of the valid values that indicate the location where the transaction was initiated
– DE 124 (MoneySend, Sender Identification Data), subfield 2 (Sender/Payer Name/User ID) and subfield 3 (Sender/Payer Address) and may contain optional subfield 4 (Date of Birth)
– DE 108 (MoneySend Reference Data), subelement 01 (Receiver/Recipient Data), subfield 1 (Receiver/Recipient First Name), and subfield 3 (Receiver/Recipient Last Name) required for cross-border transactions. DE 108, subelement 02 (Sender Data), subfield 1 (Send First Name), subfield 3 (Sender Last Name), subfield 11 (Sender Account Number) and subelement 03 (MoneySend Transaction Data), subfield 3 (Funding Source) are required for all MoneySend payment transactions.

The Authorization Platform will reject an Authorization Request/0100 or a Reversal Request/0400 message that does not meet the edits for a properly formatted MoneySend transaction.

Mastercard MoneySend Transaction Blocking Criteria

The Dual Message System supports transaction blocking for Mastercard® MoneySend™ Payment Transactions at the country and receiving financial institution (RFI).

Transaction blocking may occur at the following levels:

- Country—When Mastercard has determined that processing via MoneySend will not be supported in a particular country, the Authorization Platform automatically declines all MoneySend Payment Transaction authorization requests sent to or received from that country.
- Receiving financial institution—When Mastercard has determined that an RFI or associated RFI account range is not eligible to process transactions via MoneySend, the Authorization Platform automatically declines all MoneySend Payment Transaction authorization requests with that RFI.

Block All Transactions

Mastercard has enhanced the On-Behalf opt-in service MoneySend Issuer Transaction Controls by adding a control to block all MoneySend Payment and MoneySend Funding transactions.

The Block All control is limited to issuers on a case-by-case basis and only available upon request. The block all control will deny all the MoneySend Payment and MoneySend Funding authorization transactions that are submitted in both the Dual Message System (Authorization) and Single Message System for specific account ranges.

Authorization Report

The Authorization Parameter Summary Report (SI737010-AA) includes a MoneySend Blocking flag in the Global Parameters section that identifies whether an RFI's account range is blocked from processing transactions via the MoneySend platform.

For a sample of the Authorization Parameter Summary Report (SI737010-AA), refer to Reports.

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 transactions and U.S. domestic transactions. 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.

To Participate

Originating financial institutions are required to register and be approved to participate as originating financial institutions for Mastercard® MoneySend™ transactions.

Before launching the MoneySend program, originating financial institutions must:

- Complete the registration process by completing and submitting the appropriate forms below to the email address provided on each respective form:
  - New customers:
    - *Application for License(s) to Use Service Marks* (Form 0631)
    - *Mastercard Network Payment Transaction Service—Enrollment Form (Global)* (Form 1060)
  - Existing customers:
    - *Change in License(s) and Activity Form* (Form 0637)

  - *ICA Request Form* (Form 0658)
  - *Mastercard Network Payment Transaction Service—Enrollment Form (Global)* (Form 1060)
- Receive written confirmation from Mastercard that their participation is approved. Once approved by Mastercard, an authorized Mastercard representative signs the *Mastercard Network Payment Transaction Service—Enrollment Form (Global)* and returns it to the originating financial institution's contact person.

Receiving financial institutions must support MoneySend Payment Transactions in authorization processing, unless their country of origin prohibits it legally. If the receiving financial institution does not want to allow the cardholder to receive money via MoneySend Payment Transactions, the issuer should decline the authorization.

Receiving financial institutions that participate in the MoneySend program must adhere to requirements for Payment Transactions and the MoneySend program.

For More Information

For more information about implementing the MoneySend program, refer to the *Mastercard MoneySend Program Guide* or contact the Global Customer Service team.

For more information about supporting data requirements, refer to the *Customer Interface Specification* manual.

Mastercard Payment Gateway

The Mastercard Payment Gateway (Payment Gateway) is a Mastercard hosted, centralized, modular gateway for routing commercial payments between buyers and suppliers.

NOTE: Applies only to the U.S. region.

The Payment Gateway collects, transforms, and routes commercial payment instruction orders. The Payment Gateway accepts files containing payment instructions and remittance advice information from commercial buyers. Payment instructions are generated directly from the buyer's Enterprise Resource Planning (ERP) or Accounts Payable system.

Benefits

Key features of the Payment Gateway include:

- Data translation and routing
- Bank connectivity that is available anywhere and anytime
- Universal supplier directory
- Remittance advices to buyers and suppliers
- Payment views and reports
- Straight Through Payment Processing
- Web-based portal

How It Works

The Payment Gateway supports two payment types:

- Payables Account (virtual Purchasing Card) payments
- Electronic Funds Transfer (EFT) payments

The authorization blocking feature supports Payables Account (virtual Purchasing Card) payments only.

The Payment Gateway does not replace the financial institution's existing commercial payment offerings. Rather, it provides the entryway for receiving a buyer's payment files, thus providing a single destination or interface for business-to-business payment processing. In this way, Mastercard does all the work of file translation and data mapping, but the actual payment processing remains the domain of the financial institutions.

The Payment Gateway uses a modular approach. Financial institutions can market and package distinct modules to augment their existing payment services.

Issuers that offer commercial cards may choose to restrict the authorization of certain account ranges to occur through the Payment Gateway by participating in the Mastercard Payment Gateway Authorization Blocking service.

The Authorization Platform determines whether to continue processing or reject Payment Gateway authorization requests based on the presence of DE 48 (Additional Data—Private Use), subelement 47 (Mastercard payment Gateway Transaction Indicator), value MC-MPG/W and the issuer's participation in the Mastercard Payment Gateway Authorization Blocking service.

Authorization Reports

The Authorization Parameter Summary Report (SI737010-AA) includes a Mastercard Payment Gateway participant parameter in the Global Parameters section, which indicates when an issuer participates in the Mastercard Payment Gateway Authorization Blocking service. For a sample of this report and field descriptions, refer to Reports.

Mastercard Payment Gateway Authorization Blocking Service

The Mastercard Payment Gateway Authorization Blocking service allows issuers to restrict the authorization of transactions to only those originating from the Mastercard Payment Gateway platform.

To participate in the Mastercard Payment Gateway Authorization Blocking service, issuers can send their requests to Mastercard via email at: eB2B@Mastercard.com.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Mastercard Transit Transactions

Mastercard transit transactions are limited to transit MCCs and can be pre-funded, real-time authorized, post-authorized aggregated, or authorized-aggregated split clearing.

Pre-funded Transit Transactions

A pre-funded transit transaction occurs when the cardholder purchases value redeemable for future travel with a transit merchant. The purchased value is held by the transit merchant in an account linked to the cardholder's card or device. Any usage of the card or device following the purchase of value will reduce the value held with the transit merchant.

The transit merchant follows its usual authorization procedures by generating an Authorization Request/0100 message for the full amount of the transaction.

Real-time Authorized Transit Transactions

A real-time authorized transit transaction occurs when the transit merchant generates an Authorization Request/0100 message each time a cardholder uses his or her card or device at the transit merchant's terminal.

The transit merchant follows its usual authorization procedures by generating an Authorization Request/0100 message for the full amount of the transaction.

Post-authorized Aggregated Contactless Transit Transactions

A post-authorized aggregated contactless transit transaction occurs when the transit merchant generates a First Presentment/1240 message combining one or more contactless taps performed with one contactless account number and occurring with one transit merchant.

For the contactless transit merchant to receive chargeback protection all of the following must occur:

- The transit merchant must send a properly identified Authorization Request/0100 message, which can be for any amount not exceeding the cardholder verification method (CVM) limit amount, as published in *Chargeback Guide* on the day of the transaction.
- The issuer must have approved the transaction.
- The combined amount of the contactless taps must be equal to, or less than, the cardholder verification method (CVM) limit amount, as published in the *Chargeback Guide*.
- The maximum time period from the first contactless tap until the First Presentment/1240 message is generated must be 14 calendar days or less.

NOTE: These transit transactions are limited to MCCs 4111, 4131, and 4784.

Upon the cardholder's request, the transit merchant must provide a list of the contactless taps that were combined into a First Presentment/1240 message.

NOTE: The phrases tap the contactless card or device and contactless tap refer to the same series of actions: a cardholder touching the contactless card or device to a contactless terminal, the contactless terminal reading the card data, and then the contactless terminal flashing a light and making a sound to indicate the outcome of the tap to the cardholder.

Authorized-aggregated Split Clearing Transactions

An authorized-aggregated split clearing transaction is subject to the following restrictions.

NOTE: Applies only to domestic United Kingdom (U.K.) transactions.

- The contactless-enabled card or device must indicate that an M/Chip profile is supported.
- Tag 5F28 (Issuer Country Code) must have a value of 826.
- The denominated primary currency is GBP.
- The transaction is properly identified in the same manner as described in Post-authorized Aggregated Contactless Transit Transactions, with the exception that the value in the transit indicator field is value 4, instead of value 3.

NOTE: These transit transactions are limited to MCCs 4111, 4131, and 4784.

Post-authorized Aggregated Maestro Contactless Transit Transactions

A post-authorized aggregated Maestro contactless transit transaction occurs when the acquirer generates an Authorization Request/0100 message for an estimated or maximum amount in connection with the use of one Maestro contactless account number at one transit merchant.

The transit merchant can combine multiple Maestro contactless taps into a single transaction amount and reverse any unused funds by the cardholder at the end of the aggregation time period.

The transactions are processed as follows:

- The transit merchant sends an Authorization Request/0100 (Europe-acquired only) message containing value 06 in DE 48, subelement 64, subfield 1 (Transit Transaction Type Indicator) for an estimated or maximum amount not to exceed the applicable Maestro contactless transit transaction ceiling limit amount (or post-authorized aggregated Maestro contactless transit transaction ceiling limit amount, if established for the transit merchant's country. If not, the existing Maestro contactless transit transaction ceiling limit amount for that country applies).
- The issuer must have approved the transaction.
- The cardholder may make subsequent taps for additional rides. These taps will not be sent to the issuer for authorization. The combined amount of the taps must be equal to or less than the applicable Maestro contactless transaction ceiling limit amount.
- When the authorized amount is reached or within three calendar days (two days in Mexico), the transit merchant totals the value of all taps and generates a partial Reversal Request/0400 or an Authorization Advice/0120 message to reverse any unused funds. The Authorization Advice/0120 message option is only available for Europe region acquirers.

The transaction ceiling limit values for post-authorized aggregated Maestro contactless transactions will take the same values as the existing published Maestro contactless ceiling limits, except for select countries in the Latin America and the Caribbean region.

The transaction is properly identified in the same manner as described in Post-authorized Aggregated Contactless Transit Transactions, with the exception that the value in the transit transaction type identifier (in DE 48, subelement 64) has value 06.

NOTE: These transit transactions are limited to MCCs 4111, 4131, and 4784.

Post-authorized Aggregated Maestro Contactless Transit Transactions Criteria

All post-authorized aggregated Maestro contactless transit transactions must be properly identified.

Post-authorized aggregated Maestro contactless transit Authorization Request/0100 messages submitted by a transit merchant for Maestro contactless cards or devices must contain the following data element values.

Data Element	Subfield	Value
DE 4 (Amount, Transaction)	N/A	For post-authorized aggregated transactions, the authorization can be for any amount not exceeding the chargeback protection amount.
DE 18 (Merchant Type)	N/A	One of the following values: • 4111 (Transportation—Suburban and Local Commuter Passenger, including Ferries) • 4131 (Bus Lines) • 4784 (Bridge and Road Fees, Tolls)

Data Element	Subfield	Value
DE 22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	One of the following values: • 07 (PAN auto-entry via contactless M/Chip) • 08 (PAN auto-entry via contactless M/Chip, Contactless Mapping Service applied) • 09 (PAN entry via electronic commerce, including remote chip) • 10 (Credential on File) • 82 (PAN Auto Entry via Service [issuer, acquirer, or third-party vendor system]) • 91 (PAN auto-entry via contactless magnetic stripe) • 92 (Contactless input, Contactless Mapping Service applied when acquirer DE 22, subfield 1 = 91) **NOTE: Values 91 and 92 only apply to domestic Maestro transactions in Brazil. Acquirers do not send or receive values 08, 09, or 92. Only Mastercard sends values 08, 09, or 92 to the issuer when the Contactless Mapping Service is performed.**
DE 48 (Additional Data—Private Use), Subelement 64 (Transit Program)	1 (Transit Transaction Type Indicator)	06 (Post-Authorized Aggregated Maestro)
DE 61 (Point-of-Service [POS] Data)	1 (POS Terminal Attendance)	1 (Unattended terminal)
	3 (POS Terminal Location)	0 (On premises of card acceptor facility)
	4 (POS Cardholder Presence)	0 (Cardholder present)
	5 (POS Card Presence)	0 (Card present)
	6 (POS Card Capture Capabilities)	0 (Terminal/operator has no card capture capability)

Data Element	Subfield	Value
	7 (POS Transaction Status)	One of the following values: • 0 (Normal request) • 4 (Preauthorized request) **NOTE: Value 4 is only for Europe region acquired transactions.**
	10 (Cardholder-Activated Terminal Level)	0 (Not a CAT transaction)
	11 (POS Card Data Terminal Input Capability)	One of the following values: • 3 (Contactless M/Chip) • 4 (Contactless Magnetic Stripe)

Differences Between Post-authorized Aggregated and Authorized-aggregated Split Clearing Transit Transaction Rules

Differences between the current Mastercard post-authorized aggregated transit rule and the authorized-aggregated split clearing transit rule for U.K. transit transactions are listed in table format.

Post-authorized Aggregated Transit Transaction Rule	Authorized-aggregated Split Clearing Transaction Rule in the U.K.
The transit agency receives no chargeback protection in the event that an issuer declines the authorization.	Extends the transit agency's chargeback protection rights to include transactions for which the authorization on a U.K. issued credit, debit or prepaid card or device is declined, provided the authorization and clearing amounts are GBP 10 or less. **NOTE: Cards that do not meet the criteria to be eligible for this liability protection follow the Post-Authorized Aggregated Transit Transaction Rule, that is, an overseas issuer, issuing cards not denominated in GBP would not have any additional liability.**

Post-authorized Aggregated Transit Transaction Rule	Authorized-aggregated Split Clearing Transaction Rule in the U.K.
Each aggregation period (up to 14 days) is initiated by a single authorization and completed by a single clearing message. The aggregation period when processing Maestro transactions will be different. Time periods range from 1-3 days, depending on the region and country the transaction is being acquired.	Accommodates the UKCA transaction model by allowing the transit agency to submit a clearing message at the end of every day on which the card incurred transit spend (subject to either an approved authorization message or a declined authorization message and the spend being up to and including GBP 10.00). Therefore, there can be multiple clearing messages submitted between successive authorizations for the same card.

ATC Update Request

Authorization Request/0100 messages containing DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 6 (ATC Update) are used to notify the issuer of the most recent ATC (Application Transaction Counter) value for the contactless card or device.

All ATC Update authorization requests will have a zero value for the transaction amount. ATC update transactions may be sent on a regular basis, and issuers must ensure that these transactions do not affect the issuer's velocity checks. In addition, issuers should authorize these transactions using DE 39 (Response Code), value 00 (Approved or completed successfully) or 85 (Not declined), or decline these transactions using DE 39, value 05 (Do not honor) based on the fact that the ATC provided is within or outside of the issuer's ATC tolerance.

For approved transactions where the application cryptogram has been successfully validated, issuers should keep a record of the last seen ATC and set a feasible range. Subsequent transactions received which contain an ATC outside of this range should be treated as suspicious, but should not be routinely declined.

Acquirers supporting merchants that implement the Mastercard contactless aggregated models may support zero amount Application Transaction Counter (ATC) update Authorization Request/0100 messages to notify issuers of the most recent ATC values for the offline cardholder aggregation activity.

Transit Debt Recovery Transactions

Today, transit merchants typically work solely in a pre-paid environment in which the passenger purchases a ticket or a prepaid balance prior to travel. With transit merchants migrating to open loop payments where the card presented for payment is also used as a token at the point of entry, transit merchants may take some risk in allowing a cardholder to travel before receiving payment for his or her travel or even knowing if the account linked to the card being presented for travel is in good standing.

Mastercard Rules allow transit merchants to recover an amount owed to them (a transit debt recovery transaction) following a declined authorization request. A transit debt recovery transaction occurs when transit fare spend has been incurred, in granting a Mastercard contactless card access to travel, and as a result of the issuer declining the authorization request, the transit merchant is initially unable to collect payment for the fare spend. When this situation occurs, the transit merchant may add the card to a Deny List, thereby blocking that card from access to travel until such time as the money owed by the cardholder has been recovered.

A mechanism in which a cardholder's debt is cleared in order for the cardholder to access the transit system to resume travel is through debt recovery transactions. The Mastercard Contactless Transit Rules create the opportunity for this situation to arise:

- Post-authorized aggregated (Global)
- Authorized aggregated split clearing (U.K. and Republic of Ireland only)
- Post-authorized aggregated Maestro
- Any other transit implementation where the cardholder is allowed to travel prior to the authorization taking place (deferred authorization)

There are several methods of debt recovery that a transit merchant can implement and each method allows debt recovery transactions to recover a debt from a card or device.

Mastercard and Maestro contactless products allow debt recovery to be performed through the following mechanisms:

- Automatically—Presented as a card-not-present (CNP)/PAN key-entered transaction
- Call Centers—Presented as a CNP/MOTO (Mail Order/Telephone Order) transaction
- Websites—Presented as a CNP/e-commerce transaction
- Ticket-vending machines and other ticket office processing—Presented as a card present transaction

Support for U.K. Transit Transactions

Mastercard® and Maestro® contactless customers that choose to implement contactless cards and devices in the U.K. must process transit transactions according to the U.K. Cards Association Transit Transaction Model, published in *U.K. and Republic of Ireland Operations Bulletin* No. 6, 7 September 2011 Revised Standards for Mastercard *PayPass* Transit Transactions in the UK, *U.K. and Republic of Ireland Operations Bulletin* No. 8, 6 September 2012, and and Revised Standards for Mastercard Contactless Transit Transactions in the United Kingdom, *United Kingdom Operations Bulletin* No. 3, 7 October 2016.

All Mastercard contactless issuers globally (excluding those in the U.K.) will begin to process transactions according to global Mastercard Contactless Transit Rule 8.7.1 in *Mastercard Rules*.

Customers must ensure that their contactless cardholders are able to use their cards successfully for travel on public transport operated by Transport for London and other U.K. transit operators.

PAN-Association Requirements for Transit

Issuers that issue alternate account numbers for contactless products and respond to Authorization Request/0100 messages from MCCs 4111, 4131, 4784, and 7523 must provide the following values in DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information) when sending the Authorization Response/0110 message.

- Subfield 1 (Account Number Indicator), value E (Embossed Account Number Provided by Issuer)
- Subfield 2 (Account Number), embossed PAN
- Subfield 3 (Expiration Date), expiration date of the embossed PAN

For issuers participating in the Mastercard® Contactless Mapping Service, the Authorization Platform will provide these values on their behalf in the authorization response messages. This helps ensure that the pre-purchased fares by cardholders using the embossed PAN are properly associated with their turnstile requests. This will also help ensure proper customer service.

Acquirers processing for merchants belonging to MCC 4111, 4131, 4784, and 7523 must provide the DE 48, subelement 33 details when present in the authorization response message back to the merchants belonging to these MCCs upon their request.

Masterpass Transactions

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 **BUY WITH Masterpass** button (or the **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

For details about data requirements, refer to the *Customer Interface Specification* manual.

Member-defined Data

Mastercard allows customers to exchange as many as 299 bytes of member-defined data to and from another customer in authorization messages.

Customers may use member-defined data to transmit information such as:

- Loyalty program information
- Promotional information
- Details about a purchase or money transfer
- Any other business-related data

Structure of Member-defined Data

Acquirers may provide as many as 299 bytes of member-defined data in DE 124 of the Authorization Request/0100 message.

Issuers may provide as many as 299 bytes of member-defined data in DE 124 of the Authorization Request Response/0110 message. Issuers will receive DE 124 in Authorization Advice/0120 messages if DE 124 was present in the Authorization Request/0100 sent by the acquirer and the transaction was processed by Stand-In or X-Code processing.

The Authorization Platform will not edit the content of DE 124 as long as it is alphanumeric/special character data and is only as many as 299 bytes in length. The Authorization Platform

will limit the length of the member-defined data in DE 124 to 299 bytes in Authorization Request/0100 messages and 299 bytes in Authorization Request Response/0110 messages.

For additional details on providing member-defined data in DE 124, refer to the *Customer Interface Specification* manual.

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.

DE 48, Subelement 84 Values

Issuers can use certain values to indicate Merchant Advice codes in Authorization Request Response/0110 messages, DE 48, subelement 84.

Value	Description
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)

Common DE 39 Values

The most common values for DE 39 that issuers send in conjunction with the Merchant Advice codes are listed in table format.

Value	Description
00	Approved
05	Do not honor
14	Invalid card number

Value	Description
30	Format error
51	Insufficient funds/over credit limit
54	Expired card

DE 48, Subelement 84 with DE 39

In conjunction with existing values in DE 39 in Authorization Request Response/0110 messages, issuers should use the Merchant Advice codes provided in DE 48, subelement 84 to communicate which actions merchants can take to best support cardholders.

The following table provides examples of how issuers and acquirers should use the combination of DE 48, subelement 84 and DE 39.

DE 39	DE 48, subelement 84	Merchant Advice Description	Examples of Reasons	Suggested Merchant Action
00 05 14 51 54	01	New account information available	• Expired card • Account upgrade • Portfolio sale • Conversion	Obtain new account information before next billing cycle
51	02	Cannot Approve at This Time	• Over credit limit • Insufficient funds	Recycle transaction 72 hours later
05 14 51 54	03	Do not try again	• Account closed • Fraudulent	Obtain another type of payment from customer

DE 39	DE 48, subelement 84	Merchant Advice Description	Examples of Reasons	Suggested Merchant Action
39	04	POS cardholder presence indicator	• DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1, position 3 (UCAF Collection Indicator) = 7 (DSRP partial shipment/recurring payment) • Valid cryptography data in DE 48, subelement 43 (Universal Cardholder Authentication Field) • DE 48, subelement 43 containing PARTIALbSHIPMENTbbbbbbbbbbb or PARTIALSHIPMENT0000000000000	Resubmit with appropriate information
05	21	Payment Cancellation	Cardholder canceled agreement	Do not submit

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

The following information is required for each transaction block setup:

- ICA or Routing & 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.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual or *Quick Reference Booklet*.

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).

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.

Partial Approvals

The partial approval enables an issuer to approve a portion of the transaction amount in the authorization request when the transaction amount exceeds the amount of funds available on the debit card or prepaid card and the merchant terminal supports partial approvals.

An issuer can choose to provide a partial approval response amount that is less than or equal to the requested amount. An issuer can provide a partial approval response equal to the amount requested when the cardholder's account does not have a sufficient balance to cover any allowed amount over the requested amount for tips or service charges. The following scenario demonstrates the successful completion of a partial approval equal to the requested amount.

A cardholder pays USD 50 at a restaurant with a debit card that has an available balance of USD 50. The gratuity allowance for the restaurant MCC transaction is 20 percent. The issuer may use a partial approval response in the amount of USD 50 to indicate there are no additional funds and to obtain chargeback protection for any clearing amount submitted above USD 50 that was partially approved. The merchant must request another form of payment for any amount the cardholder may want to provide.

NOTE: For automated fuel dispenser (AFD) transactions (MCC 5542), an issuer may respond with a partial approval amount that is less than, equal to, or greater than the requested amount.

When the acquirer transmits an indicator in the authorization request that the merchant terminal supports partial approvals, the issuer has the option to respond with the partial approval amount and partial approval response code. The cardholder can then choose to use a supplemental payment method (split tender) to pay the balance and complete the purchase when the final transaction amount exceeds the partial approval amount.

All Debit Mastercard® card issuers (including prepaid) in the U.S. and Canada regions must support partial approvals and updates to the cardholder's open-to-buy balance upon receipt of a reversal (full or partial).

All acquirers in the U.S. and Canada regions that support merchants within select card acceptor business codes (MCCs) must support partial approvals for all Debit Mastercard®

account ranges, including all prepaid Debit Mastercard account ranges. This requirement applies only to card-present transactions occurring at attended terminals and at transactions identified with MCC 5542 (Fuel Dispenser, Automated).

Effective in 2020 with Release 20.Q2, issuers must support partial approvals for Debit Mastercard, Maestro, and prepaid Mastercard card account ranges. The acquirer of a merchant included in any of the MCCs listed in Effective Dates for Acquirer Mandate to Support Partial Approvals and Account Balance Responses Globally (for card present transactions conducted at attended terminals only) must support account balance responses for all prepaid card account ranges (Mastercard, Debit Mastercard, and Maestro). Mastercard reserves the right to expand the number of markets that may be required to support prior to 2020.

Benefits

The partial approval feature:

- Enables merchants and cardholders to successfully complete a higher percentage of debit card (including prepaid) purchases
- Reduces checkout time when the cardholder uses a debit card (including prepaid) with an available balance that is less than the transaction amount
- Provides acquirers to manage their financial risk by enabling them to only accept the approved amount, followed by a request for a different type of payment for a tip or service charge amount
- Allows issuers to use the current chargeback rules to prevent the approval amount from exceeding the cardholder's available balance. To use the chargeback rights, issuers will be required to respond with a partial approval amount that is less than or equal to the requested amount.

How It Works

When a merchant terminal indicates support of partial approval transactions, the acquirer sends an Authorization Request/0100 message containing DE 48 (Additional Data—Private Use), subelement 61 (POS Data, Extended Condition Codes), subfield 1 (Partial Approval Terminal Support Indicator), value 1 (Merchant terminal supports receipt of partial approvals).

When a merchant terminal indicates support of partial approval transactions and the cardholder's open-to-buy balance does not cover the full transaction amount, the issuer may respond to the authorization request with an Authorization Request Response/0110 message containing data elements necessary for a partial approval response, with DE 6 (Amount, Cardholder Billing) representing the cardholder's available purchase amount:

- DE 6 (Amount, Cardholder Billing) with the partial approval amount specified in the issuer's cardholder billing currency
- DE 38 (Authorization ID Response)
- DE 39 (Response Code), value 10 (Partial Approval)

When the issuer responds with DE 39, value 10 and the transaction is an AFD transaction, the amount in DE 6 may be less than, greater than, or equal to the requested amount in DE 6 of the Authorization Request/0100 message.

- DE 51 (Currency Code, Cardholder Billing)

Upon receipt of a partial approval, acquirers often send a balance due message to the integrated terminal. This message indicates the difference between the original purchase amount and the partial amount approved by the issuer. By displaying the remaining balance due amount, the cashier can quickly and accurately prompt the consumer to complete the split-tender purchase.

Acquirers should also advise the merchant of a partial approval that is equal to the request amount, so that the merchant does not add any gratuity.

Alternate Processing

The Stand-In processing and X-Code processing do not provide partial approval responses to authorization requests because these systems do not maintain card balances.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Payment Account Reference (PAR)

PEMVCo introduced PAR to provide an industry-aligned approach designed to help link all transactions associated with a specific account, whether PAN based or token based, without using the PAN as the linkage mechanism.

Mastercard is the BIN Controller (as defined by EMVCo standards) for PANs issued from the Mastercard product ranges of 222100–272099 and 510000–559999 and the Maestro product ranges of 639000–639099 and 670000–679999. Mastercard currently assigns a PAR to a given MDES tokenized PAN issued from these ranges.

Mastercard implemented PAR by supporting DE 56 in a limited set of Dual Message System (Authorization) and Single Message System messages, including authorization and financial request and response messages (both transactional and pre-digitization Tokenization Complete Notifications), and administrative advice pre-digitization Tokenization Complete Notifications.

This allowed Mastercard to communicate Mastercard-generated PAR values to MDES issuers and all acquirers in transactions containing a PAN associated with a BIN for which Mastercard is the BIN Controller and a PAR is available. When the issuer or third party entity is the BIN Controller and the issuer includes a PAR in the authorization request response or financial transaction request response message, Mastercard will send that PAR to the acquirer.

Mastercard supports the inclusion of DE 56 in the following messages when PAR is available for the applicable PAN and Mastercard is the BIN Controller.

Authorization	Single Message System	Mastercard is the BIN Controller
Authorization Request/0100	Financial Transaction Request/0200	Yes
Authorization Request Response/0110	Financial Transaction Request Response/0210	Yes
Authorization Request/0100—Tokenization Complete Notification	Financial Transaction Request/0200— Tokenization Complete Notification	Yes
Authorization Advice/0120—Acquirer-Generated	Financial Transaction Advice/0220—Debit Mastercard Stand-In	Yes
Authorization Advice/0120—System-Generated	Financial Transaction Advice/0220—Maestro Preauthorization Completion	Yes
Authorization Advice Response/0130—Issuer-Generated	Financial Transaction Advice Response/0230	No
Reversal Request/0400	Non-Financial Transaction Advice/0220	Yes
Reversal Request Response/0410	Issuer Reversal Advice/0422—Exception, System Initiated	No
Reversal Advice/0420	Acquirer Reversal Advice/0420—Acquirer Initiated	Yes
	Acquirer Reversal Advice/0420—Time-out-Induced, Acquirer Initiated	Yes
	Acquirer Reversal Advice/0420—Exception, System Initiated	Yes
	Acquirer Reversal Advice Response/0430—System Initiated	No
Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Complete Notification	Administrative Advice/0620—Issuer Token Notification Advice for Tokenization Complete Notification	Yes

NOTE: With Release 18.Q4, Mastercard enabled cardholders to use Near Field Communications (NFC)-enabled devices and wallets to initiate tokenized transactions at contactless ATMs. PAR values will not be included in tokenized, contactless ATM transactions.

Issuer PAR Requests

Issuers may request PAR manually, outside of the MDES tokenization process, for any account for which Mastercard is the BIN Controller using the getPaymentAccountReference service within the Payment Account Management API.

- PAR values are created for PANs when specifically requested by the issuer if Mastercard is the BIN Controller.
- Any issuer that requests the assignment of PAR values for their PANs must be capable of supporting the presence of DE 56 in the applicable Dual Message System (Authorization) and Single Message System messages.
- Mastercard includes PAR in messages sent to the issuer for any transactions involving a PAN for which a PAR value has been generated.
- Issuers should not request a PAR from Mastercard for PANs for which Mastercard is not the BIN Controller.

NOTE: PAR use is not limited to only MDES. Issuers are able to use PAR with other applications to link all transactions associated with a specific account.

Issuer Life Cycle Management of PAN-PAR Mapping

Issuers are required to properly manage PAN-PAR relationships stored by Mastercard when an account life cycle event occurs involving a PAN replacement or account closure. By properly managing the PAN-PAR relationship when a life cycle event occurs, jointly Mastercard and issuers can ensure the integrity of PAR within the payments ecosystem.

For example, if a consumer's plastic card is stolen and the PAN (for which Mastercard is the BIN Controller) is replaced, the issuer must inform Mastercard of the new PAN to ensure that the original PAR is associated with the new PAN. Or, when the issuer permanently closes a consumer's account, the issuer must inform Mastercard of the account closure to ensure the PAN-PAR relationship is eliminated.

NOTE: Issuers that recycle PANs for reissuance to subsequent consumers must ensure that obsolete PAN-PAR mapping relationships are eliminated within their systems and from Mastercard's PANPAR mapping file. This will ensure that the PAN is associated with a unique PAR value with each reuse of that PAN.

When Mastercard is the BIN Controller

When Mastercard is the BIN Controller for the PAN, issuers may choose from the following methods to manage PAR for PAN replacements and account closures.

PAN Replacement and Account Closure Methods:

- Automatic Billing Updater (ABU)
- Online or batch (bulk file type R311) Issuer File Update Request/0302 Maintenance (PAN-PAR Mapping via File Name MCC111)
- Payment Account Management (PAM) API

PAN Replacement Only Methods for MDES Issuers:

- Online or batch (bulk file type R311) Issuer File Update Request/0302 Maintenance (Token-PAN Mapping via File Name MCC 106)
- MDES Customer Service Application or MDES Customer Service API

AMS AM700010-II PAR Daily Account File Activity Report

Issuers that are connected to the Dual Message System (Authorization) have the option to request the AMS report (AM700010-II PAR Daily Account File Activity Report). This report contains PAN-PAR file maintenance activity requested by an issuer specifically via online or batch Issuer File Update Request/0302 Maintenance messages, using DE 101 File Name value MCC111. The report will be sent daily (on any day for which maintenance activity occurs), either by bulk file delivery or eService delivery, as requested by the issuer. The report is billed to issuers weekly via the following new MCBS billing event codes (based on report delivery method):

- 2RP6328B AM700010-II PAR Daily Account File Activity Report Bulk
- 2RP6328E AM700010-II PAR Daily Account File Activity Report eService

Issuers can request the new report by contacting their Global Customer Support representative.

Payment Cancellation

Payment Cancellation enables issuers to block unwanted card-not-present payment transactions identified in pre-authorization messages and completion records.

The cancellation of a payment will result in Mastercard declining future payment transactions for a specific account, if specified, from a particular merchant when requested by the cardholder.

Mastercard uses the issuer's payment blocking criteria to decline transactions when appropriate. Also, the Global Clearing Management System (GCMS) will use the same issuer payment blocking criteria to reject the clearing records.

Benefits

Payment Cancellation provides the following benefits to the parties involved in processing card-not-present and recurring payment transactions:

- Increases cardholder confidence to engage in preauthorized card-not-present and recurring payment transactions.
- Promotes card-not-present and recurring payments to increase cardholder transaction volume.
- Reduces cardholder dissatisfaction due to being charged after terminating a card-not-present or recurring payment arrangement with a merchant.
- Reduces chargebacks and costs of chargeback handling.

Once stopped, future charges will not occur, keeping the cardholder happy and saving issuers, acquirers, and merchants the expense and time to process chargebacks for cancelled transactions.

How It Works

Issuers participating in Payment Cancellation may submit recurring payment blocking criteria to the Payment Cancellation File database using one of the following methods:

- Online Issuer File Update/03xx messages (MCC105)
- Mastercard eService
- Single Message Transaction Manager

The Authorization Platform uses the issuer payment blocking criteria to decline online authorization requests for card-not-present and recurring payments, and the Global Clearing Management System (GCMS) uses the same issuer criteria to reject clearing records.

Acquirers receive Authorization Request Response/0110 messages containing DE 48 (Additional Data—Private Use), subelement 84 (Merchant Advice Code) with value 21 (Payment Cancellation [Mastercard use only]) indicating Payment Cancellation.

NOTE: The Authorization Platform—not the issuer—sends the Authorization Request Response/0110 message containing DE 48, subelement 84, value 21.

Issuers receive a store-and-forward Authorization Advice/0120 message indicating that the authorization request was blocked by the Authorization Platform.

Authorization Reports

The following reports provide information that support Payment Cancellation:

- The Authorization Parameter Summary Report (SI737010-AA) includes a Payment Cancellation participant parameter in the Global Parameters section.
- The Daily Account File Activity Report (AM700010-AA) includes a section to report the Payment Cancellation account maintenance activity. This section groups Payment Cancellation activity by rejected, accepted, and purged.
- The Delete Preview Report (AM710010-AA) includes a section to report the Payment Cancellation accounts that are due to be deleted in the next three weeks. A total field by ICA of Payment Cancellation accounts to be purged also will display.

For a sample of the Authorization Parameter Summary Report (SI737010-AA), refer to Reports. For a sample of the Daily Account File Activity Report (AM700010-AA) and Delete Preview Report (AM710010-AA), refer to the *Account Management System User Manual*.

To Participate

Issuers must notify Mastercard to participate in Payment Cancellation. To request participation, contact the Global Customer Service team.

For More Information

For more information about:

- Data requirement details, refer to the *Customer Interface Specification* manual.
- Payment Cancellation, refer to the *Payment Cancellation Program Guide*.

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, or issuer rebates and rewards.

The Payment Transaction is identified by DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 28 (Payment Transaction), DE 48 (Additional Data—Private Use), Transaction Category Code (TCC), value P (Payment Transaction), and the presence of DE 48, subelement 77 (Transaction Type Identifier).

Payment Transactions are identified in the following messages:

- Authorization Request/0100
- Authorization Advice/0120—System-generated
- Reversal Request/0400
- Reversal Advice/0420

Using the Transaction Type Identifier, acquirers can identify specific types of Payment Transactions in authorization messages. DE 48, subelement 77 will contain one of the following values:

- C01—Person-to-Person
- C02—Rebate
- C03—Load Value
- C04—Gaming Re-pay (available to Europe region customers only)
- 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 (available for Private Label card programs in the Europe region only)
- 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
- C59—MoneySend Cash2Card
- C65—MoneySend Business to Business Transfer

- F07—P2P Transfer
- F52—Account-to-Account Transfer
- F53—Agent Cash Out
- F54—Credit Account Bill Payment
- F61—Staged Wallet Load
- F64—Prepaid/Debit Card Account Load

For information about:

- Transaction Type Identifier value C04 used to support Gaming Payment Transactions (available to Europe region customers only), refer to Gaming Payment Transaction Processing in the Europe Region.
- Transaction Type Identifier values C07 and C52–C57 used to support the Mastercard® MoneySend™ Payment Transaction, refer to Mastercard MoneySend Payment Transactions.
- Transaction Type Identifier value C09 used for activation of private label prepaid cards at the point-of-sale terminal, refer to Activation and Initial Load of Private Label Prepaid Cards.

Payment Transaction Mandate

Mastercard has mandated that all acquirers and issuers support Payment Transactions.

Acquirers must support Payment Transactions according to the specifications documented in the *Customer Interface Specification* manual.

Issuers that have legal restrictions that prevent them from receiving authorization requests for Payment Transactions can request to block Payment Transactions. For issuers that meet this criteria, refer to Payment Transaction Blocking.

The following requirements apply to issuers in Italy:

- An issuer must support, process, and provide a valid authorization response to each Payment Transaction authorization request received, for all prepaid Mastercard®, Debit Mastercard® (including prepaid), and Maestro® card programs and all Mastercard charge card programs (revolving credit card programs are excluded).
- Except with respect to non-reloadable prepaid cards, an issuer must not automatically decline Payment Transactions.

For all other issuers, issuers can approve or decline Payment Transactions at their discretion.

For information about Payment Account Status Inquiry (Payment ASI) transactions, refer to Payment Account Status Inquiry.

Payment Transaction Blocking

Issuers that have legal restrictions that would prevent their participation in Payment Transactions can request to block Payment Transactions by completing and submitting the *Payment Transaction Blocking Form* (Form 530).

Mastercard must approve all issuer requests to block Payment Transaction authorizations.

For account ranges that issuers have arranged to have blocked, the Authorization Platform rejects Payment Transactions containing any account number within the account range listed in the Payment Transaction Blocked BIN file. The Authorization Platform returns a response code of Transaction not permitted to issuer/cardholder (DE 39 = 57) to the acquirer.

Issuers can block Payment Transaction authorizations at the account number range level (as many as 11 digits).

Optional Acquirer Use of the Payment Transaction Blocked BIN File

Acquirers also have the option to receive the Payment Transaction Blocked BIN file (T114 [Payment Transaction Blocked BIN File] and T115 [Test—Payment Transaction Blocked BIN File]) and may deny Payment Transactions to cardholders with accounts in the blocked account ranges.

Alternate Processing

Customers can choose to use Stand-In processing for Payment Transactions. Customers cannot use X-Code processing for Payment Transactions.

NOTE: Mastercard does not encourage customers to use Stand-In processing for Payment Transaction authorizations.

Stand-In Processing

If customers choose to use Stand-In processing for Payment Transaction authorizations, Mastercard recommends that customers use discretion for these transactions.

Parameters

Issuers may specify Stand-In processing parameters for Payment Transactions, including TCC global parameters and expanded parameter combinations with a TCC of P. The minimum/default value for Payment Transaction limits in Stand-In processing is USD 0.

NOTE: Stand-In processing declines Payment Transactions for issuers that do not specify a higher Stand-In processing limit for Payment Transactions. To set higher Stand-In processing limits, use the *Stand-In Processing—Transaction Category Code Global Parameters* (Form 0041g) to submit your requested limits.

Velocity Testing

Stand-In processing does not accumulate Payment Transaction activity for velocity testing. Stand-In processing does not add Payment Transactions to the cumulative number of approved transactions allowed or to the cumulative approved amounts allowed by the issuer.

X-Code Processing

Acquirer MIP X-Code processing will not approve Payment Transactions.

When X-Code processing processes the authorization, it will generate an authorization response of refer to card issuer (DE 39 = 01) for the Payment Transaction. During acquirer host

X-Code processing, the acquirer must issue a refer to card issuer response to the merchant for Payment Transaction authorizations.

E-Commerce Payment Transactions Using Tokens with or without Cryptographic Data

Effective 12 June 2018, Mastercard allows payment transactions to process without a cryptogram in DE 48 (Additional Data—Private Use), subelement 43 (Universal Cardholder Authentication Field [UCAF]) when they also contain DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 28 (Payment Transaction) in the Authorization Request/0100 message.

This functionality applies to the following transaction types:

- Electronic commerce (e-commerce)—Identified by DE 22 (POS Entry Mode), subfield 1 (POS Terminal PAN Entry), value 81 (PAN/Token entry via electronic commerce with optional Identity Check-AAV or DSRP cryptogram in UCAF or the Digital Payment Data Field)
- Credential on File—Identified by DE 22, subfield 1, value 10 (Credential on File)

Mastercard will reject payment transaction requests involving tokens without cryptograms that are not identified as payment transaction (DE 3, subfield 1, value 28).

PIN Management Services

Mastercard supports two PIN management services.

- Chip PIN Management Service—Supports both PIN change and PIN unblock functionality
- Magnetic Stripe PIN Management Service—Supports PIN change functionality only

Issuers that participate in the Chip PIN Management Service also must support the Magnetic Stripe PIN Management service.

Acquirers in the Europe region that process dual message transactions and that participate in the PIN Management service may optionally choose to support PIN change transactions for magnetic stripe cards.

Chip PIN Management Service

The Chip PIN Management service allows cardholders to perform the following transactions at ATMs that support Mastercard, Maestro, or Cirrus chip cards.

- PIN change—Allows cardholders to change the PIN code on their chip card.
- PIN unblock—Allows cardholders to unblock the PIN code on their chip card by resetting the PIN try counter.

The Chip PIN Management service is available only to full grade acquirers and chip grade issuers. For example, the Chip PIN Management service is not available for:

- Magnetic stripe-only cards.
- Transactions initiated with a chip card using magnetic stripe technology.
- Issuers that use the Chip to Magnetic Stripe Conversion service.

NOTE: Only Europe region acquirers are allowed to submit PIN change and PIN unblock transactions to the Dual Message System.

The Chip PIN Management service is an optional service.

Chip PIN Management Transactions

A cardholder can request a PIN change or PIN unblock only if submitting a valid online PIN. The online PIN is always transmitted to the issuer for validation.

NOTE: Participating issuers must define their own policies for handling forgotten PINs.

PIN Change Process

1. The cardholder enters a valid, online PIN at an ATM that supports Mastercard, Maestro, or Cirrus chip cards.
2. The cardholder must enter the new PIN twice. The ATM/acquirer compares the two new PIN blocks and sends a single encrypted new PIN block in DE 125 along with the old PIN encrypted in DE 52 to the issuer as part of the authorization request.
3. The ATM initiates an EMV chip transaction with the card requesting an Application Cryptogram (AC) for a transaction value of zero, unless an access fee has been applied by the acquirer for an ATM transaction in countries where application of an ATM access fee is allowed.
4. The acquirer sends the issuer an Authorization Request/0100 message containing DE 3, subfield 1, value 92 and the data from steps 2 and 3.
5. The issuer validates the online PIN and cryptogram, and then checks any other required information (for example, whether the unblock PIN status is set for the card in their system).
6. The issuer sends an Authorization Request Response/0110 message containing DE 39 (Response Code), which indicates whether to approve or decline the request. If the issuer approves the request, the 0110 message contains DE 39, value 85 (Not declined). In addition, the 0110 message may contain DE 55 with an issuer script. The issuer script contains instructions to the chip card:
   - If the issuer approves the PIN change request, the script message instructs the chip card to change the PIN on the card.
   - If the issuer declines the PIN change request, the issuer may optionally provide additional instructions to the chip card (for example, to block the card or the card application) using the related script.
7. The ATM confirms the status of the cardholder's request and the transaction is complete (that is, the script is applied successfully to the card). The cardholder will be advised if the transaction did not complete properly so that the cardholder understands the status of his or her card.

NOTE: For PIN change requests, it is important that incomplete transactions are properly reversed. A Reversal Request/0400 message must be initiated when the issuer times out or when the script is not successfully processed by the card. If not, there is a risk that the offline PIN on the card, the online PIN in the issuer host system, and the PIN thought to be correct by the cardholder become unsynchronized.

PIN Unblock Process

1. The cardholder enters a valid, online PIN at an ATM that supports Mastercard, Maestro, or Cirrus chip cards.
2. The ATM initiates an EMV chip transaction with the card, requesting an Application Cryptogram (AC) for a transaction value of zero, unless an access fee has been applied by the acquirer for an ATM transaction in countries where application of an ATM access fee is allowed. The Authorization Request/0100 message must include DE 52 to transmit the online PIN.
3. The issuer validates the online PIN and cryptogram, and then checks any other required information (for example, whether the unblock PIN status is set for the card in their system).
4. The issuer generates an Authorization Request Response/0110 message containing DE 39 (Response Code) that indicates whether to approve or decline the request. If the issuer approves the request, the 0110 message contains DE 39, value 85 (Not declined). In addition, the 0110 message will contain DE 55 with the system-generated Authorization Response Cryptogram (ARPC). Depending on the card application, DE 55 may contain an issuer script. The script message contains instructions to the chip card:
   - If the issuer approves the PIN unblock request, the script message instructs the chip card to unblock the PIN on the card.
   - 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.
5. The ATM confirms the status of the cardholder's request and the transaction is complete. The cardholder will be advised if the transaction did not complete properly so that the cardholder understands the status of his or her card.

Alternate Processing

The Authorization Platform does not support alternate processing via an alternate issuer host, the Stand-In System, or X-Code Processing for Chip PIN Management transactions.

Authorization Reports

The following reports provide information that supports the Chip PIN Management service:

- The Authorization Parameter Summary Report (SI737010-AA) includes a Chip PIN Management participant parameter in the Global Parameters section.
- The Authorization Summary Report (AB505010-AA) includes the Chip PIN Management Service values in the Response Code Decline category.

For a sample of the Authorization Summary Report (AB505010-AA) and Authorization Parameter Summary Report (SI737010-AA), refer to Reports.

Acquirer Requirements

Acquirers using the service are responsible for:

- Offering the PIN change option on their ATMs for chip cards
- Offering the PIN unblock option on their ATMs for chip cards
- Implementing the appropriate dialog between ATMs, chip cards, and cardholders to support the Chip PIN management options

Acquirers must ensure that the new PIN entered by the cardholder is correct. The new PIN is entered twice at the ATM, and the two encrypted PIN blocks must be compared either at the ATM or in the acquirer system. Acquirers only send one new encrypted PIN block to the issuer. If the two PIN blocks do not agree, the acquirer should invite the cardholder to re-enter their new PIN twice.

Acquirers must follow the normal EMV transaction flow at the ATM. The ATM is not expected to process the offline PIN in any way.

Acquirers must support script messages of any length, up to the maximum of 128 bytes.

Acquirers must ensure that the cardholder is accurately advised of the outcome of the PIN change or unblock transaction whether successful or not. This advice must take into account the response from the issuer, the network, and/or the response from the chip card once the script has been delivered to the terminal.

Acquirers send a Reversal Request/0400 message when the issuer times out or when the script is not successfully processed by the chip card.

Issuer Requirements

Issuers using the Chip PIN Management service must validate the ARQC (Authorization Request Cryptogram) transmitted in the Authorization Request/0100. Issuers should also check that the:

- Transaction amount is zero, unless an access fee has been applied by the acquirer for an ATM transaction in countries where application of an ATM access fee is allowed
- ATC (Application Transaction Counter) is greater than the last one received

An Authorization Request/0100 for a PIN unblock transaction may contain an AAC (Application Authentication Cryptogram) instead of an ARQC (depending on the issuer chip card application and card setup). The issuer must carry out the same validation checks on the AAC.

To Participate

Participating issuers and acquirers must notify Mastercard to participate in the Chip PIN Management service. To request participation, contact the Global Customer Service team.

Acquirers and issuers must complete the *PIN Management Service Request* (Form 888), and provide the form to the Global Customer Service team.

When the acquirer does not participate in the PIN Management service, the Authorization Platform sends the acquirer an Authorization Request Response/0110 message containing DE 39 (Response Code), value 58 (Transaction not permitted to acquirer/terminal). When the issuer does not participate in the service, the Authorization Platform sends the acquirer an Authorization Request Response/0110 message containing, DE 39, value 57 (Transaction not permitted to issuer/cardholder).

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Magnetic Stripe PIN Management Service

Mastercard® credit, Debit Mastercard®, Maestro®, or Cirrus® cardholders can change their PINs at any participating ATM for non-chip (magnetic stripe) cards that originate from the Mastercard Network.

Issuers that currently support PIN change for chip cards must support receiving PIN change transactions for magnetic stripe cards. Acquirers in the Europe region that currently support PIN change for chip cards and process dual message transactions may optionally choose to support PIN change transactions for magnetic stripe cards.

PIN Change Process

Participating acquirers in the Europe region that process transactions through the Dual Message System and issuers that choose to support ATM PIN change for magnetic stripe cards must process Authorization Request/0100 messages containing:

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 92 (PIN Change)
- DE 3, subfields 2 (Cardholder From Account Type Code) and 3 (Cardholder To Account Type Code), value 00 (Default Account [not specified or not applicable])
- DE 4 (Amount, Transaction) must contain a value of zero for PIN change transactions. When ATM transaction fees are allowed, DE 4 may have a value other than zero. In this case, the amount in DE 28 (Amount, Transaction Fee) is included in DE 4.
- DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) may contain a value of either:
  - 02 (PAN auto-entry via magnetic stripe—track data is not required). Value 02 is acceptable, as long as the track data is present.
  - 90 (PAN auto-entry via magnetic stripe—the full track data has been read)
- DE 52 (Personal ID Number [PIN] Data)
- DE 125 (New PIN Data) will consist of a binary block containing a derived encrypted value that corresponds with the cardholder's new PIN.

PIN Change Transactions

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 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 80 (Chip fallback) 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.

Alternate Processing

The Authorization Platform does not support alternate processing via an alternate issuer host, the Stand-In System, or X-Code System processing for PIN change transactions performed on magnetic stripe cards.

To Participate

Registration to participate in the Magnetic Stripe PIN Management service is not required for issuers and acquirers currently participating in the Chip PIN Management service. However, changes to add or delete account ranges must be submitted on the *PIN Management Service Request* (Form 888).

Acquirers in the Europe region and issuers that do not currently support PIN change transactions, but choose to support PIN change transactions performed at the ATM for magnetic stripe cards, must complete the *PIN Management Service Request* (Form 888). For more information about registration and testing, contact the Global Customer Service team.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

PIN Processing for Non-Europe Region Customers

The Authorization Platform supports processing of Mastercard purchase transactions that contain a personal identification number (PIN).

Cardholders may enter a PIN at the point-of-interaction as an alternative to signing a sales slip. The information in this section describes processing capabilities for non-Europe region acquirers and issuers that process through the Mastercard Network.

For information about PIN processing capabilities for Europe region acquirers and issuers that process through the Mastercard Network, refer to PIN Processing for Europe Region Customers.

Acquirer Requirements

Acquirers that choose to support PIN authorization requests must use their existing Mastercard MIP Authorization Platform interface connections with no changes in authorization message routing. Acquirers must comply with the following steps before processing Mastercard purchase transactions that contain a PIN in Authorization/01xx messages.

1. Determine whether to support static or dynamic PEK exchanges.

   The Authorization Platform and customers' systems use PEKs to encrypt or decrypt PINs. PEKs provide a secure means of passing PIN information in Authorization/01xx messages. Acquirers must determine whether they will support either static or dynamic PEK exchanges. For increased security, Mastercard strongly recommends using dynamic PEK exchanges.
2. Only acquirers that provide complete and unaltered track data in their Authorization Request/0100 messages can support PIN processing.
3. Ensure that applicable data elements are present in Authorization Request/0100 messages.

   For PIN authorization requests, Authorization Request/0100 messages must contain the following data elements:

   – DE 22 (Point-of-Service [POS] Entry Mode)
   – DE 26 (POS PIN Capture Code) (conditional)
   – DE 45 (Track 1 Data) or DE 35 (Track 2 Data)
   – DE 52 (PIN Data)
4. Ensure the ability to process applicable data elements in Authorization Request Response/0110 messages.

For detailed data element descriptions, refer to the *Customer Interface Specification* manual.

Issuer Requirements

Issuers must comply with the following steps before verifying the PINs in Mastercard purchase transactions that contain a PIN in Authorization Request/0100 messages.

1. Determine the method for receiving purchase transactions that contain a PIN from the following options:

- Through a Dual Message System Authorization Request/0100 message interface—This method is 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 Dual 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 Financial Transaction Request/0200 message interface—This method is the default method for issuers that currently receive their Debit Mastercard® card activity, ATM activity, or both using this interface. These transactions are identified as preauthorization requests with value 4 in position 7 of DE 61 because they must be cleared through the Mastercard clearing facility (the Global Clearing Management System) with all other purchase activity. PEKs that are already active and operational at the Dual Message System will be used for each of the issuer's BIN/card ranges.

2. Determine whether to support dynamic PEK exchanges.

   For dynamic PEK exchanges, the Authorization Platform and the issuer must establish a new single Key Encryption Key (KEK) for all BINs that the issuer will process. This new KEK must be associated with the issuer's Member Group ID that the issuer uses for sign-on, sign-off, and store-and-forward (SAF) sessions for the associated BINs.

   For increased security, Mastercard strongly recommends using dynamic PEKs.
3. Ensure the ability to process applicable data elements in Authorization Request/0100 messages.
4. Ensure the ability to process applicable data elements in Authorization Advice/0120 messages.
5. Ensure the ability to process applicable data elements in Reversal Advice/0420 messages.

NOTE: If an issuer does not comply with the requirements for verifying PIN data, the Authorization Platform will forward all authorization requests for purchase transactions that contain a PIN to the issuer with PIN data containing zeros. The issuer can then make the authorization decision based on other data within the authorization message.

For detailed data element descriptions, refer to the *Customer Interface Specification* manual.

Stand-In and Acquirer MIP X-Code Processing

Issuers may choose to have the Authorization Platform verify PIN data on their behalf. If the Authorization Platform performs PIN verification, it can perform Stand-In and X-Code processing using the existing authorization-qualifying criteria (issuer or Mastercard), 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 responds 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. For

more information about the option to allow transactions with unverified PINs in Stand-In processing, contact the Global Customer Service team.

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 use the same PEK, customers must use the same Customer ID as follows:

- As the Member Group ID for establishing the static PEK or the KEK.
- In DE 32 or DE 33 in all acquired transactions.
- In Member Group ID (DE 2) and DE 33 of the Network Management Request (PEK Exchange—On Demand)/0800 message.
- In DE 2 of the Network Management Request/0800 group sign-in message.

Authorization Platform Security Requirements

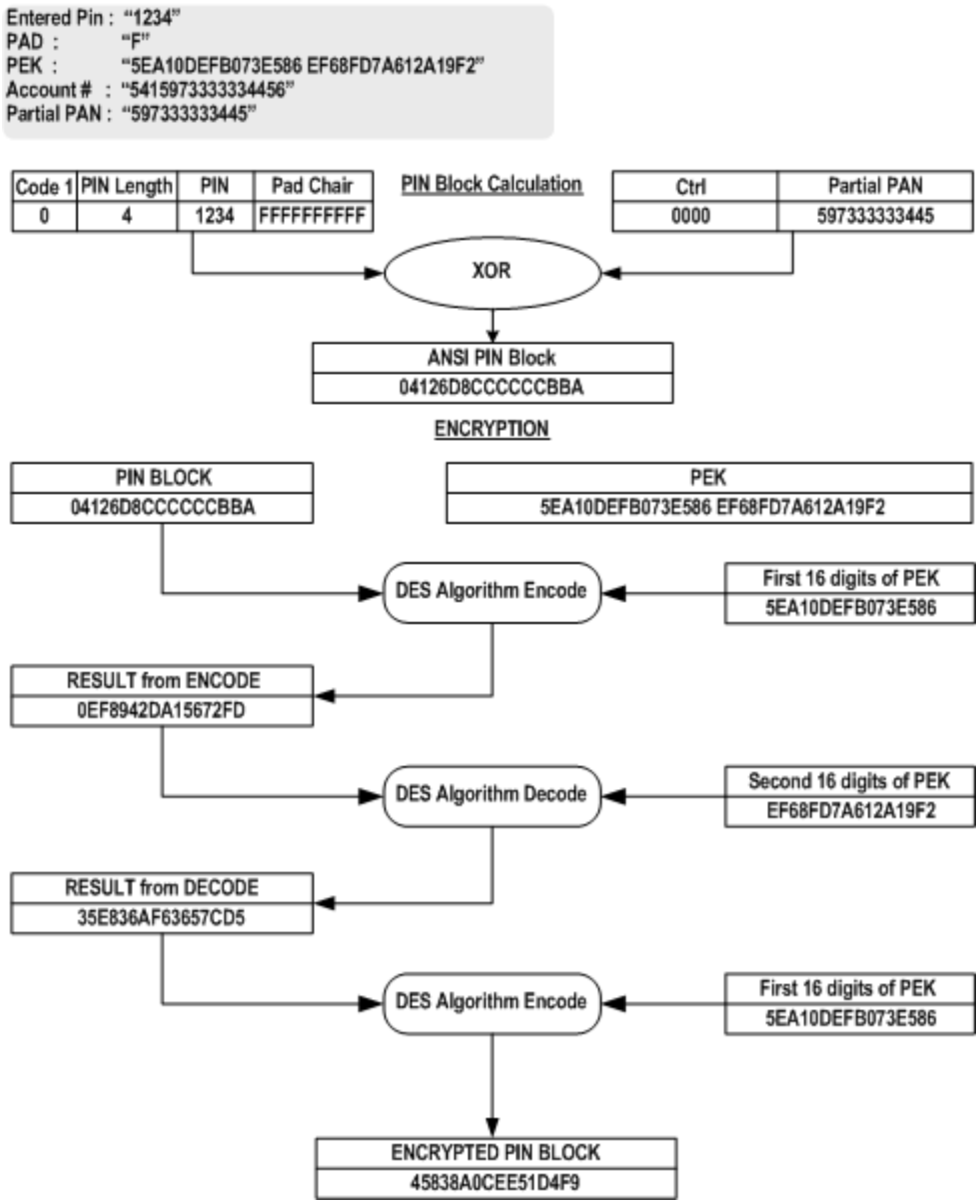
Within the Authorization Platform environment, security includes ensuring message security and integrity as well as protection against cardholder PIN disclosure. Mastercard uses secure PIN encryption in the Authorization Platform to protect all PINs.

Encryption

The approach that the Authorization Platform uses for network security management is PIN encryption using data encryption standard (DES). Customers must use Triple DES. The acquirer must send the entered PIN to the Single Message System, encrypted in an ANSI block format, as illustrated in the ANSI PIN Block Format diagram.

For more information about PIN encryption, refer to the *Single Message System Specifications* manual.

ANSI PIN Block Format



Security

Security using DES depends on the secrecy of the keys used, and therefore on the management of the keys, as illustrated in the Zone Key Management diagram. The Authorization Platform implements the zone approach rather than the end-to-end approach to key management.

The following table describes the difference between the two types of key management.

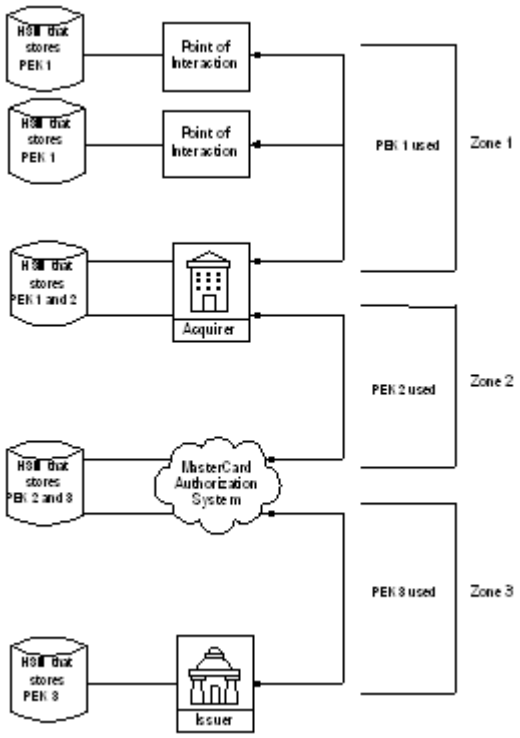
Zone	End-to-End
Encryption of data between zones using a PEK unique to the Authorization Platform/customer pair. Data that must be transmitted through several zones is decrypted and re-encrypted at each entity. For dynamic PEK exchanges, the Authorization Platform/customer pair must also maintain a unique KEK.	Encryption of data between its origination point and final destination using a key unique to the end-to-end pair. Data is encrypted at the source and not decrypted until reaching the final destination. Each point of origin must maintain a unique key for each final destination to which it transmits, and each final destination must maintain a unique key for each point of entry from which it can receive.

Mastercard chose the zone approach instead of the end-to-end approach for the following reasons:

- Key exchange is required only between issuers and acquirers connected to the Authorization Platform.
- The approach does not require loading keys to the terminal for every card that processes Mastercard purchase transactions containing a PIN.

For Mastercard purchase transactions that contain a PIN, all PINs must be encrypted at the point of entry (the terminal). The PIN remains encrypted until the issuer receives it for verification. It is translated from one zone's PEK to another zone's PEK as it is passed from one customer to another through the Authorization Platform. When the customer passes the PIN to the Authorization Platform, the Authorization Platform translates it using the ANSI PIN block format. The ANSI PIN block is the only format that the Authorization Platform supports.

Zone Key Management



Establishing PEKs

The Authorization Platform shares a PEK with each customer during PIN transaction processing. The Authorization Platform and customer use ANSI PIN block formatting for encryption and decryption.

The customer may use the same or a separate PEK for issuing and acquiring transactions.

PEK Storage

Customers are responsible for safely storing their PEKs by encrypting them under a proprietary Master File Key using hardware security procedures. Customers must store PEKs within a Tamper Resistant Security Module (TRSM).

PEK Implementation

When new PEKs are created, the customer has five minutes to implement the new PEK. During that period, the Authorization Platform attempts decryption using the previous PEK in the event that the new PEK is in error.

PEK Exchange Methods

The Authorization Platform and customers exchange PEKs in two manners: statically and dynamically. Acquirers and issuers connected to the Mastercard Network that are processing

Mastercard purchase transactions that contain a PIN may use either static or dynamic key encryption to translate the PIN in DE 52.

NOTE: For increased security, Mastercard strongly recommends using dynamic PEKs.

Static PEK

The Authorization Platform and the customer do not exchange the static PEK online; they create it through a manual (offline) process. Customers must use the *Customer Initiated Key Part Exchange Form* (Form 536) to create the static PEK with Mastercard. The Mastercard and Customer Key Officers[2] must adhere to the strict procedure described in the *Single Message System Specifications* manual to establish the static PEK.

Dynamic PEK

The Authorization Platform randomly generates dynamic PEKs for each customer. Only the Authorization Platform can send a new dynamic PEK; however, a customer may request a new PEK at any time.

The Authorization Platform will create a new dynamic PEK automatically online every 24 hours or every 2,500 transactions, whichever occurs first. It will also create a new dynamic PEK after five consecutive Sanity Check errors.

Establishing KEKs

The Authorization Platform sends new dynamic PEKs online using Network Management (08xx) messages. The customer must establish the Key Exchange Key (KEK) with the Authorization Platform before exchanging dynamic PEKs.

The Authorization Platform and the customer use a shared KEK to encrypt and decrypt each PEK. The Authorization Platform and each customer are jointly responsible for generating the unique KEKs used to exchange and encrypt PEKs.

Customers must use the *Customer Initiated Key Part Exchange Form* (Form 536) to create the KEK with Mastercard. The Mastercard and Customer Key Officers[1] must adhere to the strict procedure described in the *Single Message System Specifications* manual to establish the KEK.

The Authorization Platform uses the following process to create and communicate dynamic PEKs:

1. The Authorization Platform uses the KEK to encrypt the new PEK and check value.
2. The Authorization Platform sends the new PEK to the issuer in an online Network Management Request (PEK Exchange)/0800 message.
3. The customer validates the check value and loads the new PEK.
4. The customer uses the check values to ensure that the Authorization Platform generated the new PEK from the same unique KEK established between the customer and the Authorization Platform.

[2] Mastercard recommends that Customer Key Officers not have extensive technical backgrounds.

Sanity Check Errors

The Authorization Platform changes the PEK after five consecutive Sanity Check errors. Sanity Check errors are those that the PSD detects as possible PEK corruption by verifying that the cleartext PIN block is in the expected format.

Master Key File

Mastercard recommends that each customer establish a Master File Key (MFK) to encrypt PEKs and KEKs for secure storage on a database. MFKs work in a similar manner to PEKs and KEKs in that they are comprised of key parts. Each customer is responsible to generate and securely maintain its proprietary MFK.

PIN Verification

Mastercard provides a PIN verification service for all purchase transactions that contain a PIN. There are two PIN verification methods to choose from: DES/IBM 3624 or ABA.

The PIN verification service is an optional service.

NOTE: Track data must be present for Mastercard to perform PIN verification because the Authorization Platform must have a means to obtain offset data from the issuer.

If the issuer chooses to have the Authorization Platform perform PIN verification, it must provide PIN processing parameters to Mastercard. These parameters determine placement of PIN verification track data.

If the issuer currently uses the PIN Verification Service that the Single Message System provides for ATM transactions, the issuer may choose to have the Authorization Platform perform PIN verification on all PIN-based purchase activity using the same parameters. Issuers that choose to use the PIN Verification service must use the *PIN Processing Profile Form* (Form 269) to provide their PIN processing Parameters to Mastercard.

PIN Verification in Stand-In Processing

Mastercard provides a PIN verification service for transactions processed by Stand-In processing that contain unverified PIN data in Authorization Request/0100 messages. There are two PIN verification methods to choose from: DES/IBM 3624 or ABA.

The Stand-In System will not perform the PIN Verification Test, unless issuers participate in a PIN validation service. If no PIN validation is performed on a transaction, the Stand-In System will bypass the PIN Verification Test and proceed to the next sequential Stand-In Test.

Issuers that want Mastercard to perform the optional PIN Verification on transactions processed by the Stand-In System must participate in a PIN Pre-validation or PIN Validation in Stand-In service.

Issuers that want Mastercard to verify the PIN provided in DE 52 (Personal ID Number [PIN] Data) on transactions processed by Stand-In processing must provide PIN processing parameters to Mastercard.

WHEN the PIN data is…	THEN Stand-In processing…
Valid	Proceeds to the next appropriate Stand-In processing test.
Invalid	Sends a response of decline in the Authorization Request Response/0110 message to the acquirer.

Mastercard uses DE 48, subelement 80 (PIN Service Code) and DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code) in the Authorization Advice/0120 message to communicate the results of the PIN verification test to the issuer.

WHEN…	THEN DE 48, subelement 80 contains…	AND DE 60, subfield 2 contains…
The PIN is valid	PV (the Authorization Platform verified the PIN)	Not applicable
The PIN is invalid	PI (the Authorization Platform was unable to verify the PIN)	0004 (Reject: Invalid PIN)
The Authorization Platform is unable to perform PIN verification	PI (the Authorization Platform was unable to verify the PIN)	0030 (Reject: Unable to verify PIN data)

Issuers that want to use the PIN Verification in Stand-In Processing service can request this service by completing the *PIN Processing Profile Form* (Form 269) and by sending the PIN verification keys using the *Hard Copy Key Exchange Form* (Form 723).

Mastercard will perform the PIN Verification in Stand-In service using track data provided in the message, unless the issuer has chosen to participate in the PIN Verification Value (PVV) on File Service. For more information about the PVV service, refer to the *Debit Mastercard for the Single Message System Guide*.

Authorization Report

The Authorization Parameter Summary Report (SI737010-AA) includes a Stand-In PIN Verification Bypass indicator that identifies whether the Stand-In System will bypass the PIN Verification Test or perform the PIN Verification Test.

This indicator will be present on the report for all customers, not just those customers that elect to participate in a PIN validation service.

Portfolio Sales Support

Mastercard offers support for customers when they buy or sell a portfolio.

	Service Available for	
Service	**Full BIN Transfer**	**Partial BIN Transfer**
Transfer of BINs from one customer to another. After Mastercard transfers the BIN, the Authorization Platform processes all transactions within the BIN under the new ICA.	√	√
Transfer of AMS account listings from one customer to another. After Mastercard transfers the listings, the new ICA maintains the listings.	√	

Full BIN Transfer

To transfer an entire BIN from one ICA number to another, contact the Global Customer Service team and request support for a portfolio transfer.

You will need to provide the following information:

- Old ICA number
- New ICA number
- Time and date on which the transfer will be effective
- BIN that you are buying or selling

Automatic AMS Transfer

If you are requesting an automatic AMS transfer as part of the BIN transfer, complete section "e" of the Member Conversion Questionnaire. The Global Customer Service team will provide the questionnaire.

For examples of the automatic transfer of AMS accounts and for billing information for that service, refer to the *Account Management System User Manual*.

The following table shows the transfer of BINs and AMS accounts.

When it Occurs	Description
Before the planned transfer date	The customer (new ICA number or old ICA number) requests support for a portfolio transfer.
At the time and date when the transfer is effective	The Authorization Platform moves authorization processing from the old ICA to the new ICA.

When it Occurs	Description
On the transfer effective date, after the authorization processing transfer	Mastercard automatically transfers the ownership of the AMS accounts from the old ICA to the new ICA.
On the evening of the transfer effective date	The Daily Account File Activity Report for the new ICA shows the account listings under the new ICA.

Partial BIN Transfer

To transfer a part of a BIN from one customer to another, notify the Global Customer Service team in writing.

You will need to provide the following information:

- Old ICA number
- New ICA number
- Time and date on which the transfer will be effective
- Which portion of the BIN requires the new routing

Transfer Process for a Partial BIN

The following table shows the transfer process for a partial transfer of a BIN.

When it Occurs	Description
Before the planned transfer date	The customer (new ICA or old ICA) requests support for the transfer.
At the time and date when the transfer is effective	• The Authorization Platform routes authorization requests for the transferred part of the BIN to the new endpoint. • The Stand-In parameters of the new ICA number and BIN govern processing for the transferred part of the BIN. • Mastercard bills all issuing authorization charges to the new ICA number. • The new ICA number can add accounts within the BIN to AMS and to the Account File.

Fees

Fees apply to portfolio sales services are listed in table format.

Service	Fee
Full BIN—Authorization Processing	Flat fee, billed to the requesting customer.
Full BIN—AMS account transfer	• Flat fee, billed at ICA number/BIN level • Per-account fee, billed at the account level for each account transfer
Partial BIN—Authorization Processing	Flat fee per portfolio and BIN, billed to the requesting customer

The customers involved in the portfolio sale may decide which of them will receive the charges for the Full BIN—AMS account transfer fees. Mastercard can bill one customer for both fees, or Mastercard can bill one customer for the flat fee and another customer for the per-account fee.

Private Label Transaction Processing

The Mastercard Private Label Program leverages the existing Mastercard payment system infrastructure to provide efficient authorization, clearing, and settlement services for private label card transactions, in addition to value-added products and services that issuers may use in conjunction with their private label programs.

Mastercard has extensive network reach, acceptance, and standardized formats that provide issuers with a robust network processing solution for private label card transactions, thereby addressing the infrastructure limitations of a closed-loop processing model.

In addition to providing a superior private label transaction processing solution, the Mastercard Private Label Program provides issuers with the ability to use many of the world-class, value-added services offered by Mastercard. Issuers may optionally benefit from the array of Mastercard risk management solutions, enhanced transaction processing services, and portfolio performance management expertise to facilitate financial improvement of their portfolios.

In conjunction with the Private Label Program, issuers can use the Activation and Initial Load of Private Label Prepaid Card service, which is provided exclusively for transactions originating from the approved private label card portfolios of Mastercard issuers.

Private Label Processing

Under the Mastercard Private Label Program, private label issuers may use Mastercard account ranges (account range either within 510000–559999 or 222100–272099) or a reserved Maestro range. 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).

Activation and Initial Load of Private Label Prepaid Cards

The Authorization Platform supports card activation or deactivation requests between acquirers and private label issuers in the Europe region.

NOTE: Applies only to the Europe region for private label card programs.

Benefits

The benefits of providing private label issuers with the ability to allow their cardholders to activate and to set the amount to load on their private label prepaid cards at the moment of purchase and activation at the POS terminal are as follows:

- Allows merchants to:
  - Activate prepaid cards over the Authorization Platform as cards are being sold
  - Provide refunds to consumers with a private label prepaid card (typically a gift card) loaded with the full amount of the refund, rather than giving cash that could be spent at another merchant location.
- Allows issuers to keep prepaid accounts inactive until an activation request is received from the merchant and to help reduce fraud by enabling the activation of prepaid cards with or without a predefined amount.
- Provides a security measure to ensure that prepaid cards cannot be used before activation.

Transaction Type Identifier C09

The Authorization Platform supports Transaction Type Identifier value C09 (Card Activation) to specify private label prepaid card activation and initial load requests.

Authorization Processing

For private label prepaid cards, the Authorization Platform processes one transaction for both activating and initially loading a card. The activation request uses an Authorization Request/0100 message with a Payment Type processing code and a valid amount in DE 4 (Amount, Transaction) for private label prepaid card activation authorization messages. The activation also can be canceled by a Reversal Request/0400 message.

Based on the issuer's private label prepaid card program, the private label prepaid cards can be magnetic stripe or chip and may or may not require the entry of a PIN.

Stages for prepaid card activation at the POS terminal:

1. The cardholder purchases a private label prepaid card and requests to have it activated at the POS terminal.
2. The merchant enters a request to activate a private label prepaid card from the POS terminal.
3. The POS terminal sends an Authorization Request/0100 message to the acquirer.
4. The acquirer forwards the Authorization Request/0100 message via the Mastercard Network to the issuer for a private label prepaid card activation request.

5. The issuer validates the request and sends an approval in an Authorization Request Response/0110 message via the Mastercard Network to the acquirer. Mastercard suggests private label issuers approve card activation transactions using response code 00 (Approved or completed successfully).
6. The acquirer delivers the response to the POS terminal.
7. The issuer activates the private label prepaid card on its system.

Acquirers supporting the private label prepaid card activation request message must be able to send a Reversal Request/0400 message to deactivate the card if they are not able to deliver the Authorization Request Response/0110 message to the merchant's terminal or time-out waiting for a response from the Authorization Platform.

Private label issuers may want to define policies and rules with their merchants for governing exceptions that may occur during the activation process, such as what actions to take if there is a decline response.

Alternate Processing

Private label prepaid card activation plus initial load 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 message is returned to the acquirer with DE 39 (Response Code), value 91 (Authorization System or issuer system inoperative).

For More Information

For more information about Private Label programs.

- Supporting data requirements, refer to the *Customer Interface Specification* manual.
- Global Clearing Management System (GCMS) processing of private label transaction processing, refer to the *GCMS Reference Manual*.

Private Label Non-Financial Service

The Private Label Non-Financial Service leverages the capabilities of the Mastercard Network in combination with the Mastercard Private Label Program to offer a non-financial service using the Authorization Platform.

The Private Label Non-Financial Service provides purchase point-of-sale (POS) information to manufacturers of luxury goods for use in various applications, such as warranty registration or inventory forecasting.

Authorization Processing

The Authorization Request/0100 message that is triggered by this event includes all mandatory data elements needed to carry the product information. The Authorization Request/0100 message, capturing the purchase POS information, is initiated for purchased goods of participating merchants regardless of what form of payment was used to purchase the goods.

Product code PVA (Private Label A) is used for identification of POS information from luxury goods transactions. Product code PVA is set up in account ranges for authorization processing only. Any clearing messages received with product code PVA will be rejected.

Alternate Processing

The Authorization Request/0100 message containing value PVA in DE 63 (Network Data), subfield 1 (Financial Network Code) is routed to and declined by Stand-In processing with a response code of 05 (Do Not Honor) in DE 39 (Response Code). The X-Code System also responds with value 05 in the event that authorization cannot be obtained from Stand-In processing.

For More Information

For more information about the Mastercard Private Label Non-Financial Service, contact the Global Customer Service team.

Promotion Code

The promotion code is an alphanumeric code that customers can include in the Authorization Request/0100 message.

The promotion code service is an optional service.

About Promotion Codes

Issuers may decide to offer a promotion to merchants. This promotion may require issuers to use different authorization criteria than they do with most transactions. The promotion code allows the issuer to recognize that this transaction uses the different criteria to determine authorization responses for transactions that occur at the participating merchants.

Mastercard may also specify other uses of the promotion code. When Mastercard specifies these other uses, the *Customer Interface Specification* manual provides details about them.

How It Works

1. The merchant includes the promotion code when it sends transaction data to the acquirer.
2. The acquirer sends the promotion code in DE 48 (Additional Data—Private Use) of the Authorization Request/0100 message to the issuer for the authorization decision.
3. The issuer can use the promotion code to identify transactions that occur at a merchant that participates in that issuer's promotion program.

For details about data requirements, refer to the *Customer Interface Specification* manual.

To Participate

To participate in the Promotion Code service, issuers must notify Mastercard to participate in this service. To participate, contact the Global Customer Service team.

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.

Purchase of Goods or Services with Cash Back Transactions

Mastercard supports Purchase of Goods or Services with Cash Back transactions for Debit Mastercard® and Maestro® cards. This feature allows acquirers and issuers to globally process Debit Mastercard non-ATM purchase with cash back transactions through their Mastercard Network connection. This feature also allows Europe region acquirers and issuers to additionally process Maestro non-ATM purchase with cash back transactions through their Mastercard Network connection.

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. This service is active for all Debit Mastercard and Maestro account ranges.

Issuers can approve or decline Purchase of Goods or Services with Cash Back transactions at their discretion.

Purchase Amount Only Approval Response Code

DE 39 (Response Code), value 87 (Purchase amount only, no cash back allowed) provides issuers the option of approving the purchase amount of the transaction but not the cash back amount on purchase with cash back transactions.

The Authorization Platform allows acquirers to indicate whether the merchant terminal supports receipt of the new purchase amount only approval response code in an authorization message.

DE 39, value 87 only is applicable to purchase of goods or services with cash back transactions.

The Authorization Request/0100 message must contain:

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code), value 09 (Purchase with Cash Back)

- 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).

DE 39, value 87 is an approval code, and applicable in the following messages:

- Authorization Request Response/0110
- Authorization Advice/0120—Issuer-generated
- Reversal Request/0400
- Reversal Advice/0420

Alternate Processing

Issuers have the option to choose whether Purchase with Cash Back (PWCB) transactions are eligible for processing by the Stand-In System. An issuer may choose to allow PWCB for only PIN–based transactions, only Signature-based transactions, or allow both PIN and signature-based transactions be processed by the Stand-In System.

If the issuer identifies that PIN, signature, or both PWCB transactions are not allowed to be processed by the Stand-In System, the Authorization Platform declines the transaction using Authorization Request Response/0110 message containing DE 39 (Response Code), value 91 (Authorization System or Issuer system inoperative).

If the issuer allows Stand-In processing of PIN-based PWCB transactions, DE 52 (Personal ID Number [PIN] Data) must be present in the Authorization Request/0100 message. If DE 52 is not present in the authorization request message, the transaction will be categorized as a signature-based transaction and processed based on whether the issuer allows signature-based PWCB transactions to be processed by the Stand-In System.

Stand-In processing refers to the issuer's Decision Matrix to determine the authorization response. If an acquirer can process a purchase amount only response, Stand-In processing may provide an Authorization Request Response/0110 message containing DE 39 (Response Code), value 87 (Amount Only, No Cash Back Allowed) when the purchase portion of the PWCB transaction passes a given limit test and the cash portion fails.

Purchase with Cash Back transactions are not eligible for X-Code processing. If the transaction cannot be processed by the issuer or the Stand-In System, the Authorization Platform provides the acquirer an Authorization Request Response/0110 message containing DE 39 (Response Code), value 91 (Authorization System or Issuer system inoperative).

Reversals of Purchase of Goods or Services with Cash Back Transactions

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 transaction. 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 will apply an edit to the Reversal Request/0400 message 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).

When 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 a value of 87, Mastercard recommends that the acquirer not send DE 54 in the reversal message. If the acquirer intends the 0400 message as a partial reversal, DE 95 (Replacement Amount) 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.

NOTE: Merchants in the U.S. region may charge a fee on the cash back portion of a purchase with cash back transaction.

India Intracountry Cash Back Transactions

Mastercard supports India intracountry Cash Back transactions (that is, Cash Back without Purchase and Purchase with Cash Back) at the point of sale (POS) conducted with Debit Mastercard and Maestro cards. This functionality eliminates the need for acquirers to manage Cash Back processing at the BIN level on their host systems.

Cash Back without Purchase and Purchase with Cash Back for Debit Mastercard and Maestro transactions acquired in India are valid only for India domestic cardholders (that is, cardholders with accounts issued outside of India will be rejected if they request a cash back transaction).

South Africa Intracountry Cash Back Transactions

Mastercard supports intracountry Debit Mastercard® purchase with cash back transactions conducted with or without an accompanying purchase at South African merchant locations.

PIN verification is required for all Debit Mastercard purchase with cash back transactions conducted without an accompanying purchase.

Customers that want to implement purchase with cash back transactions conducted with or without an accompanying purchase for South Africa should contact the Global Customer Service team for guidance and support on the implementation requirements.

For More Information

For details about data requirements, see the *Customer Interface Specification* manual.

QR Code Payments

The quick response (QR) code payment is a fast, convenient payment option for consumers. These transactions may originate when either (a) a consumer mobile wallet generates a QR code that can be scanned by a merchant to receive payments or (b) a merchant generates QR code that can be scanned by a consumer's mobile device to complete payments.

Consumer Presented QR Transactions

Consumer Presented QR transactions originate when a consumer mobile wallet generates a quick response (QR) code that can be scanned by a merchant to receive payments.

NOTE: Effective 11 June 2019, Mastercard is implementing enhancements (in accordance with the EMVCo specifications for Consumer Presented QR codes) to allow customers to properly identify and process tokenized Mastercard Consumer Presented QR transactions received on the Mastercard Network.

Effective 11 June 2019, Mastercard will identify:

- Mastercard Consumer Presented QR transactions by the use of value 03 (PAN auto-entry via barcode reader) in DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)
- Mastercard Consumer Presented QR terminal capabilities through new subfield 02 (Additional Terminal Capability Indicator) in DE 48 (Additional Data—Private Use), subelement 21 (Acceptance Data)

These enhancements will help ensure that tokenized Mastercard Consumer Presented QR transactions are properly identified and securely processed on the Mastercard Network.

To Participate

To submit or process tokenized Mastercard Consumer Presented QR transactions, acquirers and issuers must contact their CIS or account representatives.

Merchant Presented QR Transactions

Mastercard® Merchant Presented QR™ transactions are consumer-initiated, push Payment Transactions with a mobile payment device through a low-cost, point-of-interaction device.

Using a mobile payment device, the consumer makes a cashless payment by scanning a quick response (QR) code at any location that accepts Mastercard Merchant Presented QR transactions. This product fulfills the need to make payments to merchants in a direct, convenient, and secure method for both the merchant and consumer.

This program extends payment services to merchants currently excluded from electronic payments and is similar to a cash experience with funds immediately available to the merchant. Merchant Presented QR provides a viable, cost-effective alternative to merchants who are cash focused, but would like an electronic option.

Merchant Presented QR operates in an alternate four-party business model which enables funds to be transferred from a licensed Mastercard Customer acting as a originating institution (OI), to a licensed Mastercard Customer acting as a receiving institution (RI). The transaction originates at the OI/consumer bank or third party wallet providers and routes to the merchant after successfully authenticating and authorizing the debit from the consumer's account. The RI will credit the merchant account upon authorization and notify the merchant that the payment has been successfully received.

The QR code based program is a Payment Transaction, the transfer of funds from a Mastercard Account or Maestro Account to a Mastercard Receiving Account using the Mastercard Network Payment Transaction, defined on the Dual Message System (Authorization) by using:

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) value 28 (Payment Transaction)
- A unique Payment Transaction type indicator DE 48 (Additional Data—Private Use), Transaction Category Code (TCC)=P (Payment Transaction), subelement 77 (Funding Transaction or Payment Transaction Type Indicator), value of C67 (Merchant Presented QR) to support the payment to the merchant.

NOTE: The QR code will include the actual merchant MCC. The MCC is a mandatory field on the QR code. The OI must obtain the MCC from the merchant's QR code and include in the ISO message or the API.

If Merchant Presented QR Transactions are enabled through a third-party wallet provider, the financial institution supporting the wallet provider will secure funds from a consumer account by initiating a Funding Transaction prior to processing the Payment Transaction.

For more information, refer to the *Mastercard Merchant Presented QR Program Guide*.

To Participate

To submit or process Mastercard Merchant Presented QR transactions, OIs and RIs must complete and submit the *Registration for Mastercard Merchant Presented QR—Global* (Form 1274) to their regional account representative.

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 Flexible Spending Account (FSA), Healthcare Reimbursement Arrangement (HRA), or Health Savings Accounts (HSA) cards when used at a merchant with a qualifying Inventory Information Approval System (IIAS).

NOTE: Applies only to the U.S. region.

Background

Internal Revenue Service Notice 2006-69 requires flexible spending account plan administrators to block card transactions occurring at non-medical MCCs (for example, grocery stores, discount stores, wholesale clubs), unless the merchant has implemented an Inventory Information Approval System (IIAS).

If FSA/HRA/HSA plan administrators allowed a transaction to be approved that contained non-verified and non-eligible merchandise, they run the risk of having their entire plan disqualified by the IRS. Beginning January 2008 all grocery stores, discount stores, and online pharmacies that accept FSA debit cards must reference an IIAS at the point of sale.

Internal Revenue Service Notice 2006-69 also requires strict recordkeeping of IIAS-processed transactions. Health plan sponsors and administrators must negotiate agreements with merchants for the merchant to maintain the transaction amount, date the expense was incurred, and nature of the expense, and make this information accessible upon request, or alternatively send the information to the employer, administrator, or other applicable entity.

Affected acquirers are responsible for determining which merchants are IIAS-compliant, as defined by SIGIS.

Merchant Validation for Real-time Substantiated Transactions

The Authorization Platform performs a real-time authorization check to ensure that an Authorization Request/0100 message is from an IIAS-compliant merchant.

The Authorization Platform identifies whether a transaction submitted as real-time substantiated is coming from a SIGIS (Special Interest Group for IIAS Standards)-compliant merchant. The Internal Revenue Service (IRS) placed additional requirements on merchants that do not use a healthcare card acceptor business code (MCC) to accept healthcare cards requiring transaction substantiation.

IIAS-Compliant Merchants

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, subfield 61 position 3 contains value 1).

To obtain Mastercard Assigned IDs for IIAS merchant validation, acquirers should send an email message to sigis_merchant_setup@Mastercard.com. The request should specify if it is an addition or update of the Mastercard Assigned ID, and at a minimum include the acquirer name, telephone number, email 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 SIGIS compliant.

Non-IIAS Compliant Merchants

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 define DE 48, subelement 61 (POS Data, Extended Condition Codes), subfield 3 (Real-time Substantiation Indicator) as value 4 (Transaction was submitted as real-time substantiated but from a non-IIAS certified merchant).

If the issuer is not participating in real-time substantiation, the original value of 1 (Merchant terminal verified the purchased items against the IIAS) is changed to value 0 (Merchant terminal did not verify the purchased items against the IIAS).

90% Rule Merchant Exemption

If the merchant generated 90 percent of its total sales from FSA/HSA/HRA-certified healthcare products in the previous fiscal year, that merchant is exempt from IIAS rules.

To indicate that the merchant is exempt from the IIAS rule based on the 90% rule, the acquirer must provide DE 48, subelement 61, subfield 3, value 2 (Merchant claims exemption from using an IIAS based on the IRS 90 percent rule) in Authorization Request/0100, Authorization Advice/0120, and Reversal Request/0400 messages.

Merchant Terminal Verification

Mastercard defines DE 48 (Additional Data—Private Use), subelement 61 (POS Data, Extended Condition Codes), subfield 3 (Real-time Substantiation Indicator) for use in the Authorization Request/0100 message to allow merchants to indicate whether the merchant terminal verified the purchased items against an IIAS.

For accurate processing of IIAS real-time substantiated transactions, Mastercard recommends that issuers validate the card acceptor business code (MCC) (DE 18) and Real-time Substantiation Indicator (DE 48, subelement 61, subfield 3).

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
- Subfields 4 and 5 are reserved for future use and must contain values of zero

Acquirers do 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 supports the processing of Real-time Substantiation transactions with an indicator to specify healthcare transactions with the healthcare amount type values 10 (Healthcare Eligibility Amount), 11 (Prescription Eligibility Amount), and 12 (Vision Rx Eligibility Amount) in DE 54 (Additional Amounts), subfield 2 (Amount Type).

Healthcare Eligibility Amount

When the acquirer provides the real-time substantiation indicator in DE 48 (Additional Data—Private Use), subelement 61 (POS Data Extended Condition Codes), subfield 3 (Real-time Substantiation Indicator), amount type 10 (Healthcare Eligibility Amount) allows the acquirer to indicate the portion of DE 4 (Amount, Transaction) that is eligible for real-time substantiation.

Prescription Eligibility Amount

In addition to the Healthcare Eligibility Amount, Mastercard supports DE 54, subfield 2, value 11 (Prescription Eligibility Amount), which allows the acquirer to indicate the portion of the healthcare eligibility amount that includes the amount spent for prescriptions.

Subfield 2, value 11 must only be present when the acquirer provides subfield 2, value 10 in the Authorization Request/0100 or the Authorization Advice/0120 message. In addition, the amount in subfield 2, value 11 must be less than or equal to the amount of subfield 2, value 10.

DE 54 occurrences with subfield 2, values 10 and 11 are not returned to the acquirer in the Authorization Request Response/0110 message or the Authorization Advice Response/0130 message.

Vision Rx Eligibility Amount (for U.S. Region Healthcare Customers Only)

Effective with Release 19.Q1, U.S. region healthcare customers may use value 12 (Vision Rx Eligibility Amount) to indicate the portion of the transaction amount that is spent for vision prescriptions (Rx).

DE 54, subfield 2, value 12 can be provided by itself in the Authorization Request/0100 or the Authorization Advice/0120 messages or in combination with value 10 or values 10 and 11.

Examples

Examples of Real-time Substantiation transaction processing are listed in table format.

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**
• DE 48, subelement 61 = 10100 (indicates terminal can handle partial approvals and has verified against IIAS) • DE 4 = USD 100 • DE 54, subfield 2, value 10 = USD 40	• DE 6 = USD 40 • DE 39 = 10	• DE 4 = USD 40 • DE 54, subfield 2, value 57 (Original Amount) = USD 100 • DE 39 = 10

Example 2—Partial Approval: Partial Healthcare Eligibility Amount

This example illustrates that the issuer approved only a portion of the Healthcare Eligibility Amount, which in this case is a partial approval of the total transaction amount. In this scenario, the merchant would ask the cardholder to use another form of payment for the remaining USD 80 or remove some items from the purchase.

Authorization Request/0100	Authorization Request Response/0110	
	From Issuer	**To Acquirer**

Authorization Request/0100	Authorization Request Response/0110	
• DE 48, subelement 61 = 10100 • DE 4 = USD 100 • DE 54, subfield 2, value 10 = USD 40	• DE 6 = USD 20 • DE 39 = 10	• DE 4 = USD 20 • DE 54, subfield 2, value 57 = USD 100 • DE 39 = 10

Example 3—Full Approval: Entire Healthcare Eligibility Amount

In this example, the merchant terminal is indicating that they do not support partial approvals; therefore, a full approval or decline is required. The issuer approves the full transaction; thereby approving the entire Healthcare Eligibility Amount.

Authorization Request/0100	Authorization Request Response/0110	
	From Issuer	**To Acquirer**
• DE 48, subelement 61 = 00100 • DE 4 = USD 100 • DE 54, subfield 2, value 10 = USD 100	• DE 4 = USD 100 • DE 39 = 00	• DE 4 = USD 100 • DE 39 = 00 No DE 54, subfield 2, value 57 (Original Amount) is provided in this scenario because the issuer responded with DE 39 = 00

Example 4—Partial Approval: Partial Healthcare Eligibility Amount, including Prescriptions

This example illustrates that the issuer approved only a portion of the Healthcare and Prescription Eligibility amounts. In this scenario, the merchant would ask the cardholder use another form of payment for the remaining USD 80 or remove some items from the purchase.

Authorization Request/0100	Authorization Request Response/0110	
	From Issuer	**To Acquirer**

Authorization Request/0100	Authorization Request Response/0110	
• DE 48, subelement 61 = 10100 • DE 4 = USD 100 • DE 54, subfield 2, value 10 = USD 40 • DE 54, subfield 2, value 11 = USD 30	• DE 6 = USD 20 • DE 39 = 10	• DE 4 = USD 20 • DE 54, subfield 2, value 57 = USD 100 • DE 39 = 10

Example 5—Full Approval: Entire Healthcare Eligibility Amount, including Prescriptions

In this example, the merchant terminal is indicating that they do not support partial approvals; therefore, a full approval or decline is required. The issuer approves the full transaction; thereby approving the entire Healthcare Eligibility Amount, including the Prescription Eligibility Amount.

Authorization Request/0100	Authorization Request Response/0110	
	From Issuer	To Acquirer
• DE 48, subelement 61 = 00100 • DE 4 = USD 100 • DE 54, subfield 2, value 10 = USD 100 • DE 54, subfield 2, value 11 = USD 60	• DE 4 = USD 100 • DE 39 = 00	• DE 4 = USD 100 • DE 39 = 00 No DE 54, subfield 2, value 57 (Original Amount) is provided in this scenario since the issuer responded with DE 39=00

Authorization Reports

The Authorization Parameter Summary Report (SI737010-AA) includes a Real-time Substantiation participant parameter in the Global Parameters section.

For a sample of this report and field descriptions, refer to Reports.

To Participate

Issuers must notify Mastercard if they want to support real-time substantiation processing by completing the *Real-time Substantiation Participation* (Form 834) and providing the form to the Global Customer Service team.

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 removes healthcare related amounts from the Authorization Request/0100 or the Authorization Advice/0120 message for non–participating issuers.

For More Information

For details about data requirements, see the *Customer Interface Specification* manual.

Recurring Payments

Recurring payments are applicable to the following systems:

- Dual Message System - Acquirers
- Dual Message System - Issuers
- Product: Credit, Prepaid and Mastercard Debit®

Mastercard® currently supports recurring payment functionality and for that has defined additional message elements to allow more recurring payment information to be communicated between the acquirer and the issuer.

Definition

Recurring payments are payments by an issuer to an acquirer on behalf of a cardholder who authorizes a merchant to bill the cardholder's account on a continued, periodic basis (such as monthly, quarterly, or annually) without a specified end date. The amount of each payment may be the same or may fluctuate.

Typical recurring payment merchants include, but are not limited to:

- Newspaper and magazine subscriptions
- Insurance Companies
- Utilities
- Internet Service Providers
- Club memberships
- Charities

In Dual Message System processed transactions, all recurring payment transactions should have first an Authorization request and then for those approved ones submit a first presentment.

Indicating a Recurring Payment

Acquirers can indicate to issuers that a transaction is a recurring payment by including a value of 4 (Standing order/recurring transactions) in DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence) in Authorization Request/0100 messages.

NOTE: The recurring payment indicator in DE 61, subfield 4 is required for all subsequent recurring payment transactions that follow the first payment made to the card acceptor pursuant to the recurring payment arrangement. The first transaction in a recurring payment arrangement must not include the recurring payment indicator.

For more information about recurring payments, refer to the "Merchant Advice Codes" section.

For more information about determining the status of the cardholder account, refer to the "Purchase Account Status Inquiry / Recurring Payment Account Status Inquiry" section.

Maestro Recurring Payments Program

The Maestro® Recurring Payments Program allows enrolled merchants to begin accepting Maestro cards for recurring payment electronic commerce (e-commerce) transactions. The initial transaction of a recurring payment arrangement may be completed face-to-face, with the subsequent transactions being submitted as standard non–face-to-face recurring payment transactions.

Maestro recurring payment e-commerce transactions are identified in Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, and Reversal Request/0400—Acquirer-generated 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 AAV). In addition, DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence), value 4 (Standing order/recurring transactions) identifies Maestro e-commerce recurring payment transactions.

If the first transaction of a recurring payment arrangement is completed face-to-face, it must be identified as a face-to-face transaction and must not contain the recurring payment indicator in DE 61, subfield 4.

Issuers must not validate DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF™]), as that validation is performed during authorization processing.

DE 48, subelement 32 (Mastercard Assigned ID) must be present, and the Authorization Platform edits DE 48, subelement 32 and subelement 43 (Static AAV) for valid values.

Alternate Processing

The Mastercard® *Identity Check*™ AAV Verification Service and Mastercard® *Identity Check*™ AAV Verification in Stand-In Processing service will not be performed on Maestro e-commerce transactions that are processed under the Maestro Recurring Payments Program for e-commerce transactions.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Refund Transactions

A refund transaction allows a cardholder to return goods or services previously purchased from a merchant. The Authorization Platform accepts refund transactions for Mastercard and Maestro® transactions, in addition to Private Label transactions.

An acquirer sends an Authorization Request/0100 message with DE 3, subfield 1 containing value 20xx00 for the refund (where xx indicates the type of account to be credited). The issuer approves or declines the refund transaction using an Authorization Request Response/0110 message.

The refund Authorization Request/0100 message can be reversed using a Reversal Request/0400 message, if the merchant or cardholder decides not to complete the refund.

All refund transactions are routed to the same issuer host as for point-of-service (POS) transactions.

Refund transactions are not processed by the Stand-In System or X-Code alternate processing.

- If the issuer is not available to respond to a refund Authorization Request/0100 message, the Authorization Platform sends an Authorization Request Response/0110 message 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 refund Reversal Request/0400 message, the Authorization Platform sends a Reversal Request Response/0410 message to the acquirer with DE 39, value 00 (Approved or completed successfully). The Authorization Platform also sends a Reversal Advice/0420 message to the issuer as notification of the reversal that was responded to on their behalf.

Refund Transaction Support Requirements

Effective as of 18 October 2019 with Release 19.Q4, all Mastercard and Debit Mastercard issuers must be able to approve or decline refund transaction authorization request messages.

Effective as of 17 April 2020 with Release 20.Q2, all acquirers of Mastercard and Debit Mastercard transactions must be able to send refund transaction authorization request messages and forward the issuer's response to the merchant, for any merchant that chooses to initiate refund transaction authorization requests. Support of refund transaction authorization request messages is optional for merchants.

The Swedish Domestic Authorization Switching Service includes support of refund transactions.

For more information about refund transactions, refer to the Transaction Processing Rules.

Sweden Domestic Authorization Switching Service

The Authorization Platform supports the authorization processing for customers that participate in Sweden Domestic Authorization Switching Service (SASS).

NOTE: Applies only to the Europe region.

The Authorization Platform supports the following authorization processing for customers that participate in SASS:

- ATM Additional Data

- Forgotten Card at ATM
- Receipt Free Text
- Refund Transactions

ATM Additional Data

DE 48 (Additional Data—Private Use), subelement 58 (ATM Additional Data) may contain ATM watermark information. Watermark is a card authentication technology supported by Swedish ATMs. The watermark card verification method is used to increase security of the card; therefore, making counterfeit cards harder to manufacture. The watermark verification only applies when there is a watermark on the card.

The acquirer sends an ATM Authorization Request/0100 or a Reversal Request/0400 message with watermark data provided by the terminal. The issuer validates the watermark data and decides whether to approve or to decline the ATM transaction.

Watermark data can only be present in Authorization Request/0100 and Reversal Request/0400 messages for ATM withdrawal transactions (DE 3, subfield 1, value 01) or balance inquiry transactions (DE 3, subfield 1, value 30).

If the issuer does not support watermark data, the Authorization Platform removes subelement 58 (ATM Additional Data) before forwarding the Authorization Request/0100 message to the issuer.

Forgotten Card at ATM

Forgotten card at ATM covers two specific cases of when a cardholder initiates an ATM withdrawal or a balance inquiry service.

- The cardholder leaves the terminal without taking the card.
- The cardholder cannot retrieve the card from the terminal for technical reasons.

The card has been read by the terminal and an Authorization Request/0100 message has or has not been sent to the issuer. Either the terminal retains the card or the cardholder leaves his or her card in the terminal without bank notes being distributed.

If no Authorization Request/0100 message was sent for the ATM withdrawal or balance inquiry, the acquirer sends a Reversal Request/0400 message with a zero transaction amount and appropriate reason code in DE 48, subelement 58.

If the issuer does not support subelement 58, the Authorization Platform provides a Reversal Request Response/0410 message to the acquirer with DE 39 (Response Code), value 57 (Transaction not permitted to issuer/cardholder).

Receipt Free Text

Free text data allows issuers to provide acquirers information that can be printed on receipts at Swedish ATMs.

Issuers provide the free text data to be printed on ATM receipts in DE 123 (Receipt Free Text) of Authorization Request Response/0110 messages.

Receipt free text data can only be present in Authorization Request Response/0110 messages for ATM withdrawal (DE 3, subfield 1, value 01) and balance inquiry (DE 3, subfield 1, value 30) transactions.

If the acquirer does not support free text data, the Authorization Platform removes DE 123 (Receipt Free Text) before forwarding the Authorization Request Response/0110 message to the acquirer.

Refund Transaction Processing

Refund Transaction Processing

For information regarding refund transaction processing, refer to the Refund Transactions section in this chapter.

Third Party Processor Identification

The Third Party Processor (TPP) Identification service assists issuers in identifying an acquirer's third-party processor. This optional service provides issuers additional information in their fraud analysis during an account data compromise event.

Issuers that choose to register for this service will receive additional information to identify the entity involved in acquiring the transaction and presenting the transaction to the acquiring MIP.

How It Works

The Authorization Platform requires acquirers to submit DE 32 (Acquiring Institution ID Code) in all Authorization Request/0100 transactions. DE 32 contains the ICA number for the institution acting as the acquiring bank or merchant bank for the transaction. If an institution is acting as a processor for the acquiring bank, DE 32 should represent the acquiring bank and DE 33 (Forwarding Institution ID Code) should contain the ICA number for the forwarding or processing institution.

In addition to the values in DE 32 and DE 33 provided by the acquirer or processor in Authorization Request/0100 and Authorization Advice/0120 messages, the Authorization Platform includes the additional entity identifier submitting the message to the Dual Message System in DE 48 (Additional Data—Private Use), subelement 16 (Processor Pseudo ICA). DE 48, subelement 16 contains a unique identifier from the Mastercard Registration Program (MRP) database for the TPP processing the Authorization Request/0100 or Authorization Advice/0120 message.

This data is sent in the Authorization Request/0100 and Authorization Advice/0120 messages only for participating account ranges.

Authorization Reports

The Authorization Parameter Summary Report (SI737010-AA) includes a TTP participant parameter in the Global Parameters section to indicate issuers that have registered to receive unique identifiers for TTPs. For a sample of the Authorization Parameter Summary Report (SI737010-AA), refer to Reports.

To Participate

Issuers must register for this optional service. To request participation, contact the Global Customer Service team.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Transaction Integrity Classification

Mastercard offers the Transaction Integrity Classification to provide a mechanism to evaluate the safety and security of a transaction.

Overview

Mastercard provides the Transaction Integrity Classification for Point-of-Sale (POS) Purchase and Purchase with Cash Back transactions initiated on the dual message Authorization Platform destined for all U.S. issuers of Mastercard® credit and Debit Mastercard® cards.

Transaction Integrity Classification encompasses the fundamental safety and security of a transaction and includes the assessment of both the validity of the card and the cardholder. Some transactions are inherently more secure than others. For example, EMV chip cards are more secure than magnetic stripe cards. There are nuances across both the technology (card) and the Cardholder Verification Method (cardholder), but the combination is assessed across the spectrum to determine the overall integrity of each transaction.

NOTE: The Transaction Integrity Classification may be introduced in other issuing markets within later releases. Currently, all acquirers must be prepared to receive the Transaction Integrity Classification in response messages. The Transaction Integrity Classification is provided only in request messages sent to U.S. issuers.

How It Works

DE 48 (Additional Data—Private Use), new 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.

The Authorization Platform supports DE 48, subelement 52 in Authorization Request/0100 and Authorization Advice/0120—System-generated messages. The Transaction Integrity Class is provided for POS Purchase and Purchase with Cash Back transactions initiated on the

Authorization Platform destined for all issuers in the U.S. region of Mastercard® credit and Debit Mastercard® cards.

All acquirers must support receiving DE 48, subelement 52 in authorization response messages.

The Transaction Integrity Class may optionally be provided in the designated clearing messages when provided by Mastercard via the Authorization Platform for 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, subelement 52 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, subelement 52 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.

Transaction Integrity Classification Values

Following is a list of the Transaction Integrity Classification values provided in DE 48 (Additional Data—Private Use), subelement 52 (Transaction Integrity Class).

Classification	Description	Value
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

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Transaction Research Request

A transaction research request is a request by a customer for Mastercard to provide information about a transaction.

Customers can use either of the following two methods to research information about previous transactions:

- Transaction Investigator tool to conduct research about specific transactions or a range of transactions for an account number. The report generated provides customers with transactional data such as card number, card validation code 2 (CVC 2) response, point-of-sale entry mode, cardholder present information, merchant advice code, and message type identifier (MTI).
- If the transaction is over 180 days, customers can submit a request using the *Authorization Research Request* (Form 074). The Global Customer Service team will perform the research for you. The team provides information about authorization transactions, duplicate reports, microfiche re-creation, currency conversion rates, BIN and ICA numbers, and conversions.

About the Transaction Research Tool

The Transaction Research tool allows users to search the Mastercard data warehouse for transactions that a customer has processed as either an issuer or an acquirer.

This capability:

- Provides secure access to proprietary authorization information
- Retrieves 17 relevant transaction data elements online with the option to view all available data elements for a transaction.
- Returns the data within seconds after the customer electronically submits the request for research

In addition, users can print the transaction data or export the information into a Microsoft® Excel file.

The transaction data is stored in the Mastercard data warehouse and is available to customers for 180 days. Most transactions are available within six to 12 hours of the transaction time.

Request the Transaction Research Tool

Complete the following steps to request the Transaction Research Tool.

Procedure

1. Log on to Mastercard Connect™.
2. Enter your **User ID** and **Password**.
3. Click **Store** on the main menu (located in the upper right corner) on the Mastercard Connect home page.
4. Scroll to or search for **Transaction Research**.
5. Click **Add to Cart**.
   A confirmation message appears.

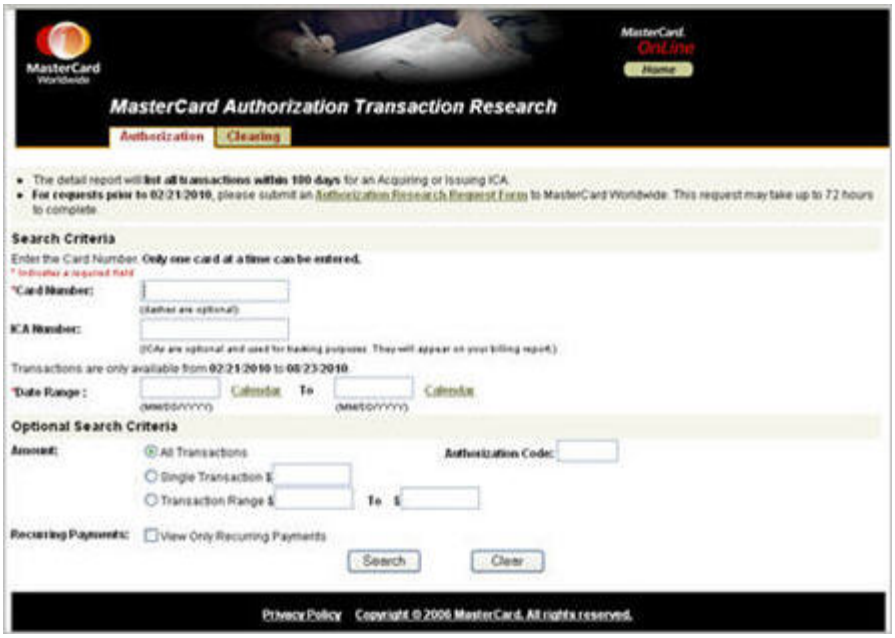
6. Click **Cart** to display the cart, and then click **Check Out** to display the Order Details window.
7. Under **Order Details**, click **Review Order** > **Place Order**.

   Once the Security Administrator approves the request, Transaction Research will appear under the Applications menu on the Mastercard Connect home page.

How to Access the Transaction Research Tool

Complete the following steps to access the Transaction Research Tool.

1. Log on to Mastercard Connect™.
2. On the **Applications** menu, click **Transaction Research**. The Mastercard Authorization Transaction Research page appears.



Research an Authorization Request

Complete the following steps to research an authorization request.

Procedure

1. In the **Card Number** box, enter the cardholder account number that you want to research.

   Note: Mastercard uses the optional ICA number for your tracking purposes only. If you enter an ICA number, it appears on your billing report to help you identify transactions.
2. In the **Data Range** area, enter a starting transaction date and an ending transaction date using a MM/DD/YYYY format or click the **Calendar** link to select a date.
3. To identify a transaction more specifically by its approval code, enter the **Authorization Code**.

4. To identify a transaction more specifically by its amount, select one of the following options:
   - Click **All Transactions** to retrieve all transactions.
   - Click **Single Transaction**, and then enter the amount in U.S. dollars to identify a single transaction.
   - Click **Transaction Range**, and then enter a starting transaction amount in U.S. dollars and the ending transaction amount in U.S. dollars to identify a range of transactions.
5. To view recurring payments only, select the **View Only Recurring Payments** check box.
6. Click **Search**. The search results page displays.
7. To display the detailed results for a specific transaction, select the transaction you want, and then click **Detail**.

Results

The Authorization Transaction Research tool displays a presence indicator for the following data elements in which they are present: DE 35 (Track 2 Data), DE 45 (Track 1 Data), and CVC 2 values in DE 48 (Additional Data—Private Use), subelement 92 (CVC 2).

Verify CVC Data

You can enter CVC 2 values to determine whether it matches the actual value in the transaction.

Procedure

1. To verify CVC data, follow these steps:
1. On the **Detail Results** screen, click **Verify CVC Data**.
2. In the **CVC 2** box, enter the appropriate CVC 2 code, and then click **Check**.
3. Depending on your CVC data validation results, a message appears indicating a **Match** or **No Match**. For example, if the results of your CVC data validation indicated a match, the message that displays would look similar to the following illustration.

About the Transaction Research Request Form

Customers can use the *Transaction Research Request* (Form 074) to request the Global Customer Service team to perform research for you.

If you submit a transaction research request by completing and sending the *Transaction Research Request* (Form 074) to Mastercard, Mastercard sends you a letter, with the authorization information, that you can use for chargeback purposes. If you request the services informally via a customer representative, you will not receive a letter.

About Fees for Transaction Research Requests

A general research fee applies to each customer inquiry requesting information that is readily available to the customer in a Mastercard publication, report, service, or other source.

Refer to the *Mastercard Consolidated Billing System* manual for fees and billing information.

Visa Transaction Processing

The Mastercard Authorization Platform allows acquirers to process Visa transactions via the Mastercard Network. It supports both transactions that qualify for the Visa Custom Payment Service Request and transactions that do not.

For diagrams that show the routing of these transactions, refer to Non-Mastercard Authorization Message Flows.

Issuer Options

Issuers may choose to accept Visa activity using their connection to the Mastercard Network. This connection is called peer-to-peer. If the issuer is not peer-to-peer, Mastercard routes authorization requests to the Visa network.

Custom Payment Service Request Transactions

For Visa transactions that indicate Custom Payment Service Request, Mastercard routes the authorization request to the Visa network.

Mastercard-acquired Custom Payment Service Request transactions have particular requirements for the Authorization Request/0100 and the Authorization Request Response/0110 messages.

For the data requirements as they apply to the authorization message formats, refer to the *Customer Interface Specification* manual.

Alternate Processing

If the Visa network is unavailable to authorize a Custom Payment Service Request transaction through the Mastercard gateway, Mastercard processes the authorization request using the Mastercard X-Code System.

Indicators

Mastercard provides support of various Visa programs by the use of specific indicators in Authorization Request/0100 messages.

Authorization Characteristics Indicator

Mastercard customers that acquire Visa transactions can receive valid Visa response values for the Authorization Characteristics Indicator (ACI).

Mastercard forwards the ACI value provided by Visa in DE 48 (Additional Data—Private Use), subelement 90 (Visa Custom Payment Service Request) of Authorization Request Response/0110 messages.

Mail/Telephone or Electronic Commerce Indicator

Visa allows acquirers to participate in its interregional interchange reimbursement fee (IRF) program in cases where the merchant and acquirer met and complied with certificate serial number requirements even though the cardholder did not.

Mastercard acquirers forwarding Visa e-commerce transactions must have the following values in Authorization Request/0100 messages.

Data Element	Value	Description
DE 22, subfield 1	10	Credential on File **NOTE: Mastercard is mandating support of the new DE 22, subfield 1, value 10 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.**
DE 22, subfield 1	81	PAN/Token entry via electronic commerce with optional Identity Check-AAV or DSRP cryptogram in UCAF field or the Digital Payment Data Field.
DE 22, subfield 1	82	PAN Auto Entry via Server (issuer, acquirer, or third party vendor system)
DE 61, subfield 10	6	Electronic Commerce
DE 48, subelement 40, subfield 01	Variable binary value 1–16 positions	To indicate that the merchant is certificate-compliant
DE 48, subelement 40, subfield 02	Not present	To indicate that the cardholder is not certificate-compliant
DE 48, subelement 42, subfield 01, position 2	1	To indicate cardholder certificate not used. For details about Visa usage for subelement 42, refer to the *Customer Interface Specification* manual

Data Element	Value	Description
DE 48, subelement 43, 44, 45		For details about Visa usage for subelements 43, 44, and 45, refer to the *Customer Interface Specification* manual.

Market-specific Data Identifier (Visa-only)

The Visa Market-Specific Data Identifier is a value used in Visa transactions to show the market-specific data identifier. Acquirers provide the appropriate Visa market-specific data identifier in DE 48 (Additional Data—Private Use), subelement 96 (Visa Market-Specific Data Identifier).

Prestigious Properties Indicator

The Prestigious Properties Indicator is a value used in Visa transactions to specify participants in the Visa Prestigious Lodging program. Acquirers provide the appropriate Visa Prestigious properties indicator in DE 48 (Additional Data—Private Use), subelement 97 (Prestigious Properties Indicator).

Relationship Participant Indicator

The Relationship Participant Indicator is a value used in Visa transactions to show that merchants have had long-term relationships with a cardholder from whom they regularly collect recurring payments.

Mastercard acquirers forwarding Visa transactions with a Relationship Participant Indicator must have value R (Merchant/Cardholder Relationship) or value I (Installment Payment) in DE 48 (Additional Data—Private Use), subelement 86 (Relationship Participant Indicator [Visa Only]) of Authorization Request/0100 messages.

Transponder Indicator

Cardholders may use transponders, which use radio frequency signals, to exchange identification information with cardholder-activated terminals or other point-of-interaction (POI) devices to initiate a transaction. These non–face-to-face transactions occur when the card is not present (when the transponder is the device activating the transaction).

Mastercard customers acquiring Visa transactions with a transponder must have value 7 in DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level) in Authorization Request/0100 messages. This value indicates that a transponder was used to exchange authorization information.

U.S. Existing Debt Indicator

When Mastercard acquirers in the U.S. region forward to Visa, through the Mastercard Network, transactions that pay an existing debt, they must indicate such in Authorization Request/0100 messages.

Acquirers must include value 9 in DE 48, subelement 85 (Visa U.S. Existing Debt Indicator) to indicate that the transaction is a payment for an existing debt.

Visa Payment Service Indicators

Mastercard has modified and expanded the existing structure of DE 48 (Additional Data—Private Use), subelement 78 (Payment Service Indicators [Visa Only]) (formerly subelement 78 [Visa U.S. Deferred Billing Indicator]) to update the Data Representation from a-1 to ans-6.

In addition, Mastercard has introduced six new subfields, three of which are defined below, and an additional three for future Visa data use.

- DE 48, subelement 78, subfield 1 (Spend Qualified Indicator) in the Authorization Request Response/0110 message contains the Spend Qualified Indicator for Visa-branded, dual-message authorization transactions.
- DE 48, subelement 78, subfield 2 (Dynamic Currency Conversion Indicator) in the Authorization Request/0100 message contains the Dynamic Currency Conversion indicator for Visa-branded, dual-message authorization transactions.
- DE 48, subelement 78, subfield 3 (U.S. Deferred Billing Indicator) in the Authorization Request/0100 message contains the U.S. Deferred Billing indicator for Visa-branded, dual-message authorization transactions.
- DE 48, subelement 78, subfields 4–6 are reserved for future use.

The U.S. Deferred Billing Indicator is a value used by U.S. acquirers in Visa transactions to notify U.S. issuers that the transaction is being submitted to bill the cardholder for merchandise that was received within the past 90 days.

Mastercard acquirers forwarding Visa transactions with the U.S. Deferred Billing Indicator must have value D (U.S. Deferred Billing Indicator) in DE 48, subelement 78, subfield 3 in Authorization Request/0100 messages.

Retail Key Entry Program

Mastercard acquirers forwarding Visa Retail Key Entry transactions must have the following values in Authorization Request/0100 messages.

Data Element	Value	Description
DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	01	Indicates that the card number was keyed into the POS device
DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence)	0	Indicates that the cardholder is present
DE 61, subfield 5 (POS Card Presence)	0	Indicates that the card is present

Data Element	Value	Description
DE 61, subfield 11 (POS Card Data Terminal Input Capability)	2, 5, 7, or 8	Indicates that the POS terminal can transmit magnetic stripe data

NOTE: For a transaction to be forwarded automatically to the Visa gateway, acquirers must identify transactions as Visa Custom Payment Services transactions. Meeting Retail Key Entry criteria will not force a transaction to the Visa gateway if the issuer is a Mastercard peer-to-peer participant.

Secure Electronic Commerce Verification Service

The Mastercard Authorization Platform supports the Visa secure electronic commerce verification service.

Mastercard will forward to the Visa gateway Authorization Request/0100 messages including secure e-commerce data that also contain a Visa account number in DE 2 (Primary Account Number [PAN]).

To participate, acquirers must provide all e-commerce data elements, including the data elements for the secure e-commerce verification, in Authorization Request/0100 messages.

Acquirers must use DE 48 (Additional Data—Private Use), subelement 43 (UCAF), and subelement 44 (Electronic Commerce Transaction Identifier) to send the secure e-commerce data in Authorization Request/0100 messages. If Visa responds with a Cardholder Authentication Verification Value (CAVV) Results Code, Mastercard forwards the code values to the acquirer in DE 48, subelement 45 (Electronic Commerce Transaction Response Code) of the Authorization Request Response/0110 message.

Visa Product ID

Acquirers that process Visa transactions through the Authorization Platform receive DE 48 (Additional Data—Private Use), subelement 46 (Product ID) in Authorization Request Response/0110 and Reversal Request Response/0410 messages. The associated Visa field for DE 48, subelement 46 is field 62.23 (Product ID).

Visa Commercial Card Inquiry

Acquirers can inquire on Visa Commercial Cards using specific values in DE 48 (Additional Data—Private Use), subelement 94 (Visa Commercial Card inquiry request and response indicator). These values are described in the *Customer Interface Specification* manual.

Visa Fleet Card

Mastercard supports processing of Visa Fleet Card transactions through the Dual Message System in DE 48, subelement 93 (Visa Fleet Card ID Request Data) indicator. For more detailed information, refer to the *Customer Interface Specification* manual.

Visa-Assigned Merchant Verification Value

Mastercard supports the Visa mandate requiring that the Merchant Verification Value (MVV) be populated in all processing messages when an MVV has been assigned to the merchant by Visa.

Mastercard only includes the Visa-assigned MVV value on those transactions that are routed to the Visa network using the Mastercard Visa Gateway.

Acquirers of Visa-branded transactions will provide, when applicable, an alphanumeric Merchant Verification Value (MVV) in DE 48 (Additional Data—Private Use), subelement 36 (Visa Defined Data), subfield 1 in Authorization Request/0100 and Reversal Request/0400 messages. If it is provided in any other message types, the Dual Message System will remove it before sending the transaction to the Visa network.

Mastercard is not aware of which merchants are assigned an MVV by Visa, and therefore will not know which acquirers provide or not provide the MVV in a message. If present, the Mastercard Network forwards the value in the transaction to the Visa network.

The Dual Message System removes DE 48, subelement 36, subfield 1 from any transaction provided by an acquirer that is not a Visa-branded transaction.

The MVV is not provided back to the acquirer in any messages. If DE 48, subelement 36, subfield 1 is provided in any response messages, the Dual Message System will remove it before sending the message to the acquirer.

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 PARTIALSHIPMENT0000000000000 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 *Identity Check* merchant has chosen not to undertake *Identity Check* 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)

Chapter 8 Reports

The Reports section contains information about the reports and logs related to the Mastercard Authorization Platform.

Related Reports in Other Manuals

Information about layouts of authorization detail and billing reports and layouts of all reports related to listing accounts or merchants listed in the Merchant File provided in other manuals.

For information about authorization details and billing reports, including the following reports, refer to the *Mastercard Consolidated Billing System* manual.

Report Name	Report Number
Issuer Authorization Detail Report	AB201010-A2
Acquirer Authorization Detail Report	AB202010-A1
Billable Customer Summary	GB071010-AA
Customer Service Summary	GB073010-AA
Customer Service Roll-Up	GB074010-AA

Please refer to the *Account Management System User Manual* for layouts of all reports related to listing accounts in the Account Management System (AMS) or merchants listed in the Merchant File.

Presentation of Reports

Each authorization report is introduced with an overview that contains the following information.

- Title—Name or title of the report
- Generated by—System generating the report
- Purpose—Reason for providing the report
- Description—Kind of information included in the report
- Frequency—How often the report is generated
- Distribution Methods—Distribution alternatives and associated bulk file or Mastercard File Express application identification numbers

A sample of the report follows each overview description. Field descriptions for the report follow the report sample.

Report Header Information

Report header information is contained in all reports generated by the Authorization Platform. This information is not described with the individual report descriptions.

- The report number appears in the upper left-hand corner of each report and identifies the report by number.
- The report header is located in the upper center of each report and identifies the report by name.
- The page number appears in the upper right-hand corner of each report and identifies the page number within the report.
- The date appears in the upper right-hand corner of each report and identifies the date the report was generated. All are St. Louis dates.
- The time, when it appears, is in the upper right-hand corner of each report and identifies the time the report was generated. All are St. Louis times.

Authorization Summary Report (AB505010-AA)

An overview of the Authorization Summary Report (AB505010-AA) is listed in table format.

Title	Authorization Summary Report
Generated by	Mastercard Authorization Platform
Purpose	To provide customers with a tool for analyzing authorization performance.
Description	This report shows authorization transaction processing volumes and percentages by BIN for the week. It reflects transactions that use the Dual Message System and billable items.
Frequency	Weekly
Distribution Methods	Paper (Sent to the authorization contact established on the Principal Member Questionnaire); Mastercard eService, Mastercard File Express, complex-to-complex, bulk ID (T829)

Report Sample

Report sample of the Authorization Summary Report (AB505010-AA).

REPORT AB505010-AA MASTERCARD INTERNATIONAL INC. PAGE 1
AUTHORIZATION SUMMARY DATE 04/26/05 TIME 05:58:39
FOR MCBS BILLING WEEK BEGINNING 04/16/05 AND ENDING 04/22/05
ICA 999999 PREFIX 999900 THRU 999999

MEMBER PROCESSED ACTIVITY	MEMBER VOLUME	MEMBER YTD VOLUME	SYSTEM VOLUME	SYSTEM YTD VOLUME	WEEKLY RANK
ACCEPT	564,630	22,883,608	50,564,716	1,889,434,968	00017/07153
PERCENT OF TOTAL	90.2	90.5	96.2	96.4	
DECLINE	59,215	2,307,720	1,741,380	60,674,795	00002/07153
PERCENT OF TOTAL	9.5	9.1	3.3	3.1	
CALL-ME	0	0	150,001	5,834,621	N/A
PERCENT OF TOTAL	0.0	0.0	0.3	0.3	
PICK-UP	2,075	87,892	121,165	4,411,816	00010/07153
PERCENT OF TOTAL	0.3	0.3	0.2	0.2	
TOTAL MEMBER PROCESSED	625,920	25,279,220	52,577,262	1,960,356,200	

MEMBER APPROVALS BY TRANSACTION TYPE	AVERAGE DOLLARS	TOTAL DOLLARS	TOTAL VOLUME	YTD AVERAGE DOLLARS	YTD TOTAL DOLLARS	YTD TOTAL VOLUME
MAIL/TELEPHONE	62.98	4,551,994.70	72,276	65.15	185,280,386.57	2,843,761
RETAIL	58.86	23,437,278.81	398,177	59.18	956,823,819.59	16,168,211
CASH ADVANCE	515.73	1,521,389.34	2,950	500.61	68,338,524.18	136,511
COLLEGE/HOSPITAL	128.54	188,570.61	1,467	159.22	11,772,145.33	73,935
HOTEL/MOTEL	129.13	2,524,940.10	19,554	124.37	96,485,766.89	775,819
VEHICLE RENTAL	147.57	672,896.56	4,560	151.75	27,413,086.86	180,651
TRANSPORTATION	205.26	1,153,968.62	5,622	210.15	50,413,442.93	239,892
RESTAURANT	33.25	1,942,706.50	58,435	33.58	80,370,436.82	2,393,379
CIRRUS/ATM	.00	.00	0	395.35	5,139.61	13
UNIQUE	270.75	430,219.68	1,589	259.43	18,532,388.74	71,436
PAYMENT TXN	.00	.00	0	0	0	0
TOTAL MEMBER APPROVALS	64.51	36,423,964.92	564,630	65.35	1,495,435,137.52	22,883,608

REPORT AB505010-AA MASTERCARD INTERNATIONAL INC. PAGE 2
AUTHORIZATION SUMMARY DATE 04/26/05 TIME 05:58:39
FOR MCBS BILLING WEEK BEGINNING 04/16/05 AND ENDING 04/22/05
ICA 999999 PREFIX 999900 THRU 999999

STAND-IN PROCESSED ACTIVITY	MEMBER VOLUME	MEMBER YTD VOLUME	SYSTEM VOLUME	SYSTEM YTD VOLUME	WEEKLY RANK
ACCEPT	411	41,001	232,355	8,355,358	00108/07153
PERCENT OF TOTAL	94.9	91.0	86.2	88.4	
DECLINE	20	3,676	15,356	500,897	00158/07153
PERCENT OF TOTAL	4.6	8.2	5.7	5.3	
CALL-ME	0	0	20,625	552,119	N/A
PERCENT OF TOTAL	0.0	0.0	7.7	5.8	
PICK-UP	2	357	1,083	39,632	00067/07153
PERCENT OF TOTAL	0.5	0.8	0.4	0.4	
TOTAL STAND-IN PROCESSED	433	45,034	269,419	9,448,006	
TIMED OUT	397	5,718	98,929	3,876,488	00046/07153
PERCENT OF TOTAL	91.7	12.7	36.7	41.0	
MEMBER DOWN	0	37,815	116,520	3,172,070	00364/07153
PERCENT OF TOTAL	0.0	84.0	43.2	33.6	
SIGNED OUT	0	1,501	53,970	2,399,448	N/A
PERCENT OF TOTAL	0.0	3.3	20.0	25.4	

NON-ACCEPTED AUTHORISATIONS BY FAIL REASON

FAIL REASON	MEMBER VOLUME	DOLLAR VOLUME
AUTH FILE	0	.00
TRANS LIMIT	20	15595.02
DAY 1 TRANS	0	.00
DAY 1 DOLLARS	0	.00
DAY 2 TRANS	0	.00
DAY 2 DOLLARS	0	.00
DAY 3 TRANS	0	.00
DAY 3 DOLLARS	0	.00
DAY 4 TRANS	0	.00
DAY 4 DOLLARS	0	.00
VIP ACCUM LIMIT	0	.00
CASH ADV ACCUMS	0	.00
MERCH SUSPIC	0	.00
INVALID CHIP/CVC	0	.00

ACCEPTED DOLLARS $19,193.36 NON-ACCEPTED DOLLARS $15,684.82

LIMIT-1 MIP PROCESSED ACTIVITY	MEMBER VOLUME	MEMBER YTD VOLUME	SYSTEM VOLUME	SYSTEM YTD VOLUME	WEEKLY RANK
ACCEPT	0	0	1,319,640	78,253,680	N/A
PERCENT OF TOTAL	0.0	0.0	99.9	99.9	
DECLINE	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
CALL-ME	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
PICK-UP	0	0	665	45,597	N/A
PERCENT OF TOTAL	0.0	0.0	0.1	0.1	
TOTAL LIMIT-1 PROCESSED	0	0	1,320,305	78,299,277	

REPORT AB505010-AA MASTERCARD INTERNATIONAL INC. PAGE 3
AUTHORIZATION SUMMARY DATE 04/26/05 TIME 05:58:39
FOR MCBS BILLING WEEK BEGINNING 04/16/05 AND ENDING 04/22/05
ICA 999999 PREFIX 999900 THRU 999999

MAIL/TELEPHONE	0	0	10,479	429,365	N/A
PERCENT OF TOTAL	0.0	0.0	0.8	0.5	
CASH ADVANCE	0	0	294	24,068	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
RETAIL	0	0	1,116,166	69,546,553	N/A
PERCENT OF TOTAL	0.0	0.0	84.5	88.8	
TRAVEL/ENTERTAINMENT	0	0	193,366	8,299,291	N/A
PERCENT OF TOTAL	0.0	0.0	14.6	10.6	

X-CODE MIP PROCESSED ACTIVITY	MEMBER VOLUME	MEMBER YTD VOLUME	SYSTEM VOLUME	SYSTEM YTD VOLUME	WEEKLY RANK
ACCEPT	459	27,852	48,775	2,139,689	00020/07153
PERCENT OF TOTAL	95.4	96.9	79.7	78.2	
DECLINE	8	103	6,182	282,101	00087/07153
PERCENT OF TOTAL	1.7	0.4	10.1	10.3	
CALL-MC	14	723	6,222	313,486	00033/07153
PERCENT OF TOTAL	2.9	2.5	10.2	11.5	
PICK-UP	0	52	47	2,216	N/A
PERCENT OF TOTAL	0.0	0.2	0.1	0.1	
TOTAL X-CODE PROCESSED	481	28,730	61,226	2,737,492	

MIP PROCESSED ACTIVITY	MEMBER VOLUME	MEMBER YTD VOLUME	SYSTEM VOLUME	SYSTEM YTD VOLUME	WEEKLY RANK
ACCEPT	0	23	19	1,866	N/A
PERCENT OF TOTAL	0.0	52.3	48.7	56.0	
DECLINE	0	21	20	1,465	N/A
PERCENT OF TOTAL	0.0	47.7	51.3	44.0	
CALL-MC	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
PICK-UP	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
TOTAL MIP PROCESSED	0	44	39	3,331	

BAT PROCESSED ACTIVITY	MEMBER VOLUME	MEMBER YTD VOLUME	SYSTEM VOLUME	SYSTEM YTD VOLUME	WEEKLY RANK
ACCEPT	51	84	542	1,862	00000/13568
PERCENT OF TOTAL	100.0	100.0	98.5	94.2	
DECLINE	0	0	3	16	N/A
PERCENT OF TOTAL	0.0	0.0	0.5	10.3	
CALL-MC	0	0	5	101	N/A
PERCENT OF TOTAL	0.0	0.0	0.9	5.1	
PICK-UP	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
TOTAL BAT PROCESSED	51	84	550	2,000	

REPORT AB505010-AA MASTERCARD INTERNATIONAL INC. PAGE 4
AUTHORIZATION SUMMARY DATE 04/26/05 TIME 05:58:39
FOR MCBS BILLING WEEK BEGINNING 04/16/05 AND ENDING 04/22/05
ICA 999999 PREFIX 999900 THRU 999999

WEEKLY TOTALS

WEEKLY TOTAL ACTIVITY	MEMBER VOLUME	MEMBER YTD VOLUME	SYSTEM VOLUME	SYSTEM YTD VOLUME	WEEKLY RANK
ACCEPT	565,500	22,952,484	52,165,505	1,978,185,561	00017/07153
PERCENT OF TOTAL	90.2	90.5	96.2	96.5	
DECLINE	59,243	2,311,520	1,762,938	61,459,258	00002/07153
PERCENT OF TOTAL	9.5	723	3.3	3.0	
CALL-MX	14	9.1	176,848	6,700,226	00711/07153
PERCENT OF TOTAL	0.0	0.0	0.3	0.3	
PICK-UP	2,077	88,301	122,960	4,499,261	00010/07153
PERCENT OF TOTAL	0.3	0.3	0.2	0.2	
TOTAL PROCESSED	626,834	25,353,028	54,228,251	2,050,844,306	

REPORT AB505010-AA MASTERCARD INTERNATIONAL, INC. PAGE 5
ACQUIRER GENERATED REVERSAL AUTHORIZATION SUMMARY DATE 04/26/05 TIME 05:58:39
FOR MCBS BILLING WEEK BEGINNING 04/16/05 AND ENDING 04/22/05
ICA 999999 PREFIX 999900 THRU 999999

REVERSAL PROCESSED ACTIVITY	REVERSAL VOLUME	REVERSAL YTD VOLUME	SYSTEM VOLUME	SYSTEM YTD VOLUME	WEEKLY RANK
ACCEPT	0	0	0	5	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	100.0	
DECLINE	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
CALL-ME	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
PICK-UP	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
TOTAL REVERSAL PROCESSED	0	0	0	5	

REPORT AB505010-AA MASTERCARD INTERNATIONAL, INC. PAGE 6

ACQUIRER GENERATED REVERSAL AUTHORIZATION SUMMARY DATE 04/26/05 TIME 05:58:39

FOR MCBS BILLING WEEK BEGINNING 04/16/05 AND ENDING 04/22/05

ICA 999999 PREFIX 999999 THRU 999900

W E E K L Y T O T A L S

WEEKLY REVERSAL TOTAL ACTIVITY	REVERSAL VOLUME	REVERSAL YTD VOLUME	SYSTEM VOLUME	SYSTEM YTD VOLUME	WEEKLY RANK
ACCEPT	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
DECLINE	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
CALL-ME	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
PICK-UP	0	0	0	0	N/A
PERCENT OF TOTAL	0.0	0.0	0.0	0.0	
TOTAL PROCESSED	0	0	0	0	

Field Descriptions

The fields on the Authorization Summary Report (AB505010-AA) are listed in table format.

Field	Description
Member Processed Activity	Summary of all authorization activity received and processed by the issuer, listed by the following response categories: • Accept (approved) • Decline • Call-Me (refer to card issuer) • Pick-Up (capture card)

Field		Description
	Member Volume	Total transaction volume processed by the customer that generated the specific response and the percentage it represents of total member transaction volume.
	Member YTD Volume	Summary of the customer's authorization volume for the calendar year-to-date (by response category) and the percentage it represents of total member volume for the year-to-date.
	System Volume	Volume of authorization transactions processed by the entire membership that week and the percentage it represents of total volume for the membership for the week.
	System YTD Volume	Volume of authorization transactions processed by the entire membership for the calendar year-to-date and the percentage it represents of total volume for the membership for the year-to-date.
	Weekly Rank	Ranking by bank identification number (BIN) of member volume within the membership (compared to total system volume). This field shows where each BIN stands in relation to other BINs. In the sample, the Weekly Rank column at the Accept Category line shows 00017/07153. This indicates that this BIN ranks 17th out of a total of 7,153 BINs in issuing approvals; 16 BINs issued more approvals and 7,136 BINs issued fewer approvals.
Member Approvals by Transaction Type		Summary of all approved responses returned, broken down by the following transaction categories: • Mail/Telephone • Retail • Cash Advance • College/Hospital • Hotel/Motel • Vehicle Rental • Transportation • Restaurant • Cirrus/ATM • Unique • Payment Transaction
	Average Dollars	Average dollar amount approved for the week, listed by transaction type.

Field		Description
	Total Dollars	Total dollar amount approved for the week, listed by transaction type
	Total Volume	Total transaction volume processed by the customer for the week, listed by transaction type. In the sample, the total volume for MO/TO transactions is 72,276. This indicates that out of a total of 564,630 approved transactions, 72,276 were for MO/TO.
	YTD Average Dollars	Average U.S. dollar amount approved, by transaction type, for the calendar year-to-date. This amount is the result of dividing the YTD TOTAL DOLLARS by the YTD TOTAL VOLUME.
	YTD Total Dollars	Total U.S. dollar amount approved by the customer, listed by transaction type, for the calendar year-to-date.
	YTD Total Volume	Total transaction volume approved by the customer, listed by transaction type, for the calendar year-to-date.
	Total Member Approvals	Average U.S. dollar amount, total U.S. dollar amount, total transaction volume, and year-to-date totals for all transactions approved by the customer.
Stand-In Processed Activity		Summary of all authorization activity received and processed by Stand-In processing, listed by the following response categories: • Accept (approved) • Decline • Call-Me (refer to card issuer) • Pick-Up (capture card) Refer to field descriptions for an explanation of Member Volume, Member YTD Volume, System Volume, System YTD Volume, and Weekly Rank. All values are for authorization activity processed by Stand-In processing on behalf of the customer.
	Timed Out (Percent of Total)	Number of times the Mastercard Network authorization application sent the original authorization request to the issuer for processing but the acquiring MIP did not receive a response in the allocated time. The second line indicates the percentage of total authorization requests that timed out in this manner.

Field		Description
	Member Down (Percent of Total)	Number of authorization requests sent to Stand-In processing because the Mastercard Network authorization application recognized that the issuer's host was down. Transactions that left the acquiring node but did not reach the issuing MIP, or did reach the issuing MIP but could not communicate with the issuer's host, are included in this count. The second line indicates the percentage of total authorization requests sent that the application handled in this manner.
	Signed Out (Percent of Total)	Number of transactions sent to Stand-In processing because the issuer was signed out. The second line indicates the percentage of total authorization requests sent that went to Stand-In processing for this reason.
Non-accepted Authorizations by Fail Reason		Summary of all authorization activity processed by Stand-In that Stand-In did not approve because it failed the indicated tests performed during Stand-In processing.
	Fail Reason	List of the Stand-In tests that authorization requests must pass to be approved. **NOTE: The Fail Reason INVALID CHIP/CVC includes both transactions that failed for invalid CHIP/CVC in Stand-In and transactions that failed for magnetic stripe/CVC error (codes A–J) at the MIP.**
	Member Volume	Total volume of transactions declined authorization because of failure to pass the Stand-In test listed.
	Dollar Volume	Total U.S. dollar amount declined authorization because of failure to pass the Stand-In test listed.
	Accepted Dollars	Total U.S. dollar amount that Stand-In authorized on behalf of the issuer for the week reported.
	Non-Accepted Dollars	Total U.S. dollar amount that Stand-In did not authorize when processing on behalf of the issuer for the week reported.

Field	Description
X-Code MIP Processed Activity	Summary of all authorization activity processed as X-Code transactions at the acquirer MIP. These transactions are transactions that should have gone to the issuer or to Stand-In for processing, but the authorization application could not obtain a response from either one. Transactions are listed by the following response categories: • Accept (approved) • Decline • Call-Me (refer to card issuer) • Pick-Up (capture card) Refer to field descriptions for an explanation of Member Volume, Member YTD Volume, System Volume, System YTD Volume, and Weekly Rank. All values are for authorization activity processed at the acquirer MIP using X-Code parameters.
MIP Processed Activity	Summary of all authorization activity involving certain cardholder-activated terminals processed at the MIP that would not be processed by an issuer or Stand-In. Transactions are listed by the following response categories: • Accept (approved) • Decline • Call-Me (refer to card issuer) • Pick-Up (capture card) Refer to field descriptions for an explanation of Member Volume, Member YTD Volume, System Volume, System YTD Volume, and Weekly Rank. All values are for authorization activity processed at the MIP using X-Code parameters or those transactions declined by the MIP Transaction Blocking service.
Weekly Total Activity	Summary of total transaction volume processed by the customer, Stand-In, X-Code, MIP, and BAT on behalf of the customer for the week reported. Refer to field descriptions for an explanation of Member Volume, Member YTD Volume, System Volume, System YTD Volume, and Weekly Rank.

Field		Description
Acquirer Reversal Processed Activity		Summary of Reversal Request/0400 message activity received and processed by the issuer, listed by the following response categories: • Accept (approved) • Decline • Call-Me (refer to card issuer) • Pick-Up (capture card)
	Reversal Volume	Total reversal volume processed by the customer that generated the specific response and the percentage it represents of total member transaction volume.
	Reversal YTD Volume	Summary of the customer's reversal volume for the calendar year-to-date (by response category) and the percentage it represents of total member volume for the year-to-date.
	System Volume	Volume of reversal transactions processed by the entire membership that week and the percentage it represents of total volume for the membership for the week.
	System YTD Volume	Volume of reversal transactions processed by the entire membership for the calendar year-to-date and the percentage it represents of total volume for the membership for the year-to-date.
	Weekly Rank	Ranking by bank identification number (BIN) of member volume within the membership (compared to total system volume). This field shows where each BIN stands in relation to other BINs.
	Total Reversal Processed	Average U.S. dollar amount, total U.S. dollar amount, total transaction volume, and year-to-date totals for all transactions approved by the customer.

Field		Description
Reversal Approvals by Transaction Type		Summary of all approved responses returned, broken down by the following transaction categories: • Mail/Telephone • Retail • Cash Advance • College/Hospital • Hotel/Motel • Vehicle Rental • Transportation • Restaurant • Cirrus/ATM • Unique • Payment Transaction
	Average Dollars	Average dollar amount approved for the week, listed by transaction type.
	Total Dollars	Total dollar amount approved for the week, listed by transaction type.
	Total Volume	Total transaction volume processed by the customer for the week, listed by transaction type.
	YTD Average Dollars	Average U.S. dollar amount approved, by transaction type, for the calendar year-to-date. This amount is the result of dividing the YTD TOTAL DOLLARS by the YTD TOTAL VOLUME.
	YTD Total Dollars	Total U.S. dollar amount approved by the customer, listed by transaction type, for the calendar year-to-date.
	YTD Total Volume	Total transaction volume approved by the customer, listed by transaction type, for the calendar year-to-date.
	Total Reversals Approvals	Average U.S. dollar amount, total U.S. dollar amount, total transaction volume, and year-to-date totals for all transactions approved by the customer.

Field	Description
MIP Reversal Processed Activity	Summary of all reversal activity received and processed by Stand-In, listed by the following response categories: • Accept (approved) • Decline • Call-Me (refer to card issuer) • Pick-Up (capture card) Refer to field descriptions for an explanation of Reversal Volume, Reversal YTD Volume, System Volume, System YTD Volume, and Weekly Rank. All values are for authorization activity processed by Stand-In processing on behalf of the customer.
Total MIP Reversal Processed	Total reversal transaction volume, and year-to-date totals for all reversals approved by the customer.
Weekly Total Activity	Summary of total reversal transaction volume processed by the customer, Stand-In, X-Code, MIP, and BAT on behalf of the customer for the week reported. Refer to field descriptions for an explanation of Reversal Volume, Reversal YTD Volume, System Volume, System YTD Volume, and Weekly Rank.

Authorization Processing Integrity Acquirer Detail Report (AB605010-AA and AB605010-FF)

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 optically choose to receive this report. Mastercard generates the report weekly. The report is delivered each Monday at 18:30 (St. Louis, Missouri, USA time). Acquirers can request to receive the report by contacting Global Customer Service.

AB605010-AA Image Report

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, it is likely to be large (in excess of 350,000 lines). Delivery via bulk file 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-complaint authorizations to report within a billing period, the image format report (AB605010-AA) is not generated.

Report Sample

Report sample of the Authorization Processing Integrity Acquirer Detail Report (AB605010-AA).

```
1REPORT NUMBER: AB605010-AA                              MASTERCARD INTERNATIONAL                                 RUN DATE: JUL 09 2018
 BILLING CYCLE DATE: JUL 08 2018                        CONSOLIDATED BILLING SYSTEM                               RUN TIME: 16.02.16
0                                             AUTHORIZATION PROCESSING INTEGRITY ACQUIRER DETAIL REPORT           PAGE:              1
 ACQUIRER ICA/CUST ID:   XXXXX                     NAME:   XXXXXXXXXXXXXXXXXX
 Final Authorization Not Meeting Necessary Requirement
 CARDHOLDER          AUTH          CLRNG          POS  FWD-INST      AUTH      CLRNG     AUTH    FIN-NET  AUTH      BRAND MCC   TRAN
 NUMBER              AMT           AMT           CNTRY    ID         DATE      DATE       ID      CODE     BRN                  STATUS
 MERCHANT        MERCHANT                                  FINAL    RESP   AUTH-CURR  CLRNG-CURR PROC CLRNG      CLRNG
 ID              NAME                                    AUTH-IND CODE      CODE       CODE      CODE  BRN       MATCH
 FINAL AUTH   CURR MISMATCH   AMT MISMATCH   BILL-CURR    BILL CONV     MIP OWNER    ADDTL   ADDTL   BILLING-EVENT
 RVSL IND     IND             IND            CODE         AUTH AMT          ICA      RESP 1  RESP 2
 516815XXXXXX1981   999999999999 999999999999 XXX  99999999999  9999999.          999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX XXXXXXXXX   XXX   9      99     999                    99            N
 N                                        999      999:99                  000     000    XXXXXXXX
 516815XXXXXX1557   999999999999 999999999999 XXX  99999999999  9999999.          999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX XXXXXXXXX   XXX   9      99     999                    99            N
 Y                                        999      999:99                  000     000    XXXXXXXX
 516815XXXXXX2756   999999999999 999999999999 XXX  99999999999  9999999.          999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX XXXXXXXXX   XXX   9      99     999                    99            N
 Y                                        999      999:99                  000     000    XXXXXXXX
 516815XXXXXX6787   999999999999 999999999999 XXX  99999999999  9999999. 99999999 999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX. XXXXXXXXX  XXX   9      99     999        999         99  XXXXXXXXX  Y
 N            N               Y           999      999:99                  000     000    XXXXXXXX
 672291XXXXXXXXX9463 999999999999 999999999999 XXX  99999999999  9999999. 99999999 999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX. XXXXXXXXX  XXX   9      99     999        999         99  XXXXXXXXX  Y
 N            N               Y           999      999:99                  000     000    XXXXXXXX
 516815XXXXXX8466   999999999999 999999999999 XXX  99999999999  9999999. 99999999 999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX. XXXXXXXXX  XXX   9      99     999        999         99  XXXXXXXXX  Y
 N            N               Y           999      999:99                  000     000    XXXXXXXX
 516815XXXXXX6111   999999999999 999999999999 XXX  99999999999  9999999. 99999999 999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX. XXXXXXXXX  XXX   9      99     999        999         99  XXXXXXXXX  Y
 N            N               Y           999      999:99                  000     000    XXXXXXXX
 516815XXXXXX9847   999999999999 999999999999 XXX  99999999999  9999999. 99999999 999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX. XXXXXXXXX  XXX   9      99     999        999         99  XXXXXXXXX  Y
 N            N               Y           999      999:99                  000     000    XXXXXXXX
 554501XXXXXX1172   999999999999 999999999999 XXX  99999999999  9999999. 99999999 999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX. XXXXXXXXX  XXX   9      99     999        999         99  XXXXXXXXX  Y
 N            N               Y           999      999:99                  000     000    XXXXXXXX
 516815XXXXXX2777   999999999999 999999999999 XXX  99999999999  9999999. 99999999 999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX. XXXXXXXXX  XXX   9      99     999        999         99  XXXXXXXXX  N
 N                                        999      999:99                  000     000    XXXXXXXX
 516815XXXXXX9313   999999999999 999999999999 XXX  99999999999  9999999. 99999999 999999 XXX      XXXXXX     XXX  9999   0
 999999          XXXXXXXXXXXXXXXXXXXXX  XXXXXXXXXXXXX XXX   9    99     999        999         99  XXXXXXXXX  N
 Y                                        999      999:99                  000     000    XXXXXXXX
 516815XXXXXX9583   999999999999 999999999999 XXX  99999999999  9999999. 99999999 999999 XXX      XXXXXX     XXX  9999   0
 9999999         XXXXXXXXXXXXXXXXXXXXX  XXXXXXXXX  XXX   9      99     999        999         99  XXXXXXXXX  N
 Y                                        999      999.99                  000     000    XXXXXXXX
 534244XXXXXX8128   999999999999 999999999999 XXX  99999999999  9999999. 99999999 999999 XXX      XXXXXX     XXX  9999   0
 99999999        XXXXXXXXXXXXXXXXXXXXX  XXXXXXXXX  XXX   9      99     999        999         99  XXXXXXXXX  N
```

Field Descriptions

The format and layout of the data file follows.

Field Name Displayed in Report	Field Name (expanded)	Data Element (DE)	Field Description
ACQUIRER ICA/ CUST ID	Acquirer Institution ID	DE 32	Space filled, left justified (for example, 9744).
CARDHOLDER NUMBER	Cardholder Number	DE 2	Masked (obfuscated) PAN. First six and last four digits of the PAN will be shown (for example, 999999XXXXXX9999). Space filled, left justified.
AUTH AMT	Authorization Transaction Amount	DE 4	Zero filled, right justified (for example, 00000001211).
CLRNG AMT	Clearing Transaction Amount	DE 4	Zero filled, right justified (for example, 00000001211). Blank if not applicable for billing event.
POS CNTRY	POS Country	DE 61, subfield 13	Alpha country code.
FWD-INST ID	Forwarding Institution ID	DE 33	Zero filled, right justified (for example, 00000008434).
AUTH DATE	Authorization Date	DE 15	YYYYMMDD Derived YYYY, DE 15 MMDD
CLRNG DATE	Clearing Date	PDS 0158, subfield 5	YYYYMMDD Derived YYYY, PDS 0158 subfield 5 YYMMDD. Blank if not applicable for billing event.
AUTH ID	Authorization ID	DE 38	
FIN-NET CODE	Financial Network Code	DE 63, subfield 1	
AUTH BRN	Authorization Banknet Reference Number	DE 63, subfield 2	Left justified.
BRAND	Acceptance Brand		
MCC	Merchant Category Code	DE 18	

Field Name Displayed in Report	Field Name (expanded)	Data Element (DE)	Field Description
TRAN STATUS	Point of Service Transaction Status	DE 61, subfield 7	
MERCHANT ID	Merchant ID	DE 42	Space filled, left justified.
MERCHANT NAME	Merchant Name Location	DE 43	Space filled, left justified.
FINAL AUTH IND	Final Authorization Indicator	DE 48, subelement 61, subfield 5	
RESP CODE	Response Code	DE 39	
AUTH-CURR CODE	Authorization Currency Code	DE 49	
CLRNG-CURR CODE	Clearing Currency Code	DE 49	Contains XXX if multiple clearing records are processed for a single authorization and one clearing record currency code differs from the authorization currency code. Otherwise, contains the clearing currency code of the last clearing record processed for the authorization. Blank if not applicable for billing event.
PROC CODE	Processing Code	DE 3, subfield 1	
CLRNG BRN	Clearing Banknet Reference Number	DE 63, subfield 2	Space filled, left justified. Blank if not applicable for billing event.

Field Name Displayed in Report	Field Name (expanded)	Data Element (DE)	Field Description
CLRNG MATCH	Clearing Match		Identifies if a matching clearing transaction was found for an authorization. Values are: • Y—Matching clearing found • N—Matching clearing not found • M—Multiple clearing records processed for a single authorization request • Blank—Not applicable for billing event
FINAL AUTH RVSL IND	Final Auth Reversal Indicator		Identifies if a final authorization was reversed, which resulted in a matching clearing transaction not being found for an authorization. • Y—Authorization was reversed • N—Authorization was not reversed • Blank—Not applicable for billing event
CURR MISMATCH IND	Currency Mismatch Indicator		Identifies if the authorization and clearing Transaction Currency Code (DE 49) are not the same. Values are: • Y—Authorization and clearing currencies do not match • N—Authorization and clearing currencies match • Blank—Not applicable for billing event

Field Name Displayed in Report	Field Name (expanded)	Data Element (DE)	Field Description
AMT MISMATCH IND	Amount Mismatch Indicator		Identifies if the authorization and clearing Transaction Amount (DE 4) are not the same. Values are: • Y—Authorization and clearing amounts do not match • N—Authorization and clearing amounts match • Blank—Not applicable for billing event
BILL-CURR CODE	Billing Currency Code		Identifies the currency code of the assessed fee.
BILL CONV AUTH AMT	Billing Converted Authorization Amount		Authorization Transaction Amount converted to the currency of the assessed fee. Space Filled, left justified, and may contain an embedded decimal point based on the currency exponent (for example, 1234.56).
MIP OWNER ICA	MIP Owner ICA		Identifies the owner ICA of the MIP.
ADDTL RESP 1	Additional Response 1		Identifies the data element in error.
ADDTL RESP 2	Additional Response 2		Identifies the subelement in error. (Subelement for Single Message System is positions 4–5 with a leading zero.)
BILLING-EVENT	Billing Event		Identifies which fee was assessed. Left justified.

AB605010-FF Data File

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-complaint authorizations to report within a billing period, the data file format report (AB605010-FF) will be generated and include a trailer record with a record count of zero.

- Seven TKR8 bulk files are delivered each Monday following Sunday's weekly billing cycle. A separate file of non-compliant transactions is generated for each day (Sunday-Saturday) of the prior week containing non-compliant transactions.

Field Descriptions

The format and layout of the data file follows. It is a fixed format file, and all fields are delimited by ';'.

Field Name	Start	End	Length	Data Element (DE)	Field Description	Field Data Type
Cardholder Number	1	19	19	DE 2	Masked (obfuscated) PAN. First six and last four digits of the PAN will be shown (for example, 999999XXXXXX9999). Space filled, left justified.	Alphanumeric
Delimiter	20	20	1		All fields delimited by ";".	Alphanumeric
Authorization Transaction Amount	21	32	12	DE 4	Zero filled, right justified (for example, 00000001211).	Numeric
Delimiter	33	33	1		All fields delimited by ";".	Alphanumeric
Clearing Transaction Amount	34	45	12	DE 4	Zero filled, right justified (for example, 00000001211). Blank if not applicable for billing event.	Numeric
Delimiter	46	46	1		All fields delimited by ";".	Alphanumeric
Acquirer Institution ID	47	57	11	DE 32	Space filled, left justified (for example, 9744).	Alphanumeric
Delimiter	58	58	1		All fields delimited by ";".	Alphanumeric
POS Country	59	61	3	DE 61, subfield 13	Alpha country code.	Alphanumeric
Delimiter	62	62	1		All fields delimited by ";".	Alphanumeric

Field Name	Start	End	Length	Data Element (DE)	Field Description	Field Data Type
Forwarding Institution ID	63	73	11	DE 33	Zero filled, right justified (for example, 00000008434).	Numeric
Delimiter	74	74	1		All fields delimited by ";".	Alphanumeric
Authorization Date	75	82	8	DE 15	YYYYMMDD Derived YYYY, DE 15 MMDD	Alphanumeric
Delimiter	83	83	1		All fields delimited by ";".	Alphanumeric
Clearing Date	84	91	8	PDS 0158, subfield 5	YYYYMMDD Derived YYYY, PDS 0158 subfield 5 YYMMDD. Blank if not applicable for billing event.	Alphanumeric
Delimiter	92	92	1		All fields delimited by ";".	Alphanumeric
Merchant ID	93	107	15	DE 42	Space filled, left justified.	Alphanumeric
Delimiter	108	108	1		All fields delimited by ";".	Alphanumeric
Merchant Name Location	109	148	40	DE 43	Space filled, left justified.	Alphanumeric
Delimiter	149	149	1		All fields delimited by ";".	Alphanumeric
Authorization ID	150	155	6	DE 38		Alphanumeric
Delimiter	156	156	1		All fields delimited by ";".	Alphanumeric
Financial Network Code	157	159	3	DE 63, subfield 1		Alphanumeric
Delimiter	160	160	1		All fields delimited by ";".	Alphanumeric
Authorization Banknet Reference Number	161	169	9	DE 63, subfield 2	Left justified.	Alphanumeric
Delimiter	170	170	1		All fields delimited by ";".	Alphanumeric
Acceptance Brand	171	173	3			Alphanumeric
Delimiter	174	174	1		All fields delimited by ";".	Alphanumeric

Field Name	Start	End	Length	Data Element (DE)	Field Description	Field Data Type
Merchant Category Code	175	178	4	DE 18		Alphanumeric
Delimiter	179	179	1		All fields delimited by ";".	Alphanumeric
Point of Service Transaction Status	180	180	1	DE 61, subfield 7		Alphanumeric
Delimiter	181	181	1		All fields delimited by ";".	Alphanumeric
Final Authorization Indicator	182	182	1	DE 48, subelement 61, subfield 5		Alphanumeric
Delimiter	183	183	1		All fields delimited by ";".	Alphanumeric
Response Code	184	185	2	DE 39		Alphanumeric
Delimiter	186	186	1		All fields delimited by ";".	Alphanumeric
Authorization Currency Code	187	189	3	DE 49		Alphanumeric
Delimiter	190	190	1		All fields delimited by ";".	Alphanumeric
Clearing Currency Code	191	193	3	DE 49	Contains XXX if multiple clearing records are processed for a single authorization and one clearing record currency code differs from the authorization currency code. Otherwise, contains the clearing currency code of the last clearing record processed for the authorization. Blank if not applicable for billing event.	Alphanumeric
Delimiter	194	194	1		All fields delimited by ";".	Alphanumeric

Field Name	Start	End	Length	Data Element (DE)	Field Description	Field Data Type
Processing Code	195	196	2	DE 3, subfield 1		Alphanumeric
Delimiter	197	197	1		All fields delimited by ";".	Alphanumeric
Clearing Banknet Reference Number	198	206	9	DE 63, subfield 2	Space filled, left justified. Blank if not applicable for billing event.	Alphanumeric
Delimiter	207	207	1		All fields delimited by ";".	Alphanumeric
Clearing Match	208	208	1		Identifies if a matching clearing transaction was found for an authorization. Values are: • Y—Matching clearing found • N—Matching clearing not found • M—Multiple clearing records processed for a single authorization request • Blank—Not applicable for billing event	Alphanumeric
Delimiter	209	209	1		All fields delimited by ";".	Alphanumeric
Final Auth Reversal Indicator	210	210	1		Identifies if a final authorization was reversed, which resulted in a matching clearing transaction not being found for an authorization. • Y—Authorization was reversed • N—Authorization was not reversed • Blank—Not applicable for billing event	Alphanumeric
Delimiter	211	211	1		All fields delimited by ";".	Alphanumeric

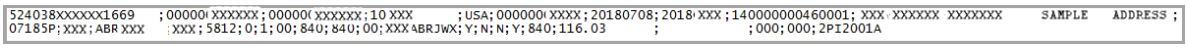
Field Name	Start	End	Length	Data Element (DE)	Field Description	Field Data Type
Currency Mismatch Indicator	212	212	1		Identifies if the authorization and clearing Transaction Currency Code (DE 49) are not the same. Values are: • Y—Authorization and clearing currencies do not match • N—Authorization and clearing currencies match • Blank—Not applicable for billing event	Alphanumeric
Delimiter	213	213	1		All fields delimited by ";".	Alphanumeric
Amount Mismatch Indicator	214	214	1		Identifies if the authorization and clearing Transaction Amount (DE 4) are not the same. Values are: • Y—Authorization and clearing currencies do not match • N—Authorization and clearing currencies match • Blank—Not applicable for billing event	Alphanumeric
Delimiter	215	215	1		All fields delimited by ";".	Alphanumeric
Billing Currency Code	216	218	3		Identifies the currency code of the assessed fee.	Alphanumeric
Delimiter	219	219	1		All fields delimited by ";".	Alphanumeric

Field Name	Start	End	Length	Data Element (DE)	Field Description	Field Data Type
Billing Converted Authorization Amount	220	231	12		Authorization Transaction Amount converted to the currency of the assessed fee. Space filled, left justified, and may contain an embedded decimal point based on the currency exponent (for example, 1234.56).	Alphanumeric
Delimiter	232	232	1		All fields delimited by ";".	Alphanumeric
MIP Owner ICA	233	243	11	N/A	Space filled, left justified (for example, 9744) Blank if not applicable for billing event.	Numeric
Delimiter	244	244	1		All fields delimited by ";".	Alphanumeric
Additional Response 1	245	247	3	DE 44, pos 1–3	Data Element Error Blank if not applicable for billing event.	Numeric
Delimiter	248	248	1		All fields delimited by ";".	Alphanumeric
Additional Response 2	249	251	3	DE 44, pos 4–6	Subelement Error (Subelement for Single Message System is pos 4–5 with a leading zero.) Blank if not applicable for billing event.	Numeric
Delimiter	252	252	1		All fields delimited by ";".	Alphanumeric
Billing Event	253	263	11		Identifies which fee was assessed. Left justified.	Alphanumeric
Filler	264	300	37		Blanks	Alphanumeric

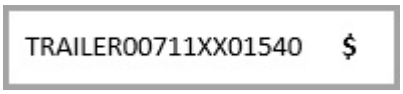
AB605010-FF File Trailer

Field Name	Start	End	Length	Data Element (DE)	Field Description	Field Data Type
Record Type	1	7	7		Identifies the trailer record. Contains the value TRAILER.	Alphanumeric
Endpoint	8	14	7		ID of the endpoint to which the bulk file was delivered.	Alphanumeric
Record Count	15	26	12		Count of transaction detail records included in the bulk file. Space filled, left justified.	Alphanumeric
Filler	27	300	274		Blanks	

Sample Detail Record



Sample Trailer Record



NOTE: $ symbol is used above just to indicate the end of the record for understanding purpose. The actual record will not contain a $ symbol to indicate end of the record but will have a hidden new line character.

Authorization Parameter Summary Report (SI737010-AA)

An overview of the Authorization Parameter Summary Report (SI737010-AA) is listed in table format.

Title	Authorization Parameter Summary Report

Generated by	Mastercard Authorization Platform
Purpose	To provide customers with a list of authorization parameters.
Description	This report includes a comprehensive list of the parameters that the customer uses. It includes global parameters and Stand-In parameters. Mastercard provides updates to this report when customers' parameters change.
Frequency	Weekly
Distribution Methods	Paper (Sent to the authorization contact established on the Principal Member Questionnaire); Mastercard eService, Mastercard File Express, complex-to-complex, bulk ID (T300)

Report Sample

Report sample of the Authorization Parameter Summary Report (SI737010-AA).

```
SI737010-AA                                  MASTERCARD INTERNATIONAL                                  RUN DATE   10/28/13
ICA:             999999                  AUTHORIZATION PARAMETER SUMMARY REPORT                          PAGE:         1
ACQUIRER PARAMETERS N/A
ISSUER PARAMETERS

ACCOUNT RANGE: FROM: 5XXXXXXX000
               THRU: 5XXXXXXX999
                                              GLOBAL PARAMETERS
-------------------------------------------------------------------------------------------------------------------------
PRODUCT CODE            CARDHOLDER BILLING     CVC2 PARTICIPANT         AVS LEVEL PARTICIPANT       RPCS PARTICIPANT    PAN MAPPING
                         CURRENCY CODE                                                                                  PARTICIPANT
 MCP                           840                  N                        1                          N              N
-------------------------------------------------------------------------------------------------------------------------
EXPIRATION DATE PARTICIPANT        POS BALANCE INQUIRY PARTICIPANT        ACQUIRER REVERSAL MESSAGE PARTICIPATION
          N                                 N                          Y - ISSUER RECEIVES THE 0400 MESSAGE
-------------------------------------------------------------------------------------------------------------------------
REAL-TIME SUBSTANTIATION PARTICIPANT                            INCONTROL REAL CARD SPEND CONTROL
          N                                                                 N
-------------------------------------------------------------------------------------------------------------------------
RECEIVE SETTLEMENT AMOUNTS        MPG BLOCKING PARTICIPANT        OPTIONAL NON-VALID CVC3 PROCESSING        CVC3 TRUNCACTION IND
          N                                 N
-------------------------------------------------------------------------------------------------------------------------
ISSUER PIN BLOCK FORMAT CODE        BANKNET PIN PROCESSING        PVV ON-FILE-PARTICIPATION         MASTERCARD INCONTROL MAPPING
          01                                M                              NO                                  N
-------------------------------------------------------------------------------------------------------------------------
MERCHANT VERIFICATION SERVICE     MASTERCARD ONLINE CHECKOUT SERVICE     ADC EVENT PARTICIPATION     TPP IDENTIFICATION SERVICE
             N                                 N                                N                             N
-------------------------------------------------------------------------------------------------------------------------
INCONTROL FLEX CARD             INCONTROL ENHANCED ROUTING        MONEYSEND BLOCKING        PAY WITH REWARDS       IPC FRAUD CONTROL
          N                                 N                              Y                         N                    Y
-------------------------------------------------------------------------------------------------------------------------
STAND-IN PIN VERIFICATION BYPASS          MASTERCARD DIGITAL ENABLEMENT SERVICE PARTICIPATION
          Y                                                 Y

-------------------------------------------------------------------------------------------------------------------------
IN-FLIGHT COMMERCE BLOCKED RANGE

-------------------------------------------------------------------------------------------------------------------------
PAYMENT TRANSACTION BLOCKED RANGE

-------------------------------------------------------------------------------------------------------------------------
TRANSACTION BLOCKING SERVICE

-------------------------------------------------------------------------------------------------------------------------
GARS PARTICIPANT                   AUTHORIZATION REFERRAL                  INTERNATIONAL GARS                   SECURITY NUMBER
       Y                               00000000000
-------------------------------------------------------------------------------------------------------------------------
 LOST/STOLEN                           CUSTOMER SERVICE


-------------------------------------------------------------------------------------------------------------------------
```

```
SI737010-AA                                    MASTERCARD INTERNATIONAL                                    RUN DATE   10/28/13
ICA:            999999                    AUTHORIZATION PARAMETER SUMMARY REPORT                            PAGE:        2
ACQUIRER PARAMETERS N/A
ISSUER PARAMETERS

ACCOUNT RANGE: FROM: 5XXXXXXX000              THRU: 5XXXXXXX999
                                                STAND-IN PARAMETERS
-------------------------------------------------------------------------------------------------------------------------------
                                                HOURS OF OPERATION:
UTC. OFFSET: 0000 + OR - +    D.S.T.  START DATE: 000000  TIME: 0000
                                      END DATE:   000000  TIME: 0000

LOCAL TIME    OPEN  CLSE    OPEN  CLSE    OPEN  CLSE
       SUN    0000  2400    0000  0000    0000  0000
       MON    0000  2400    0000  0000    0000  0000
       TUE    0000  2400    0000  0000    0000  0000
       WED    0000  2400    0000  0000    0000  0000
       THU    0000  2400    0000  0000    0000  0000
       FRI    0000  2400    0000  0000    0000  0000
       SAT    0000  2400    0000  0000    0000  0000

-------------------------------------------------------------------------------------------------------------------------------
                                          HOLIDAYS FOR CALL REFERRAL CENTER:

     DATE      OPEN  CLSE    OPEN  CLSE                          DATE      OPEN  CLSE    OPEN  CLSE
01. N/A        N/A   N/A     N/A   N/A                    14.   N/A       N/A   N/A     N/A   N/A
02. N/A        N/A   N/A     N/A   N/A                    15.   N/A       N/A   N/A     N/A   N/A
03. N/A        N/A   N/A     N/A   N/A                    16.   N/A       N/A   N/A     N/A   N/A
04. N/A        N/A   N/A     N/A   N/A                    17.   N/A       N/A   N/A     N/A   N/A
05. N/A        N/A   N/A     N/A   N/A                    18.   N/A       N/A   N/A     N/A   N/A
06. N/A        N/A   N/A     N/A   N/A                    19.   N/A       N/A   N/A     N/A   N/A
07. N/A        N/A   N/A     N/A   N/A                    20.   N/A       N/A   N/A     N/A   N/A
08. N/A        N/A   N/A     N/A   N/A                    21.   N/A       N/A   N/A     N/A   N/A
09. N/A        N/A   N/A     N/A   N/A                    22.   N/A       N/A   N/A     N/A   N/A
10. N/A        N/A   N/A     N/A   N/A                    23.   N/A       N/A   N/A     N/A   N/A
11. N/A        N/A   N/A     N/A   N/A                    24.   N/A       N/A   N/A     N/A   N/A
12. N/A        N/A   N/A     N/A   N/A                    25.   N/A       N/A   N/A     N/A   N/A
13. N/A        N/A   N/A     N/A   N/A                    26.   N/A       N/A   N/A     N/A   N/A
-------------------------------------------------------------------------------------------------------------------------------
SI737010-AA                                    MASTERCARD INTERNATIONAL                                    RUN DATE   10/28/13
ICA:            999999                    AUTHORIZATION PARAMETER SUMMARY REPORT                            PAGE:        3
ACQUIRER PARAMETERS N/A
ISSUER PARAMETERS

ACCOUNT RANGE: FROM: 5XXXXXXX000
               THRU: 5XXXXXXX999
                                                STAND-IN PARAMETERS
-------------------------------------------------------------------------------------------------------------------------------
                                                DECISION MATRIX:
OPEN  SIGNED-IN:    ACCOUNT FILE        TRANSACTION        ACCUMULATIVE       PREMIUM
                          N                   N                  N               N
OPEN  SIGNED-OUT:   ACCOUNT FILE        TRANSACTION        ACCUMULATIVE       PREMIUM
                          N                   N                  N               N
CLOSED SIGNED-IN:   ACCOUNT FILE        TRANSACTION        ACCUMULATIVE       PREMIUM
                          N                   N                  N               N
CLOSED SIGNED-OUT:  ACCOUNT FILE        TRANSACTION        ACCUMULATIVE       PREMIUM
                          N                   N                  N               N

-------------------------------------------------------------------------------------------------------------------------------
    CARD LEVEL SUPPORT PARTICIPANT     MULTI-CURRENCY LIMITS PARTICIPANT        STAND-IN PIN RETRIES
              N                                 N                                    00000
-------------------------------------------------------------------------------------------------------------------------------
STORE AND FORWARD CONTROLS
DELIVERY TYPE:                        SOLICITED
ADVICE RESPONSE WAIT TIME:            035 SECONDS
AUTOMATIC DELETION OPTION:            Y
NO RESPONSE RESEND LIMIT:             00

-------------------------------------------------------------------------------------------------------------------------------
```

```
SI737010-AA                                    MASTERCARD INTERNATIONAL                                RUN DATE   10/28/13
ICA:            999999                  AUTHORIZATION PARAMETER SUMMARY REPORT                          PAGE:          4
ACQUIRER PARAMETERS N/A
ISSUER PARAMETERS

ACCOUNT RANGE: FROM: 5XXXXXXX000
               THRU: 5XXXXXXX999
-------------------------------------------------------------------------------------------------------------------------------
                                          TRANSACTION PROCESSING PARAMETERS:

    TARGET        PROMO     CAT     PRODUCT    MCC/TCC   CURRENCY
    COUNTRY       CODE     LEVEL      ID                  CODE
    GLOBAL       ******      *        CBP        TCC      840

TCC VALUES              CARD PRESENT     CARD NOT PRESENT
T - MAIL/PHONE                 0                0
R - RETAIL                   110                0
F - RESTAURANT               110                0
O - COLLEGE/HOSPITAL           0                0
H - HOTEL/MOTEL              110                0
A - AUTOMOBILE               110                0
X - OTHER TRANSPORT            0                0
Z - ATM                        0                0
U - UNIQUE                     0                0
C - CASH ADVANCE               0                0
P - PAYMENT                    0                0
SI737010-AA                                    MASTERCARD INTERNATIONAL                                RUN DATE   10/28/13
ICA:            999999                  AUTHORIZATION PARAMETER SUMMARY REPORT                          PAGE:          5
ACQUIRER PARAMETERS N/A
ISSUER PARAMETERS

ACCOUNT RANGE: FROM: 5XXXXXXX000
               THRU: 5XXXXXXX999
-------------------------------------------------------------------------------------------------------------------------------
                                PRODUCT GRADUATION TRANSACTION LIMITS PROCESSING PARAMETERS :

   TARGET        PROMO     CAT     PRODUCT    MCC/TCC   CURRENCY   CSI
   COUNTRY       CODE     LEVEL      ID                  CODE      CODE
   000          MCGARS      *        ***        TCC      840      *******

TCC VALUES              CARD PRESENT     CARD NOT PRESENT
T - MAIL/PHONE                150              150
R - RETAIL                    500              500
F - RESTAURANT                225              225
O - COLLEGE/HOSPITAL          450              450
H - HOTEL/MOTEL               750              750
A - AUTOMOBILE                375              375
X - OTHER TRANSPORT          1125             1125
Z - ATM                         0                0
U - UNIQUE                    150              150
C - CASH ADVANCE              200              200
P - PAYMENT                     0                0
```

```
SI737010-AA                                    MASTERCARD INTERNATIONAL                                    RUN DATE   10/28/13
ICA:          999999          PRODUCT GRADUATION LIMITS AUTHORIZATION PARAMETER SUMMARY                        PAGE:          6
ISSUER PARAMETERS

ACCOUNT RANGE: FROM: 5XXXXXXX999                  CSI CODE: *******
               THRU: 5XXXXXXX000
-------------------------------------------------------------------------------------------------------------------------------
                                                ACCUMULATIVE LIMITS:
CURRENCY CODE: 840
DAYS          COUNT            AMOUNT
 01             1                50
 02             1               100
 03             1               150
 04             1               200

CASH ADVANCE:   DAYS            AMOUNT
                  0                0

                                             PREMIUM ACCUMULATIVE LIMITS:
CURRENCY CODE: 840
DAYS          COUNT            AMOUNT
 01             1                0
 02             1                0
 03             1                0
 04             1                0

CASH ADVANCE:   DAYS            AMOUNT
                  0                0

-------------------------------------------------------------------------------------------------------------------------------
                                                PREMIUM CONTROLS
 DAYS     COUNT
   4       999

 -----------------------------------------------------------------------------------------------------------------------------
                                                LIMIT 1 PROCESSING
           MAIL/TELEPHONE:          150
           TRAVEL:                   25
           CASH-DISBURSEMENT:        50
           RETAIL:                  100
           NTH TRANSACTION:           3
 -----------------------------------------------------------------------------------------------------------------------------
                                                ON-BEHALF SERVICES
              DESCRIPTION
              PIN VERIFICATION IN STAND-IN
              PIN PRE-VERIFICATION
              CVC1 VERIFICATION IN STAND-IN
              PAYPASS CVC3 PRE-VALIDATION
              PAYPASS CVC3 VALIDATION IN STAND-IN
              PAYPASS DYNAMIC CVC3 PRE-VALIDATION
              PAYPASS DYNAMIC CVC3 VALIDATION IN STAND-IN
              M/CHIP CRYPTOGRAM PRE-VALIDATION SERVICE
              M/CHIP CRYPTOGRAM VALIDATION IN STAND-IN
              SECURECODE AAV PRE-VERIFICATION
              SECURECODE AAV VERIFICATION IN STAND-IN
```

Field Descriptions

The fields on the Authorization Parameter Summary Report (SI737010-AA) are listed in table format.

The Authorization Parameter Summary Report (SI737010-AA) includes:

- Header Information
- Global Parameters
- Stand-In Parameters

NOTE: Mastercard provides an updated version of this report for customers when their parameters change.

Header Information

The header information fields in the Authorization Parameter Summary Report (SI737010-AA) are listed in table format.

The Authorization Parameter Summary Report (SI737010-AA) header information includes the following data.

ICA	Unique six-digit ID number assigned by Mastercard to identify a customer or processing end-point (Sequenced by ICA).
Acquirer Parameters—N/A	For future use.
Issuer Parameters	All parameters relating to that issuer.
Account Range	Range of accounts within From…Thru. These range numbers are associated with the customer's ICA number.
From: Thru:	Range of account numbers for the issuer's parameters. The report shows the first 19 digits of each range.

Global Parameters

The Global Parameters fields on the Authorization Parameter Summary Report (SI737010-AA) are listed in table format.

The Authorization Parameter Summary Report (SI737010-AA) global parameters may include the following data.

Field	Description
Product Code	Three-position field that identifies Financial Network Code.
Cardholder Billing Currency Code	Three-digit number that identifies the participant's currency code.
CVC 2 Participant	A one-character flag that indicates whether a customer participates in CVC 2. CVC 2 is a three-digit numeric character code that is indent-printed into the signature panel in the back of a card. • Y—Customer participates in CVC 2. • N—Customer does not participate in CVC 2.

Field	Description
AVS Level Participant	A one-position field that indicates a customer's AVS service level. • 0—AVS not supported. • 1—Issuer provides AVS, receives full address data. • 2—Issuer provides AVS, receives condensed address data. This level supports the algorithm that uses the first five numeric digits in an address (when scanning the address from left to right). • 3—Issuer provides AVS, receives condensed address data. This level supports the algorithm that uses the first five numeric digits in an address. This algorithm stops searching for numbers after it encounters an alphabetic character or space (when scanning the address from left to right). • 4—Issuer provides AVS, receives condensed postal/ZIP code and address data. This level supports the algorithm that uses only numeric digits (with a maximum of nine digits) in the cardholder postal/ZIP code, and the first five numeric digits in an address (when scanning the address from left to right).
Payment Cancellation Participant	A one-character flag that indicates whether a customer participates in Payment Cancellation. • Y—Customer participates in Payment Cancellation • N—Customer does not participate in Payment Cancellation
PAN Mapping Participant	A one-character flag that indicates whether a customer participates in the Contactless Mapping Service. • Y—Customer participates in the Contactless Mapping Service. • N—Customer does not participate in the Contactless Mapping Service.
Expiration Date Participant	A one-character flag that indicates whether a customer participates in the Expired Card Override service. • Y—Customer participates in the Expired Card Override service. • N—Customer does not participate in the Expired Card Override service.
POS Balance Inquiry Participant	A one-character flag that indicates whether the account range participates in POS balance inquiries. • Y—Account range participates in POS balance inquiries. • N—Account range does not participate in POS balance inquiries.

Field	Description
Acquirer Reversal Message Participation	A one-character flag that indicates whether the issuer participates in the reversal request message functionality. • Y—Issuer receives the 0400 message. • N—Issuer does not receive the 0400 message.
Real-time Substantiation	A one-character flag that indicates whether the issuer supports real-time substantiation at the POS. • Y—Issuer supports real-time substantiation. • N—Issuer does not support real-time substantiation.
In Control Real Card Spend Control	A one-character flag that indicates whether the issuer participates in the Consumer Controls services. • Y—Issuer participates in Consumer Controls services. • N—Issuer does not participate in Consumer Controls services.
Mastercard Spend Alerts Service	A one-character flag that indicates whether the issuer participates in the Mastercard Spend Alerts Service. • Y—Issuer participates in Mastercard Spend Alerts Service. • N—Issuer does not participate in Mastercard Spend Alerts Service.
Mastercard Spend Controls Service	A one-character flag that indicates whether the issuer participates in the Mastercard Spend Controls Service. • Y—Issuer participates in Mastercard Spend Controls Service. • N—Issuer does not participate in Mastercard Spend Controls Service.
Receive Settlement Amounts	A one-character flag that indicates whether the issuer receives settlement amount-related data elements. • Y—Issuer receives settlement amount-related data elements. • N—Issuer does not receive settlement amount-related data elements.
MPG Blocking Participant	A one-character flag that indicates whether the issuer participates in the Mastercard Payment Gateway (MPG) Authorization Blocking service. • Y—Issuer participates in the MPG Blocking service. • N—Issuer does not participate in the MPG Blocking service.

Field	Description
Optional Non-Valid CVC 3 Processing	A one-character flag that indicates whether the issuer participates in Optional Non-Valid CVC 3 Processing. • Y—Issuer participates in the Optional Non-Valid CVC 3 Processing. • N—Issuer does not participate in the Optional Non-Valid CVC 3 Processing.
CVC 3 Truncation Ind	A one-character flag that indicates whether the CVC 3 transaction is valid—that is, the value in DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), subfield 2 (On-behalf [OB] Result 1). This indicator is available to issuers participating in the Non-Valid CVC Processing option and participating in one of the CVC 3 services. • Y—CVC 3 transaction is valid. • N—CVC 3 transaction is not valid.
Issuer PIN Block Format Code	Applies only to the Europe region. A two-position field that indicates the issuer's PIN block format. • 01 = ANSI 1 • 02 = ANSI 2 • 03 = ANSI 2 • 10 = ISO Format 0 • 11 = ISO Format 1 • 19 = ISO Format 0 or ISO Format 1
Banknet PIN Processing	A one-position field that indicates the service platform on which an issuer's PIN processing will be performed. • B = Banknet PIN processing • M = MDS PIN processing

Field	Description
PVV On-File Participation	Applies only to the Europe region. Supports PIN Validation using PVV on-file that issuers submit as basis to override PVV data provided in the card's magnetic stripe. Valid values are as follows: • No = Does not participate in PVV/PIN Offset on File service. • Optional = On File, the Authorization Platform retrieves the PVV value. If the PVV value is found, validates using that value. If the PVV value is not found, the data in the track is used. • Mandatory = On File, the Authorization Platform uses the data on file if found to validate the PIN. If the PVV value is not found, PIN validation indicates mandatory PVV not on file as result.
Mastercard In Control Mapping	A one-character flag that indicates whether the issuer participates in the Mastercard In Control™ service. • Y—Issuer participates in the Mastercard In Control service. • N—Issuer does not participate in the Mastercard In Control service.
Mastercard Online Checkout Service	A one-character flag that indicates whether the issuer participates in Mastercard online checkout service. N—Issuer does not participate in Mastercard online checkout service.
ADC Event Participation (Account Data Compromise)	A one-character flag that indicates whether compromised event data has been found. • Y—Compromised Event Data Found. • N—Compromised Event Data Not Found.
TPP Identification Service	A one-character flag that indicates whether the issuer participates in the Third Party Processor (TPP) service. • Y—Issuer participates in the TPP service. • N—Issuer does not participate in the TPP service.

Field	Description
MoneySend Blocking	A one-character flag that identifies whether a receiving financial institution (RFI) account range is blocked from processing transactions via the MoneySend platform. • Y—MoneySend Payment Transactions are not allowed because the country, RFI, or RFI's account range associated with the ICA/account range is blocked from processing transactions via the MoneySend platform. • N—MoneySend Payment Transactions are allowed to the ICA/account range.
IPC Fraud Control	A one-character flag that indicates whether the issuer participates in IPC Fraud Control service. • Y—Issuer participates in the IPC Fraud Control service. • N—Issuer does not participate in the IPC Fraud Control service.
Receive ATM Additional Data	Applies only to the Europe region. A one-character flag that indicates support of ATM additional data in DE 48, subelement 58 (ATM Additional Data) by customers participating in the Sweden Domestic Authorization Switching Service (SASS). • Y—Issuer supports ATM additional data in DE 48, subelement 58. • N—Issuer does not support ATM additional data in DE 48, subelement 58.
PIN Management Participant	A one-character flag that indicates whether the issuer participates in the Chip PIN Management service. • Y—Issuer participates in the PIN Management service. • N—Issuer does not participate in the PIN Management service.
Domestic Debit ATM Processing	A one-character flag that indicates whether the issuer participates in domestic Debit ATM processing. • Y—Issuer participates in the domestic Debit ATM processing. • N—Issuer does not participate in the domestic Debit ATM processing.
In-Flight Commerce Blocked Range	Two 19-digit account range numbers that indicate the from and the to account ranges to block for in-flight commerce service. In-flight commerce (IFC) is a service that identifies transactions conducted via interactive video terminals by passengers on a long-distance airplane flight.

Field	Description
Stand-In PIN Verification Bypass	A one-character flag indicating whether the Stand-In System will bypass or perform a PIN Verification Test. Issuers that want Stand-In to perform this test are required to participate in a PIN validation service. • Y—Stand-In System will bypass PIN Verification Test. • N—Stand-In System will perform PIN Verification Test.
MDES Participation	A one-character flag indicating whether the issuer participates in MDES. • Y—Issuer participates in MDES. • N—Issuer does not participate in MDES.
Payment Transaction Blocked Range	Two 19-digit numeric account range numbers that indicate the from and the to account ranges to block for this transaction type. A Payment Transaction is a transaction in which a Payment Service Provider facilitates the transfer of funds to an issuer for posting to a cardholder's Mastercard account.
MIP Transaction Blocking Service	MIP Transaction Blocking is a service that enables an issuer to decline specified types of transaction requests by issuer ICA number or account range, in combination with additional transaction parameters.
Range From Range To	Two 11-digit account range numbers that indicate the from and the to account ranges to block for the MIP Transaction Blocking service.
Response Code	Indicates the response code applicable to the transaction block, based on the response codes available for the Authorization Request Response/0110 message. The following list identifies the valid response code values: • 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)

Field	Description
Scope	Indicates whether transactions are blocked for all routes or transactions are only blocked from going to the Stand-In System when the issuer is unavailable. • All • Stand-In
Blocking Criteria	Transaction blocking criteria. Indicates that transactions will be blocked based on 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 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]) In the first example, the report sample shows that the Merchant Type, value 5555 is the transaction blocking criteria; in the second example, POS Terminal PAN Entry Mode, value 02 is the transaction blocking criteria.
GARS Participant	A one-character flag that indicates whether the customer is a Global Automated Referral System (GARS) participant. • Y—Customer participates in the GARS service. • N—Customer does not participate in the GARS service.
Authorization Referral	Indicates the phone number GARS uses to contact the issuer on domestic-call referral responses.
International GARS	Indicates the phone number GARS uses to contact the issuer on international call referral responses.
Security Number	This phone number is not displayed.
Lost/Stolen	This phone number is not displayed.
Customer Service	This phone number is not displayed.

Stand-In Parameters

Descriptions of the Stand-In Parameter fields in the Authorization Parameter Summary Report (SI737010-AA).

The Authorization Parameter Summary Report (SI737010-AA) Stand-In parameters include the following data.

Field	Description
Hours of Operation	Indicates the hours of operations for the issuer's authorization system.
UTC Offset	Time difference between the customer's local time and Coordinated Universal Time (UTC—formerly GMT [Greenwich mean time]). UTC Offset represents whether the local time is ahead (+) or behind (-) UTC by the number of hours indicated in the UTC Offset field.
D.S.T.	Daylight Saving Time (D.S.T.) represents the daylight-saving time start and end dates and times for the customer.
Local Time	Indicates the open and close local time for the customer.
Holidays for Call Referral Center	Definition of 26 holidays for the issuer's Call Referral Center, with up to two openings and closings per holiday.
Decision Matrix	A matrix that contains values that represent a customer's choice of Stand-In processing responses to transactions if a transaction goes to Stand-In processing in a given state. • C—Call referral • N—Decline • A—Continue with Stand-In processing • P—Capture card
Open Signed In, Closed Signed In	Indicates times when the issuer's authorization center is open versus when it is closed.
Open Signed Out, Closed Signed Out	Indicates times when the issuer's authorization center is signed in versus when it is signed out (for online issuers).
Card Level Support Participant	A one-character flag that indicates if the customer is a Card Level Support participant. • Y—Customer participates in Card Level Support. • N—Customer does not participate in Card Level Support.

Field	Description
Multi-Currency Limits Participant	A one-character flag that indicates if the customer participates in multi-currency limits in Stand-In processing. • Y—Customer participates in multi-currency limits. • N—Customer does not participate in multi-currency limits.
Stand-In PIN Retries	Applies only to the Europe region. Indicates the number of invalid PIN attempts allowed using a value of 1–5. This parameter applies only to the Online PIN Validation in Stand-In.
Store-and-Forward (SAF) Controls	Additional parameters by which issuers can receive their SAF messages.
Delivery Type	Unsolicited—Issuer receives SAF messages after signing on to the Mastercard Network using a Network Management Request/0800 message containing DE 70 (Network Management Information), value 001 (Sign-on [by BIN]) or value 061 (Group sign on [by Mastercard group sign on]).
Number of Simultaneous Sessions	Represents the Number of Simultaneous Advice Messages that can be processed simultaneously. There is a maximum of 10 advice messages that can be processed simultaneously. Default is 10.
Advice Response Wait Time	Advice response wait time in seconds (30–180 seconds) before SAF session termination (Default is 30 seconds).
Automatic Deletion Option	Indicates whether the Stand-In System should delete the SAF message from the SAF queue when the Stand-In System processing exceeds the number of times the issuer requested Stand-In to resend a SAF message when no response is received from the issuer. The Stand-In System will attempt to resend the SAF message from the SAF queue until a response is received, the resend limit has been reached, or the advice is on file for four days (Default is No).
No Response Resend Limit	Number of times (1–20) that the Stand-In System attempts to resend a SAF message without response from the issuer before auto-deleting SAF messages. If Automatic Deletion Option is selected, default is 3.
Transaction Processing Parameters	This section of the report depends on the number of rules that apply to a customer. The report reflects all rules that apply to that particular customer.

Field	Description
Target Country	Indicates the acquirer country for which the limits are applied. Mastercard has established minimum and maximum values for certain parameters. Mastercard will set the minimum limits as default values to establish customer's limits. • Foreign Default—Established limits outside of the country of issuance. • Global—Established limits for all customers by product code, MCC, and/or CAT level.
Promo Code (Promotion Code)	Indicates the promotion code for which the limits are applied. Lists the six-character alphanumeric codes that an issuer establishes to identify transactions that meet requirements for an issuer's promotional program for a card range.
CAT Level	Lists a one-character numeric code that identifies transactions that occur at a CAT. A CAT is a cardholder-activated terminal that is usually unattended and accepts payment cards, debit, charge, and proprietary cards for a card range. CATs are defined by levels. • 0—Not a CAT transaction • 1—Automated dispensing machines with PIN • 2—Self-service terminals • 3—Limited-amount terminals • 4—In-flight commerce terminals • 6—Electronic commerce • 7—Transponder
Product ID	Lists the three-character code that identifies the type of card program for an account, such as Gold Mastercard® card.
MCC/TCC	Lists the card acceptor business code (MCC) and the transaction category code (TCC) for which limits are applied.
Currency Code	Three-digit number that identifies the customer's chosen currency code for amount limits.
Card Present Amount	Transaction amount limit when a card is present.
Card Not Present Amount	Transaction amount limit when a card is not present.

Field	Description
Product Graduation Transaction Limits Processing Parameters	This section of the report depends on whether the account range has product graduated limits. If the account range does not have product graduated limits, this section does not display. For each account range that contains product graduated cards to which a Customer Specific Index (CSI) is assigned, a set of Stand-In processing limits for accounts that are registered to participate in Product Graduation displays.
Target Country	Indicates the acquirer country for which the limits are applied. Mastercard has established minimum and maximum values for certain parameters. Mastercard will set the minimum limits as default values to establish customer's limits. • Foreign Default—Established limits outside of the country of issuance. • Global—Established limits for all customers by product code, MCC, and/or CAT level.
Promo Code (Promotion Code)	Indicates the promotion code for which the limits are applied. Lists the six-character alphanumeric codes that an issuer establishes to identify transactions that meet requirements for an issuer's promotional program for a card range.
CAT Level	Lists a one-character numeric code that identifies transactions that occur at a CAT. A CAT is a cardholder-activated terminal that is usually unattended and accepts bankcards, debit, charge, and proprietary cards for a card range. CATs are defined by levels. • 0—Not a CAT transaction • 1—Automated dispensing machines with PIN • 2—Self-service terminals • 3—Limited-amount terminals • 4—In-flight commerce terminals • 6—Electronic commerce • 7—Transponder
Product ID	Lists the three-character code that identifies the type of card program for an account, such as Gold Mastercard® card.
MCC/TCC	Lists the card acceptor business code (MCC) and the transaction category code (TCC) for which limits are applied.
Currency Code	Three-digit number that identifies the customer's chosen currency code for amount limits.

Field	Description
CSI Code	Seven-position alphanumeric value that is provided when registering accounts for Product Graduation.
Card Present Amount	Transaction amount limit when a card is present.
Card Not Present Amount	Transaction amount limit when a card is not present.
Product Graduation Limits Authorization Parameter Summary	This section of the report depends on whether the account range has product graduated limits. If the account range does not have product graduated limits, this section does not display. For each account range that contains product graduated cards to which a Customer Specific Index (CSI) is assigned, a set of Stand-In processing limits for accounts that are registered to participate in Product Graduation displays.
CSI Code	Seven-position alphanumeric value provided when registering accounts for Product Graduation.
Accumulative Limits	Four-day accumulative day and amount limits established by the issuer. The accumulation limits are for the number of transactions and amounts. Stand-In processing will not approve any amount that raises the accumulative amount already approved above the specified limit for the specified period of days.
Currency Code	Three-digit number that identifies the customer's chosen currency code for amount limits.
Premium Controls	Indicates specific limits that Stand-In processing applies to accounts listed in the Account File as Premium Listings. The Premium Listings designation is a method of identifying cardholder accounts that should have higher authorization limits than standard limits for the card type. During the Accumulative Limits test for Premium accounts, Stand-In processing applies the Days and Count Limit parameters.
Group and Series	Identifies a range of card account numbers listed in the Electronic Warning Bulletin file submitted by Mastercard on behalf of an issuer to the Account Management System for the purpose of notifying a merchant to capture any card bearing an account number that falls within that range.

Field	Description
Stand-In Blocked Range	Identifies a range of card numbers within a BIN that have not been issued to cardholders or card ranges previously blocked and should be unblocked. Range Blocking only applies for transactions processed by Stand-In. Card numbers within blocked ranges do not automatically appear in the Account Management System (AMS) Electronic Warning Bulletin file.
On-behalf Services	Lists the on-behalf service description for the on-behalf services that are enabled for an account range. There is a maximum of 10 on-behalf services.

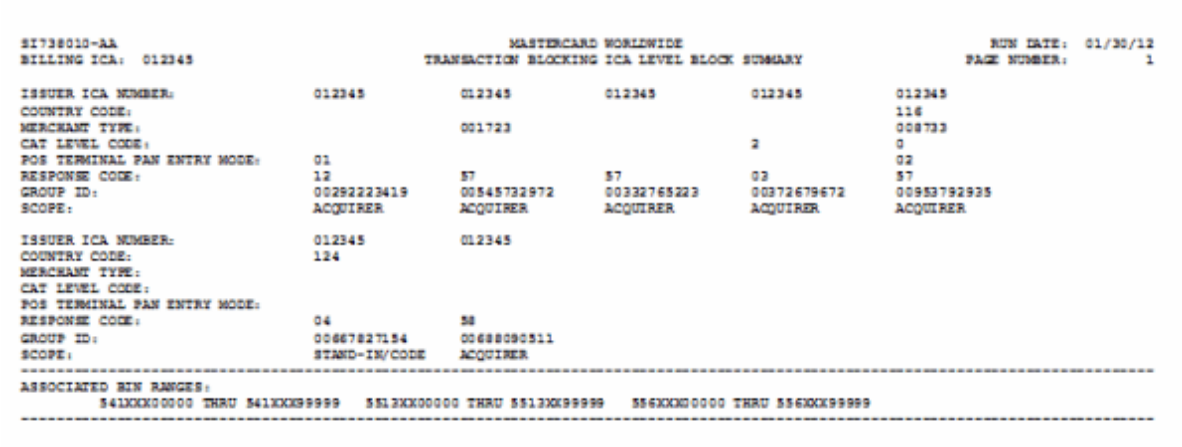
MIP Transaction Blocking ICA Level Block Summary (SI738010–AA)

An overview of the MIP Transaction Blocking ICA Level Block Summary (SI738010–AA) is listed in table format.

Title	MIP Transaction Blocking ICA Level Block Summary
Generated by	Mastercard Authorization Platform
Purpose	To provide customers with a tool to identify all BINs that are associated with ICAs that are subscribed to the MIP Transaction Blocking Service.
Description	This report includes a comprehensive list of the parameters for each BIN when the MIP Transaction Blocking Service is invoked at the ICA level. Mastercard provides updates to this report when customers' parameters change.
Frequency	Weekly
Distribution Methods	Paper (Sent to the authorization contact established on the Principal Member Questionnaire); Mastercard eService, Mastercard File Express, complex-to-complex, bulk ID (T300)

Report Sample

Report sample of the MIP Transaction Blocking ICA Level Block Summary (SI738010-AA) report.



```
SI738010-AA                                MASTERCARD WORLDWIDE                                RUN DATE:  01/30/12
BILLING ICA:  012345                TRANSACTION BLOCKING ICA LEVEL BLOCK SUMMARY              PAGE NUMBER:        1

ISSUER ICA NUMBER:          012345          012345          012345          012345          012345
COUNTRY CODE:                                                                               116
MERCHANT TYPE:                              001723                                          008733
CAT LEVEL CODE:                                                             2               0
POS TERMINAL PAN ENTRY MODE:  01                                                            02
RESPONSE CODE:              12              57              57              03              57
GROUP ID:                   00292223419     00545732972     00332765223     00372679672     00953792935
SCOPE:                      ACQUIRER        ACQUIRER        ACQUIRER        ACQUIRER        ACQUIRER

ISSUER ICA NUMBER:          012345          012345
COUNTRY CODE:               124
MERCHANT TYPE:
CAT LEVEL CODE:
POS TERMINAL PAN ENTRY MODE:
RESPONSE CODE:              04              58
GROUP ID:                   00667827154     00688090511
SCOPE:                      STAND-IN/CODE   ACQUIRER
-------------------------------------------------------------------------------------------------------------------------
ASSOCIATED BIN RANGES:
        541XXX00000 THRU 541XXX99999   551XXX00000 THRU 551XXX99999   556XXX00000 THRU 556XXX99999
-------------------------------------------------------------------------------------------------------------------------
```

Field Descriptions

The fields on the MIP Transaction Blocking ICA Level Block Summary (SI738010–AA) report are listed in table format.

Field	Description
Billing ICA	ICA that is billed for the Issuer ICA Number Transaction Blocking Service activity. This ICA may be the same or different than the Issuer ICA number.
Issuer ICA	Unique six-digit ID number assigned by Mastercard to identify a customer or processing endpoint. Sequenced by ICA and listed numerically. This ICA may be the same or different than the Billing ICA number.
Country Code	A three-digit, numeric code that identifies the country. Issuers may use these codes to establish higher or lower transaction limits for a country or countries where the transaction is acquired.
Merchant Type	DE 18 (Merchant Type) is the classification (card acceptor business code [MCC]) of the merchant's type of business or service.
CAT Level Code	DE 61 (Point-of Service [POS] Data), subfield 10 (Card Activated Terminal Level [CAT]) indicates whether the cardholder activated the terminal with the use of the card and the CAT security level.

Field	Description
POS Terminal PAN Entry Mode	DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) indicates how the PAN was entered at the terminal.
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. If an authorization is declined, the response code indicates the reason for rejection and may indicate an action to be taken at the card acceptor.
Group ID	Identifies a grouping of issuer account ranges that use the same transaction criteria for routing to the same destination route.
Scope	Indicates where the block occurs. • Acquirer—Indicates that the block occurred at the acquirer MIP. • Stand-In—Indicates that the block occurred during Stand-In processing.
Associated BIN Ranges	Identifies a range of card numbers within a BIN that are associated to that blocking ICA. These blocks occur at the MIP and not in Stand-In processing. These ranges may or may not have been issued to cardholders.

Authorization Summary by CAT Level Report (SI458010-AA)

An overview of the Authorization Summary by CAT Level Report (SI458010-AA) is listed in table format.

Title	Authorization Summary by CAT Level
Generated by	Mastercard Authorization Platform
Purpose	To provide customers with a tool for analyzing authorization performance for cardholder-activated transactions.

Description	Mastercard produces this report for each CAT level. The report shows authorization transaction processing volumes and percentages by BIN for the week for the CAT level of the report. It reflects network usage—that is, transactions that travel across the Mastercard Network, not only billable items, which are listed apart from other transactions in the authorization detail reports located in the *Mastercard Consolidated Billing System* manual. The report displays activity by authorization response: Accept (approved), Decline (decline), Call-Me (refer to card issuer), and Pick-Up (capture card). It also displays transactions by transaction category, such as mail/telephone and retail.
Frequency	Weekly
Distribution Methods	Paper (Sent to the authorization contact established on the Principal Member Questionnaire); Mastercard eService

Report Sample

Report sample of the Authorization Summary by CAT Level Report (SI458010-AA).

```
REPORT SI458010-AA                    MASTERCARD INTERNATIONAL, INC.                                PAGE   1
                                        AUTHORIZATION SUMMARY BY CAT LEVEL          DATE 07/27/08 TIME 13:28:56
                              FOR CAT 1 WEEK BEGINNING 07/19/08 AND ENDING 07/25/08
                                        ICA 999999   PREFIX 999999
CAT 1 PROCESSED                 MEMBER      MEMBER YTD        SYSTEM      SYSTEM YTD
  ACTIVITY                      VOLUME          VOLUME        VOLUME          VOLUME

ACCEPT                              35              642       101,711       2,286,263
  PERCENT OF TOTAL                58.3             64.5          74.4            88.4

DECLINE                             25              353        34,861         298,884
  PERCENT OF TOTAL                41.7             35.5          25.5            11.6

CALL-ME                              0                0            33             768
  PERCENT OF TOTAL                 0.0              0.0           0.0             0.0

PICK-UP                              0                0           129           1,129
  PERCENT OF TOTAL                 0.0              0.0           0.1             0.0

TOTAL MEMBER PROCESSED              60              995       136,734       2,587,044
-------------------------------------------------------------------------------------------------------------------
APPROVALS BY                  AVERAGE           TOTAL         TOTAL     YTD AVERAGE         YTD TOTAL      YTD TOTAL
TRANSACTION TYPE              DOLLARS         DOLLARS       VOLUME         DOLLARS           DOLLARS         VOLUME

MAIL/TELEPHONE                   0.00            0.00            0            0.20              0.20              1
RETAIL                          92.86        1,485.87           16           78.19         16,108.42            206
CASH ADVANCE                     0.00            0.00            0            0.00              0.00              0
COLLEGE/HOSPITAL                 0.00            0.00            0            0.00              0.00              0
HOTEL/MOTEL                      0.00            0.00            0            0.00              0.00              0
VEHICLE RENTAL                   0.00            0.00            0            0.00              0.00              0
TRANSPORTATION                  12.01          216.18           18           20.32          8,800.53            433
RESTAURANT                       0.00            0.00            0            0.00              0.00              0
CIRRUS/ATM                     173.68          173.68            1          162.12            324.25              2
UNIQUE                           0.00            0.00            0            0.00              0.00              0
PAYMENT                          0.00            0.00            0            0.00              0.00              0
    TOTAL MEMBER APPROVALS      53.59        1,875.73           35           39.30         25,233.40            642
```

REPORT SI458010-AA MASTERCARD INTERNATIONAL, INC. PAGE 2
AUTHORIZATION SUMMARY BY CAT LEVEL DATE 07/27/08 TIME 13:28:56
FOR CAT 1 WEEK BEGINNING 07/19/08 AND ENDING 07/25/08
ICA 999999 - TOTAL FOR ALL PREFIXES

CAT 1 PROCESSED ACTIVITY	MEMBER VOLUME	MEMBER YTD VOLUME	SYSTEM VOLUME	SYSTEM YTD VOLUME
ACCEPT	663,668	16,648,839	29,272,736	823,159,564
PERCENT OF TOTAL	95.6	95.8	98.1	98.2
DECLINE	30,519	723,577	544,600	14,441,774
PERCENT OF TOTAL	4.4	4.2	1.8	1.7
CALL-ME	1	52	9,218	213,076
PERCENT OF TOTAL	0.0	0.0	0.0	0.0
PICK-UP	0	5	10,493	297,930
PERCENT OF TOTAL	0.0	0.0	0.0	0.0
TOTAL MEMBER PROCESSED	694,188	17,372,473	29,837,047	838,112,344

APPROVALS BY TRANSACTION TYPE	AVERAGE DOLLARS	TOTAL DOLLARS	TOTAL VOLUME	YTD AVERAGE DOLLARS	YTD TOTAL DOLLARS	YTD TOTAL VOLUME
MAIL/TELEPHONE	366.63	19,431.81	53	258.97	495,675.52	1,914
RETAIL	1.25	827,520.16	661,843	1.23	20,490,219.34	16,612,041
CASH ADVANCE	0.00	0.00	0	0.00	0.00	0
COLLEGE/HOSPITAL	0.00	0.00	0	6.08	834.25	137
HOTEL/MOTEL	157.51	630.06	4	158.13	30,046.18	190
VEHICLE RENTAL	0.00	0.00	0	0.00	0.00	0
TRANSPORTATION	20.49	26,748.08	1,305	19.60	621,326.41	31,695
RESTAURANT	17.02	7,883.02	463	15.91	45,455.72	2,856
CIRRUS/ATM	0.00	0.00	0	0.00	0.00	0
UNIQUE	0.00	0.00	0	13.69	82.18	6
PAYMENT	0.00	0.00	0	0.00	0.00	0
TOTAL MEMBER APPROVALS	1.33	882,213.13	663,668	1.30	21,683,639.60	16,648,839

Field Descriptions

The fields on the Authorization Summary by CAT Level Report (SI458010-AA) are listed in table format.

Field	Description
CAT Processed Activity	Summary of all authorization activity received and processed by the issuer for the CAT level on the report, listed by the following response categories: • Accept (approved) • Decline • Call-Me (refer to card issuer) • Pick-Up (capture card)
Member Volume	Total CAT transaction volume processed by the customer that generated the specific response and the percentage it represents of total customer CAT transaction volume.

Field	Description
Member YTD Volume	Summary of the customer's CAT authorization volume for the calendar year-to-date (by response category) and the percentage it represents of total member CAT volume for the year-to-date.
System Volume	Volume of CAT authorization transactions processed by the entire membership that week and the percentage it represents of total CAT volume for the membership for the week.
System YTD Volume	Volume of CAT authorization transactions processed by the entire membership for the calendar year-to-date and the percentage it represents of total CAT volume for the membership for the year-to-date.
Total Member Processed	Total member CAT volume, year-to-date volume, system volume, and system year-to-date volume for all authorization responses.
Approvals by Transaction Type	Summary of all approved responses returned for CAT transactions, divided by the following transaction categories: • Mail/Telephone • Retail • Cash Advance • College/Hospital • Hotel/Motel • Vehicle Rental • Transportation • Restaurant • ATM • Unique • Payment Transaction
Average Dollars	Average dollar amount approved for CAT transactions for the week, listed by transaction type.
Total Dollars	Total dollar amount approved for CAT transactions for the week, listed by transaction type.
Total Volume	Total CAT transaction volume processed by the customer for the week, listed by transaction type. In the sample, the total volume for Restaurant transactions is 3. This indicates that out of a total of 86 approved CAT 2 transactions, 3 were for Restaurant.

Field	Description
YTD Average Dollars	Average U.S. dollar amount approved, by transaction type, for CAT transactions for the calendar year-to-date. This amount is the result of dividing the YTD TOTAL DOLLARS by the YTD TOTAL VOLUME.
YTD Total Dollars	Total U.S. dollar amount of CAT transactions approved by the customer for the calendar year-to-date.
YTD Total Volume	Total CAT transaction volume approved by the customer for the calendar year-to-date.
Total Member Approvals	Average U.S. dollar amount, total U.S. dollar amount, total transaction volume, and year-to-date totals for all CAT transactions approved by the customer.
Total For All Prefixes	Activity totals for all the customer's BINs (all of the previous pages of the report). Totals are listed by authorization response (such as accept, decline, call-me, and pick-up) and by transaction category (such as mail/telephone and retail).

Chapter 9 EMV Transactions

This section explains the impact of chip contact technology on the Authorization Platform.

Introduction to Chip Card Technology

The following information provides a brief introduction to chip card technology.

The introduction of chip technology brings a dramatic increase to the computing power available at the point-of-interaction (POI). Sophisticated cards meet equally sophisticated terminals, all of which have been manufactured by a large number of independent vendors throughout the world. The need for interoperability is obvious.

EMV

In 1996, Europay (now Mastercard Europe sprl), Mastercard, and Visa (EMV) developed standards for integrated circuit cards (ICCs), terminals, and applications. EMVCo, LLC, established in 1999, is the organization that oversees and maintains the EMV specifications. The EMV standard applies to cards and to terminals and is intended to ensure that any compliant card works in any compliant terminal, therefore the EMV specifications guarantee the interoperability between the card and the terminal.

Chip Terminals

A hybrid Automated Teller Machine (ATM), Point-of-Service (POS) terminal, and Cardholder-Activated Terminal (CAT) support both contact EMV chip and magnetic stripe technology.

The ATM, POS, and CAT terminals that accept Mastercard®, Debit Mastercard®, Maestro®, and Cirrus® may be either hybrid, which support both chip and magnetic stripe technology, or magnetic stripe only. These terminals are not allowed to be chip-only because magnetic stripe only cards would not be accepted.

Mastercard Branded Hybrid Cards

A hybrid Mastercard, Debit Mastercard, Maestro, and Cirrus card is a card that supports both contact EMV chip and magnetic stripe technology. These cards are not allowed to be chip-only because they would not be accepted at Mastercard merchants operating magnetic stripe only terminals.

Transaction Flow

The magnetic stripe transaction process is listed in table format.

1. The terminal reads the Track 1 or Track 2 data from the magnetic stripe. Although there may be different proprietary implementations, the terminal usually identifies the payment system and the brand of the card from the magnetic stripe's PAN.
2. The magnetic stripe terminal decides, based on the rules fixed by the payment system, how to authenticate the cardholder either with a PIN, signature, or no Cardholder Verification Method (CVM).
3. The magnetic stripe terminal also decides whether the transaction must be authorized online or authorized offline. This decision is governed by the floor limits.

NOTE: All magnetic stripe transactions performed on online capable terminals should be online authorized, regardless of the transaction amount.

Contrary to magnetic stripe, a chip transaction allows more than one application to be supported on the same card. The chip transaction uses the following process:

1. The terminal determines the applications that are supported on both the chip card and terminal.
2. If there is more than one application and if the terminal supports a dialog with the cardholder, the terminal prompts the cardholder for his or her choice.
3. After the terminal selects the application chosen by the cardholder, it reads the data on the chip, and then performs a range of checks in combination with the chip card.
4. The result of these tests is reported in EMV tag 95 (Terminal Verification Result [TVR]).
5. Based on the result of these tests, the terminal and the card either decides to:
   - Decline (the card replies Application Authentication Cryptogram [AAC], or
   - Accept offline (the card replies Transaction Certificate [TC]), or
   - Go online (the card replies Authorization Request Cryptogram [ARQC]).

In the first decision, the transaction is terminated. In the second decision, the transaction is accepted offline. In the third decision, the transaction is sent for online authorization.

Online Authorization

The third decision of the transaction flow—the online authorization—is described.

There are two scenarios with online authorization:

- The terminal receives an online response from the issuer.
- The terminal is unable to connect to the issuer.

If the chip technology fails at any of the processes described earlier, the magnetic stripe technology is used as fallback at the attended POS. Fallback to magnetic stripe is not allowed on offline-only unattended terminals. Supporting fallback to magnetic stripe on ATMs and unattended online terminals is also required, except if it is prohibited by regional rules (for example in Europe).

Online Response

When the terminal receives an online response from the issuer, the online chip transaction follows a path similar to a magnetic stripe transaction.

When authorizing the online transaction on the issuer's host, the issuer usually applies the same tests as for a magnetic stripe transaction. The issuer also verifies additional chip data fields that include the Authorization Request Cryptogram (ARQC), an Application Cryptogram (AC), and a Transaction Certificate Cryptogram (TC) provided in DE 55, which is a Message Authentication Code (MAC) over other data in DE 55. A correct ARQC proves to the issuer that the card is genuine, and the other data in DE 55 that was used as input to the ARQC was not altered.

Another chip data field is the Card Verification Result (CVR). The CVR, which is a subset of the Issuer Application Data (EMV subelement 9F10), is calculated by the chip. The CVR gives the issuer more information about the transaction. Another important subelement in DE 55 is Terminal Verification Results (TVR). The TVR provides issuers with the transaction processing results from the terminal. Mastercard recommends that issuers verify both the CVR and the TVR.

To indicate in the online reply that the chip transaction is approved or declined, the issuer uses the following process:

1. The issuer sends the authorization response message containing DE 39 (Response Code) with the same values as for magnetic stripe.
2. If the cryptogram validation fails, the issuer uses DE 48 (Additional Data—Private Use), subelement 74 (Additional Processing Information) to indicate the reason why the ARQC or TC cryptogram validation failed to the acquirer.
3. For chip transactions, a full-chip issuer host sends DE 55 in the authorization response message.

   In this context, DE 55 contains the Issuer Authentication Data, a cryptographic value that proves to the chip that the transaction is approved by the genuine issuer. DE 55 in the authorization response message also may contain ICC post-issuance commands (referred to as issuer scripts) to be sent to the card by the issuer, for example to update a chip card parameter.
4. The terminal asks the card to approve or decline, according to the issuer's decision communicated, as for magnetic stripe in DE 39.
5. Together with the issuer's decision, the terminal sends to the card the Issuer Authentication Data present in DE 55 of the authorization response message.
6. If the transaction is approved, this confirms to the chip that the approval comes from the genuine issuer.

   The card takes the final decision, and depending on internal parameters decides whether to reset its offline cumulative counters. The transaction is terminated.

For information about online responses from the issuer and data requirements, refer to Impact of Chip Technology on the Network Message.

Unable to Connect to the Issuer

If the terminal did not get a valid reply from the acquirer, the terminal switches to the EMV mode Unable to go online.

If the acquirer (or an intermediate processor) falls into time out on the online authorization response message, the online authorization response message is corrupted, or the acquirer cannot connect to online authorization, the acquirer sends a response to the terminal to inform it of the problem (how this information is sent is proprietary). Once the terminal receives this response from the acquirer, it must continue the EMV transaction in the Unable to Go Online EMV mode.

In the EMV mode Unable to Go Online, depending on the conditions set by the issuer on the card in the IAC-Default and by the acquirer on the terminal in the TAC-Default, the transaction may either be approved offline or declined.

Processing steps are as follows:

1. The terminal will ask the card to approve or decline. It is essential that the authorization response code (a data element requested by the card) is set by the terminal to the appropriate code Y3 (or Z3) to indicate Approved (or Declined)—Unable to Go Online. Because the response is not initiated by the issuer, no Issuer Authentication Data is sent to the card.

   The absence of the Issuer Authentication Data in the reply from the acquirer may not be considered a reason for the terminal to apply the EMV mode Unable to go online. Only the proprietary flag described earlier instructs the terminal to do so.
2. The card returns an Application Cryptogram that reflects its final decision.

Issuers

Issuers that want to make use of the chip-related information in the authorization request can start with magnetic stripe grade issuing, and then upgrade to Full Chip Grade issuing later.

Full Chip Grade Issuing

Full chip issuing is the term used to describe an issuer that has upgraded its host system as follows.

- Verify the ARQC provided in DE 55 of the authorization request.
- Send valid issuer authentication data in DE 55 of the authorization response.

A full chip card normally is programmed to approve an online transaction if and only if the Issuer Authentication Data is present and valid. If the Issuer Authentication Data is either not present or present and incorrect, the standard Full chip card is set to decline.

With full chip grade issuing:

- Full chip issuers must verify the ARQC and generate Issuer Authentication Data.
- Full chip issuers must support the processing of DE 23 (Card Sequence Number) and DE 55 on their online authorization host.
- Full chip issuers that subscribe to the M/Chip Cryptogram Pre-validation service do not need to support the chip cryptography on their online authorization host. These issuers also benefit from the pre-validation service when their host is not available because Stand-In processing considers the result of the cryptogram pre-validation when responding to the authorization request.
- Full chip issuers that do not subscribe to the M/Chip Cryptogram Pre-validation service must support the chip cryptography on their online authorization host. To ensure successful chip transactions while their host is not available, issuers must sign up for the M/Chip Cryptogram Validation in Stand-In Processing service.

- Full chip issuers that request Stand-In processing must sign up for the M/Chip Cryptogram Validation in Stand-In Processing service to guarantee the success of the transaction.
- Cards issued with the chip grade issuing profile will decline chip transactions when no Issuer Authentication Data is returned in the authorization response message.

Magnetic Stripe Grade Issuing

Magnetic stripe grade issuing is the term used to describe an issuer that has not upgraded its host system to perform chip cryptography. Although authorization request messages contain DE 55, magnetic stripe grade issuers do not verify the ARQC or TC; therefore, do not use the data in DE 55. These issuers do not generate DE 55 in the online response because they cannot provide Issuer Authentication Data or send issuer scripts.

Magnetic stripe grade issuing provides the following benefits:

- Offline card authentication method (CAM)
- Offline CVM (where applicable)
- Card risk management

Because magnetic stripe grade issuers do not verify the ARQC or TC, they process the chip transaction as a magnetic stripe authorization (even though chip technology was used).

By not supporting DE 55, there is:

- No guarantee that the data in DE 55 was not altered
- No online CAM
- No online mutual authentication
- No script processing, therefore no possibility to update the card

Magnetic stripe grade issuers must personalize their cards so that they do not decline an online-authorized transaction because Issuer Authentication Data is not provided.

Magnetic stripe grade issuers that subscribe to the Chip to Magnetic Stripe Conversion service can support chip transactions without any change to their online issuer authorization host to support chip.

Magnetic stripe grade issuers that do not subscribe to the Chip to Magnetic Stripe Conversion service must support DE 23 and DE 55 on their online authorization host.

Acquirers

Chip acquirers must be full grade, that is, they must support DE 55 in the online authorization request message and response message.

X-Code Processing

If the transaction uses chip technology, the acquirer can perform acquirer host X-Code processing only if the acquirer's infrastructure is upgraded to instruct the terminal to switch to Unable to go online EMV mode.

If the acquirer's infrastructure is not able to instruct the terminal to process the transaction in the mode Unable to go online, the acquirer must decline the chip transaction.

An X-Code transaction is only approved if the terminal proposes to the card to approve the transaction in the Unable to go online EMV mode and if the card also accepts this proposal. Otherwise, the transaction is declined.

Acquirer Authorization Below International Floor Limit

There may be situations where the terminal routinely goes online to the acquirer host for a transaction, even if it is below the international floor limit and could be approved in offline mode.

Although the terminal goes online to the acquirer, it is possible that the acquirer does not want to send an online request to the issuer (for example, the transaction is below the international floor limit, and the card is not effective in a regional Warning Bulletin), and approves the transaction on behalf of the issuer.

The transaction is then an offline transaction. This processing is often referred to as acquirer truncation, and in most countries is not allowed for magnetic stripe transactions because their floor limit for such transactions is zero. In addition, Mastercard does not recommend this process for chip transactions because potentially valid transactions may be declined.

For offline transactions, the acquirer instructs the terminal to accept the transaction using the Unable to go online EMV mode. As discussed earlier, the terminal must set the authorization response code (a data element requested by the card) to the appropriate value Y3 (or Z3), indicating Approved (or Declined)—Unable to Go Online.

Care must be given when the chip application generates an ARQC, and the acquirer does not want to go online to the issuer for transactions below the international floor limit. It is not possible to know whether the chip application's Card Risk Management will subsequently approve that transaction offline when instructed that the terminal was Unable to Go Online.

If the acquirer decides to authorize in offline mode, even if the result of the Action Codes Default is to request a Transaction Certificate (TC), the acquirer will be liable if the chip application responds with an Application Authentication Cryptogram (AAC). If the acquirer does not take the liability, it declines a transaction that could have been approved online by the issuer.

For this reason, Mastercard recommends that all transactions where an ARQC was generated be sent to the issuer for online authorization.

Refer to Card Issuer

If the transaction uses chip technology and the issuer responds with refer to card issuer, the terminal must terminate the chip transaction by requesting an AAC to the card, and the merchant should follow the refer to card issuer procedures, as for magnetic stripe.

Online Reversal Advices

In some circumstances, such as a terminal failure, terminals decline transactions that were online approved. In such cases, the terminal should send an online reversal advice to inform the issuer.

With chip technology, situations may occur due to the terminal or card chip application being instructed to override the issuer's decision. A reversal should be sent as well; however, such situations should be exceptional.

M/Chip Processing Services

To assist issuers migrating to chip, Mastercard has several M/Chip processing network services that allow issuers to migrate at their own pace. Although these services are fully described in the *M/Chip Processing Services—Service Description* guide, the following information provides a brief description of each of these services.

Chip to Magnetic Stripe Conversion Service

The Chip to Magnetic Stripe Conversion service removes all the chip data from authorization messages and passes them on to the issuer. Issuers can therefore issue chip cards, but leave their host systems unchanged. An issuer that has requested this service is a magnetic stripe issuer.

When the Chip to Magnetic Stripe Conversion service processing is performed on a transaction, the original method used to enter the primary account number (PAN) in the Authorization Platform will be indicated in DE 48 (Additional Data—Private Use), subelement 71 (On-behalf [OB] Services), subfield 2 (On-behalf Result 1) before sending Authorization Request/0100, Authorization Advice/0120, and Reversal Request/0400 messages to the issuer for processing.

M/Chip Cryptogram Pre-validation Service

The M/Chip Cryptogram Pre-validation service validates the Authorization Request Cryptogram (ARQC) and Transaction Certificate Cryptogram (TC) in the authorization message, verifies the Card Verification Results (CVR) and the Terminal Verification Result (TVR), passes the result of the check in the message on to the issuer host system, and generates on-behalf of the issuer an Authorization Request Cryptogram (ARPC) for the response. It enables issuers to begin using chip cards as full chip issuers without implementing full chip cryptography on their host system.

These issuers also benefit from the pre-validation service when their host is not available because Stand-In processing considers the result of the cryptogram pre-validation when responding to the authorization request. When issuers have developed full chip cryptography support on their online authorization host, they must subscribe to the M/Chip Cryptogram Validation in Stand-In Processing service so Mastercard can attempt to validate the cryptogram for any chip transactions that route to Stand-In.

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.

When an authorization request containing chip data is submitted and the issuer participates in this combined service, the Authorization Platform performs the M/Chip Cryptogram Pre-validation service before performing the Chip to Magnetic Stripe Conversion service. The Authorization Platform identifies the services it performed, along with their validation results, by populating separate occurrences within DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), and forwards the authorization request to the issuer. This allows the issuer to use the results of the cryptogram validation, along with existing risk management logic, to approve or decline the transaction while processing the authorization response as a normal magnetic stripe transaction.

Issuers that want to use both services must contact Mastercard and identify the account range and expiry date that the service will support using the Chip Processing Services Member Requirements and Parameters form, which is available in Appendix A of the *M/Chip Processing Services—Service Description* guide and in the Business Forms section of Mastercard Connect™. Issuers also must provide the keys and parameters according to the *On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications* manuals.

M/Chip Cryptogram Validation in Stand-In Processing

The M/Chip Cryptogram Validation in Stand-In Processing service authorizes transactions based on the issuer's parameters similar to the normal magnetic stripe Stand-In processing. This service checks the ARQC and TC (to perform online CAM), verifies the CVR and the TVR, and generates an ARPC so that the card will authenticate the response correctly.

NOTE: All issuers globally that participate in Stand-In processing must have M/Chip Cryptogram Validation in Stand-In Processing performed during Stand-In processing.

A full chip issuer that subscribes to the Stand-In processing service for magnetic stripe must request the M/Chip Cryptogram Validation in Stand-In Processing service.

A magnetic stripe grade issuer that subscribes to Stand-In processing does not need to request the M/Chip Cryptogram Validation in Stand-In Processing service.

When Stand-In processing performs the optional CVC 1 test on issuer's request, the CVC 1 test is done only for a magnetic stripe transaction. It is not done for a chip transaction because the chip online dynamic card authentication method (CAM) is done.

MIP X-Code Processing

A transaction approved by the MIP X-Code processing is identical to a transaction approved by the issuer, except that there is no DE 55 in the reply. Full chip cards decline the transaction while magnetic stripe grade cards are not impacted.

Impact of Chip Technology on the Network Message

The following information explains the impact of chip technology on the network message.

DE 22—Point-of-Service (POS) Entry Mode

Data requirements for DE 22 in network messages.

Subfield 1—POS Terminal PAN Entry Mode

DE 22, subfield 1, value 05 (PAN auto-entry via chip) indicates that chip contact technology is used for the transaction. Acquirers must be certified with the full grade profile to use this value. If DE 22, subfield 1 contains value 05, DE 55 (Integrated Circuit Card [ICC] System-related Data) must be present.

Partial Grade acquiring means that for a chip transaction, DE 55 is not present. Although Partial Grade acquiring is no longer allowed, chip issuers must continue to support Partial Grade acquired transactions (that is, transactions where DE 22 = 05 without DE 55 present in the online request) until Partial Grade acquirers have all rolled out to full grade acquiring.

DE 22, subfield 1, value 80 indicates that chip technology should have been used because it is supported by both card and terminal, however due to a failure of the chip technology magnetic stripe technology is used as fallback. Acquirers must use value 80 as follows:

- The terminal and the acquirer are certified to accept a Mastercard card with chip technology.
- Mastercard card supports chip technology, which is indicated by a service code 2xx or 6xx on the magnetic stripe.

DE 22, subfield 1 also supports contactless chip technology. DE 22, subfield 1, value 07 (PAN auto-entry via contactless M/Chip), value 91 (PAN auto-entry via contactless magnetic stripe), and value 92 (Contactless input, Contactless Mapping Service applied when acquirer DE 22, subfield 1 contains value 91) indicate contactless chip technology is used for the transaction. For more information about contactless chip technology, refer to the *Contactless On-behalf Services Guide*.

Chip Technical Fallback

Authorization Request/0100 messages containing transactions submitted as chip fallback (DE 22, subfield 1, value 80) are cross-referenced with the acquirer's chip testing level certification indicator stored at Mastercard. If the value indicates that the acquirer is not certified to process these types of transactions, the Authorization Platform downgrades (DE 22, subfield

1, value 90) the chip transaction before forwarding it to the issuer for authorization. The values in DE 48, subelement 74 (Additional Processing Information), subfield 1 and subfield 2 notify acquirers whenever this occurs in Authorization Request Response/0110 and Reversal Request Response/0410 messages.

Issuers also will receive downgraded chip transactions sent by non–chip compliant acquirers in the following messages containing DE 22, subfield 1, value 80:

- Authorization Advice/0120—Acquirer-generated
- Authorization Advice/0120—System-generated
- Reversal Request/0400
- Reversal Advice/0420

Subfield 2—POS Terminal PIN Entry Mode

Issuers should not edit this subfield. Acquirers must use values that reflect the terminal capability. A terminal that supports PIN must use value 1 (Terminal has PIN entry capability) to indicate the terminal has a PIN entry capability. Because a Maestro terminal and an ATM support PIN, terminals always must use value 1.

DE 23—Card Sequence Number

Acquirers must populate DE 23 with the chip data Application PAN Sequence Number (EMV tag 5F34) from the chip when given by the card to the terminal. If there are several applications on the chip that have the same PAN, this field allows the issuer to know which one is used.

DE 35—Track 2 Data

DE 35 contains the track 2 data.

Acquirers must populate DE 35 with the magnetic stripe Track 2 data if DE 22, subfield 1 contains value 80 or value 90 and with the chip Track 2 equivalent EMV tag 57 from the chip if DE 22, subfield contains value 05.

DE 48—Additional Data—Private Use

Data requirements for DE 48 in network messages. For more information about the values in this subelement, refer to the *Customer Interface Specification* manual.

Subelement 71—On-behalf Services

This subelement identifies the on-behalf service performed on the transaction, and the results when converting an M/Chip transaction to a magnetic stripe transaction or when validating the Authorization Request Cryptogram (ARQC).

Subelement 72—Issuer Chip Authentication

Subelement 72 carries the Issuer Authentication Data calculated by the on-behalf service.

Subelement 74—Additional Processing Information

Subelement 74 provides information when there is a chip cryptogram issue.

When issuers perform chip cryptogram validation and there is an issue with the cryptogram, issuers should include DE 48, subelement 74. For chip cryptogram issues, issuers should use DE 39 (Response Code), value 57 (Transaction not permitted to issuer/cardholder).

Acquirers that process chip transactions must be prepared to receive DE 48, subelement 74.

Acquirers also will see when a chip transaction has been downgraded to a magnetic stripe transaction. When a chip transaction has been downgraded to a magnetic stripe transaction, the transaction should be submitted to the Global Clearing Management System (GCMS) as a magnetic stripe transaction.

Acquirers receiving subelement 74, subfield 1 (Processing Indicator), value 90 (Chip Fall-back Transaction Downgrade Processing) in Authorization Request Response/0110 messages may be liable for disputes under the Chip Liability Shift Program, even if the issuer approved the transaction. Acquirers receiving subelement 74, subfield 1, value 90 must contact their Mastercard representative in the region to cross check their chip certification status and to initiate, as required, the relevant chip certification process.

Subelement 79—Chip CVR/TVR Bit Error Results Listing

Subelement 79 provides issuers that participate in M/Chip Cryptogram Pre-validation and M/Chip Cryptogram Validation in Stand-In Processing services with a list of specific bits within the Terminal Verification Results (TVR) and Card Verification Results (CVR) that were found to have an unexpected value provided by the issuer during the M/Chip Cryptogram Pre-validation service or the M/Chip Cryptogram Validation in Stand-In Processing service.

DE 55—Integrated Circuit Card (ICC) System-related Data

DE 55 in the online request contains data elements that were exchanged on the card terminal interface. The format of the data follows the value TLV (tag, length, value) format. The value of data elements in DE 55 must contain the exact value—bit per bit—that was present on the card to terminal interface. Padding data is not allowed because it may cause Application Cryptogram verification to fail. If the same data appears several times on the card to terminal interface, DE 55 must contain the last data value that was present on the card terminal interface within a transaction.

Mastercard network interface specifications for DE 55 indicate that:

- Acquirers must send all data elements defined as mandatory by EMV in DE 55. Additionally, acquirers must send data that is defined as conditional by EMV if the condition is satisfied.
- Acquirers may send data that is defined as optional by EMV.
- Acquirers are not allowed to send any data other than mandatory, conditional, or optional data.

The data in DE 55 in the online request must not be echoed in the online response.

For more information about the format of the EMV data, refer to the following documents:

- *M/Chip Requirements* document
- *Customer Interface Specification* manual
- *Single Message System Specifications* manual
- EMV Specification version 4.1–Book 4–Cardholder, Attendant, and Acquirer Interface Requirements

DE 61—Point-of-Service (POS) Data

Subfield 11 (POS Card Data Terminal Input Capability) indicates the terminal is EMV chip if and only if the terminal and the acquirer are certified to accept a Mastercard card with chip technology.

Digital Secure Remote Payment with EMV Data

Mastercard provides DSRP to enable secure mobile-originated transactions for remote payments.

DSRP authorization request messages may be transmitted either with full EMV data or cryptographic data within the UCAF field or Digital Payment Data Field.

For details about DSRP, including examples of process flow, refer to Digital Secure Remote Payment in Authorization Services Details.

Chapter 10 PIN Processing for Europe Region Customers

Europe Region. *This section explains how the Authorization Platform supports PIN translations for acquirers and issuers and issuer PIN validation on the Dual Message System.*

About PIN Processing for Europe Region Customers

The Authorization Platform supports PIN translation for acquirers and issuers and issuer magnetic stripe PIN validation for Track 1 and Track 2 on the Mastercard Network.

Static Key Definition

Mastercard allows customers to provide multiple PIN keys that can be used for PIN encryption. Mastercard uses the customer-specified PIN encryption key for PIN translation.

Mastercard requires that acquirers use DE 53 (Security-related Control Information) in Authorization Request/0100 messages to identify the key used for PIN encryption. Issuers optionally provide DE 53 in Network Management Request/0800 messages when signing on to the Mastercard Network to identify the encryption key to use for transaction processing. Customers can define a maximum of 99 keys.

PIN Block Formats

Translation of encrypted PINs is supported using any of the following PIN block formats:

- 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)

PIN Validation Services

PIN validation for both Track 1 and Track 2 is based on the track present in the Authorization Request/0100 message. Mastercard offers the following on-behalf services to issuers for PIN validation.

Online PIN Pre-validation

The Online PIN Pre-validation service is an optional service for issuers that are not capable of validating PIN data.

Online PIN Pre-validation provides the results of the PIN validation to issuers in DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services) of the Authorization Request/0100 message and to acquirers in DE 48 (Additional Data—Private Use), subelement 80 (PIN Service Code) of the Authorization Request Response/0110 message.

Issuers may provide a PIN Verification Value (PVV) file for use during PIN validation.

The Stand-In System uses the result of the PIN pre-validation when the issuer is not available. The Authorization Advice/0120—System-generated message will contain the results of the PIN pre-validation in DE 48 (Additional Data—Private Use), subelement 71 (On-behalf Services), and DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code).

The Authorization Platform supports five PIN failed attempts for the Online PIN Pre-validation service.

Issuers participating in the Online PIN Pre-validation service are not required to provide DE 53 in their Network Management Request/0800 messages when signing on to the Mastercard Network.

For details about data requirements, refer to the *Customer Interface Specification* manual.

Online PIN Validation in Stand-In

The Online PIN Validation in Stand-In service is an optional service for issuers that perform PIN validation and want the Authorization Platform to provide PIN validation when they are not available.

Online PIN Validation in Stand-In will provide the results of the PIN validation to issuers in DE 48, subelement 71 and DE 60, subfield 2 of the Authorization Advice/0120—System-generated message and to acquirers in DE 48, subelement 80 of the Authorization Request Response/0110 message.

The Authorization Platform will allow the issuer to provide a value less than five for PIN failed attempts.

Issuers may provide a PVV file to use during PIN validation.

Issuers participating in the Online PIN Validation in Stand-In service are required to provide DE 53 in their Network Management Request/0800 messages when signing on to the Mastercard Network.

For details about data requirements, refer to the *Customer Interface Specification* manual.

NOTE: Acquirers and issuers should reference the Key Management Services (KMS) interface section in the *On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications* manuals for security procedures, technical format of PIN encryption keys, and PIN validation keys to exchange manually with the KMS.

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 Dual Message System.

DE 53 (Security-related Control Information) provides more flexibility for those customers that want to change the PIN encryption key frequently. Issuers use DE 53 to specify the PIN key to use for processing PIN transactions using the Network Management Request/0800 message when they perform PIN processing in-house or when they participate in the Online PIN Validation in Stand-In service. Acquirers can specify the key used to encrypt the PIN by providing DE 53 in the Authorization Request/0100 message.

Each acquirer and issuer will associate the PIN key index number to identify a specific security key and may define a maximum of 99 security keys for use during PIN translation.

PIN Validation Processing

The Authorization Platform performs PIN validation on DE 52 for issuers subscribing to the Online PIN Pre-validation service or the Online PIN Validation in Stand-In service.

The Authorization Platform supports PIN validation using static validation keys only. Issuers that subscribe to one of the PIN validation on-behalf services must identify an expiration date range for the account range when supplying the PIN validation information. Mastercard will forward to the issuer transactions for cards with an expiration date outside the specified range without performing the validation service.

The Authorization Platform supports the following PIN validation methods:

- IBM3624 (variable length)
- ABA (Mastercard/VISA PVV)

PIN validation results are provided in DE 48, subelement 71 (On-behalf Services) in Authorization Request/0100, DE 48, subelement 80 (PIN Service Code) in Authorization Request Response/0110 and DE 48, subelement 71, and DE 60, subfield 2 in Authorization Advice/0120—System-generated messages when PIN validation has been performed on-behalf of the issuer.

The Authorization Platform manages 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.

PIN Key Management

The Key Management Services (KMS) group manages 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 (PVV)/PIN Offset on File Service

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 to override the information encoded on the track.

Upon receipt of the file at Mastercard, the file will be processed and the information available at the end of processing.

Mastercard activates the PVV/PIN Offset data from an issuer upon receipt of the PVV/PIN Offset File at Mastercard. Issuers may send a full file replacement.

Benefits

The PVV/PIN Offset on File service offers various benefits.

- Issuers that do not encode a PVV/PIN Offset on their cards' Track 1 or Track 2 have access to PIN validation services.
- When PVV/PIN offsets are incorrectly encoded on Track 1 or Track 2, correct PVV/PIN offsets can be provided by file rather than having to re-issue cards.
- Issuers can move their card portfolios away from service providers that perform PIN validation services on their behalf.

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.

Alternate Processing

Mastercard will support issuers subscribing to the Online PIN Pre-validation service that are not available to respond to the Authorization Request/0100 message and issuers subscribing to the Online PIN Validation in Stand-In for Magnetic Stripe service 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.

Issuers participating in one of the PIN validation on-behalf services should reference the KMS interface section defined in the *On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications* manuals for information relating to PIN validation.

Authorization Reports

Certain reports provide information that supports the PIN processing.

- The Authorization Parameter Summary Report (SI737010-AA) includes an indicator to identify issuer participation in the PVV/PIN Offset service in the Global Parameters section. Additionally, participation in either the Online PIN Pre-validation or Online PIN Validation in Stand-In displays in the On-behalf Services section of the report.
- The Authorization Summary Report (AB505010-AA) includes appropriate values in the Response Code Decline category.

For samples of these reports and field descriptions, refer to Reports.

For More Information

For details about data requirements, see the *Customer Interface Specification* manual.

For the PVV/PIN Offset file format, refer to File Layouts.

Chapter 11 PSD2 Authentication Requirements

This chapter describes specific authorization requirements linked to PSD2 RTS.

About PSD2 and RTS

This chapter describes specific authorization requirements linked to PSD2 RTS.

The Payment Service Directive 2 (PSD2) and the Regulatory Technical Standards (RTS) require that remote electronic transactions apply Strong Customer Authentication (SCA) unless specific exemptions (eg low value payment up to €30, low risk acquirer or issuer) apply. Certain transaction types (eg Merchant Initiated Transactions or MIT) are out of scope of this regulation.

The PSD2 and RTS apply in 31 countries which belong to the European Economic Area (EEA).

Low-Risk Merchant Indicator

When SCA by the issuer is not required under PSD2 RTS, or when it has been delegated, the acquirer must provide the reason by populating the appropriate value in DE 48 (Additional Data—Private Use), subelement 22 (Multi-Purpose Merchant Indicator), subfield 01 (Low-Risk Merchant Indicator) in the authorization message:

- 01 = Merchant Initiated Transaction
- 02 = Acquirer low fraud and Transaction Risk Analysis
- 03 = Recurring payment
- 04 = Low value payment
- 05 = SCA Delegation under Authentication Express
- 06 = Secure Corporate Payment

Trace ID for Merchant-Initiated Transactions and Recurring Payments

As of 18 October 2019 for intra-EEA recurring payment transactions, acquirers must provide the unique Trace ID of the initial recurring payment authorization in DE 48, subelement 63 (Trace ID) of subsequent recurring payment transaction authorizations to allow the issuer to validate that SCA occurred on the initial recurring payment authorization, as is required under PSD2 RTS. This rule does not apply to reversals, which must continue to include the Trace ID of the authorization to be reversed.

If the initial authorization happened before 14 September 2019 and the initial Trace ID is not available (for example, was not stored), or if the recurring payment was set-up via mail order, telephone order, or via face-to-face and the initial Trace ID is not available, then the Trace ID must have the following values:

- Positions 1–3 = card acceptor business code (MCC)
- Positions 4–9 = 999999
- Positions 10–13 = 1231
- Positions 14–15 = blank filled

Alternatively, if the initial authorization occurred before 14 September 2019, then the Trace ID can refer to any other authorization belonging to that same recurring payment arrangement provided this authorization took place before 14 September 2019.

Merchant Name Recommendation

It is recommended that acquirers use the same merchant name in authentication and authorization as this facilitates dynamic linking under PSD2 RTS.

Response Code 65 for Strong Customer Authentication

As of 14 September 2019:

- Issuers in the Europe region must decline CNP authorizations without prior 3DS authentication that requires SCA with Response Code 65 (in DE 39). Issuers must not use Response Code 65 if the authorization request was fully authenticated.
- Acquirers' online merchants in the Europe region must retry with an 3DS authentication in response to a declined authorization message with Response Code 65. Until all issuers support Response Code 65, it is recommended that merchants always send an authentication request following a non-3DS authorization that was declined for non-financial and non-technical reasons.

Dynamic Linking

Mastercard requires that issuers validate the SPA AAV in real time before generating the authorization response; Mastercard has implemented this requirement to raise the minimum security standards for electronic commerce (e-commerce) transactions and align with the European Union's PSD2 requirements for dynamic linking.

In support of this activity, Mastercard has made available an on-behalf-of SPA AAV validation service that is invoked as transactions flow through the authorization network and can be configured to perform validation on all transactions or only during Stand-In processing.

For More Information

Other rules related to PSD2 are described in the *Authentication Guidelines for Europe*, which can be found on MastercardConnect.

Appendix A Non-Mastercard Authorization Message Flows

This section explains Mastercard support of non-Mastercard transactions and illustrates the flows of authorization messages for those types of transactions.

Authorization Flows for Visa Cards

When an acquirer enters a Visa transaction into the Mastercard authorization network, Mastercard provides one or more of the following paths to ensure proper authorization:

- Direct to the Visa issuer (only when the Visa issuer has a direct connection to the Mastercard Network [peer-to-peer] and the transaction does not qualify for the Visa Custom Payment Service Request program)[3]
- Routing to the Visa issuer through the Visa network
- Routing to Mastercard X-Code processing

Primary paths are always the first path attempted. Secondary paths are followed only if the primary path is unavailable. Tertiary paths are followed only if the first two paths are unavailable.

Flows for a Peer-to-Peer Visa Issuer—Transaction Does Not Qualify for Visa Custom Payment Service Request

If the transaction is for a peer-to-peer Visa issuer and does not qualify for the Visa Custom Payment Service Request program, the transaction follows one of the following flows:

- Primary Path—Direct to the Issuer
- Secondary Path—Routing through the Visa Network
- Tertiary Path—X-Code Processing

To receive Visa transactions via this direct connection, the Visa issuer must be set up for peer-to-peer processing by a Mastercard Customer and Technology Support representative and must complete testing. Contact the Global Customer Service team to arrange for this service.

Primary Path—Direct to the Issuer

If the transaction can be delivered directly to the Visa issuer, the transaction follows the flow depicted in the following diagram.

Authorization Flow Peer-to-Peer Issuer Non-Visa Custom Payment Service Request Transaction Direct to the Issuer

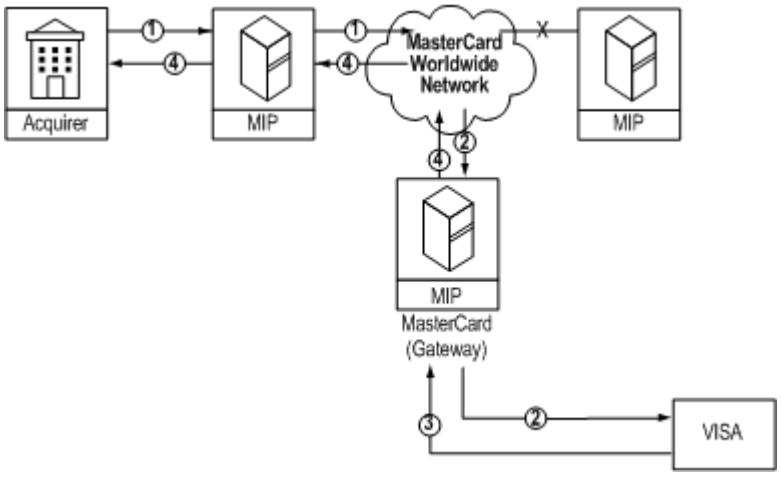
[3] Custom Payment Service Request is a Visa interchange discount program that applies to certain transactions routed through the Visa authorization network.

1. The acquirer creates an authorization request conforming to Mastercard specifications for Visa transactions. The Authorization Platform routes the Visa authorization request through the Mastercard Network to the Visa issuer.
2. The Visa issuer formats an authorization response conforming to Mastercard specifications. The request travels back to the Mastercard Network. The Mastercard Network delivers the authorization response to the acquirer.
3. Online acquirers may generate an authorization acknowledgement message to acknowledge receipt of the response.

Secondary Path—Routing through the Visa Network

If the Mastercard Network connectivity to the Visa issuer is not functioning, the Authorization Platform routes the transaction to the Visa network via a Mastercard gateway.

Authorization Flow Peer-to-Peer Issuer Non-Visa Custom Payment Service Request Transaction to the Issuer via the Visa Network

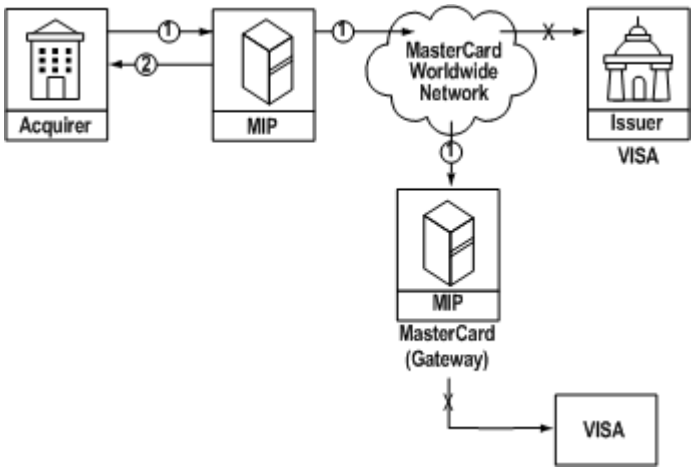


1. The acquirer creates an authorization request conforming to Mastercard specifications for Visa transactions. The Visa authorization request flows through the acquirer MIP to the Mastercard Network.
2. The Authorization Platform, unable to route the authorization request to the Visa issuer, routes it instead to the Mastercard gateway to the Visa authorization network.
3. The Authorization Platform receives the authorization response from Visa.
4. The Authorization Platform delivers the authorization response to the acquirer.

Tertiary Path—X-Code Processing

If Mastercard Network connectivity to both the Visa issuer and the Visa network is down, Mastercard X-Code processing returns a response of decline.

Authorization Flow Peer-to-Peer Issuer Non-Visa Custom Payment Service Request Transaction X-Code Processing



1. The acquirer creates an authorization request conforming to Mastercard specifications for Visa transactions. The Visa authorization request flows through the acquirer MIP to the Mastercard Network.
2. The Authorization Platform is unable to deliver the request to the Visa issuer or the Visa network. X-Code processing returns a response code that indicates Authorization System or issuer system inoperative and that prompts an acquirer response of decline.

Flows for a Peer-to-Peer Visa Issuer—Transaction Qualifies for Visa Custom Payment Service Request

If the peer-to-peer Visa issuer chooses to receive Visa transactions via its Mastercard Network connection and the transaction does qualify for the Visa Custom Payment Service Request program, the transaction follows one of the following flows.

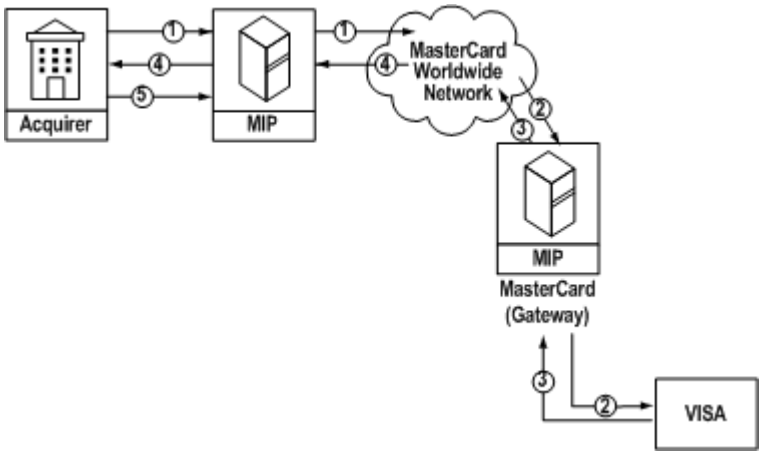
- Primary Path—Routing through the Visa Network
- Secondary Path—Mastercard X-Code Processing

Although the Visa issuer in this scenario is directly connected to the Mastercard Network, Mastercard nevertheless attempts to route the transaction through the Visa network to secure the Custom Payment Service Request discounts for the issuer.

Primary Path—Routing through the Visa Network

The primary path for transactions that qualify for the Visa Custom Payment Service Request program always leads to the Visa network.

Authorization Flow Peer-to-Peer Issuer Visa Custom Payment Service Request Transaction to the Issuer via the Visa Network

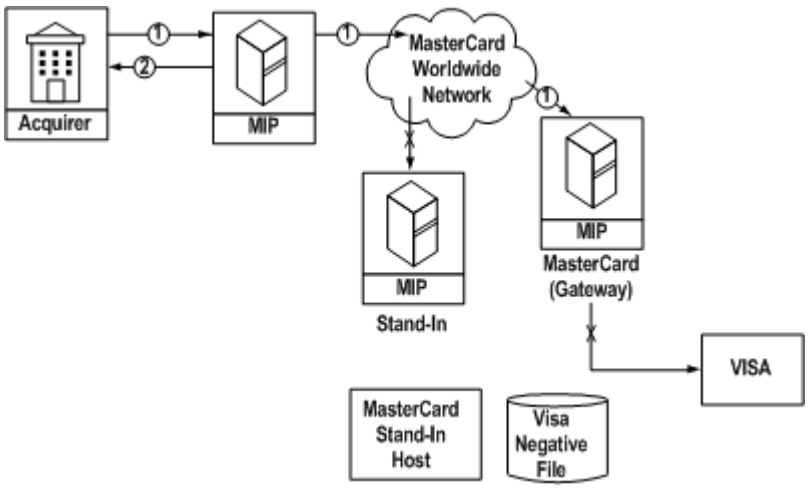


1. The acquirer creates an authorization request conforming to Mastercard specifications for Visa transactions. The Visa authorization request flows through the acquirer MIP to the Mastercard Network.
2. The Authorization Platform routes the authorization request to the Visa network.
3. Visa delivers an authorization response to the Mastercard Network.
4. The Authorization Platform delivers the authorization response to the acquirer.
5. The acquirer has the option to return an acknowledgement message.

Secondary Path—Mastercard X-Code Processing

If Mastercard Network connectivity to the Visa network is not functional, Mastercard X-Code processing returns a response of decline.

Authorization Flow Peer-to-Peer Issuer Visa Custom Payment Service Request Transaction X-Code Processing



1. The acquirer creates an authorization request conforming to Mastercard specifications for Visa transactions. The Visa authorization request flows through the acquirer MIP to the Mastercard Network.
2. The Authorization Platform is unable to route the request to the Visa network or Stand-In processing. X-Code processing at the acquirer MIP returns a response code that indicates, Authorization System or issuer system inoperative and that prompts an acquirer response of decline.

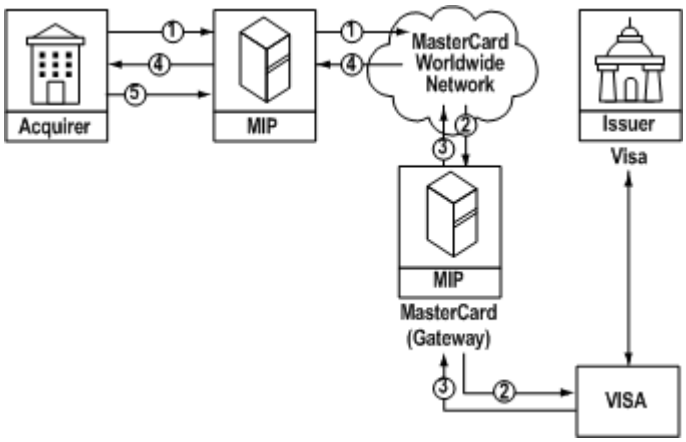
Flows for a Non–Peer-to-Peer Visa Issuer

If the Visa issuer is not connected to the Mastercard Network or chooses not to receive Visa transactions via its Mastercard Network connection, the transaction follows one of the flows depicted in the following illustrations.

Primary Path—Routing through the Visa Network

When the issuer does not have direct connectivity to the Mastercard Network, the primary path for all transactions leads to the Visa network, as illustrated in the following diagram. Visa issuers do not receive PIN data with Visa ATM transactions that are routed to the gateway.

Authorization Flows Non–Peer-to-Peer Issuer to the Issuer via the Visa Network

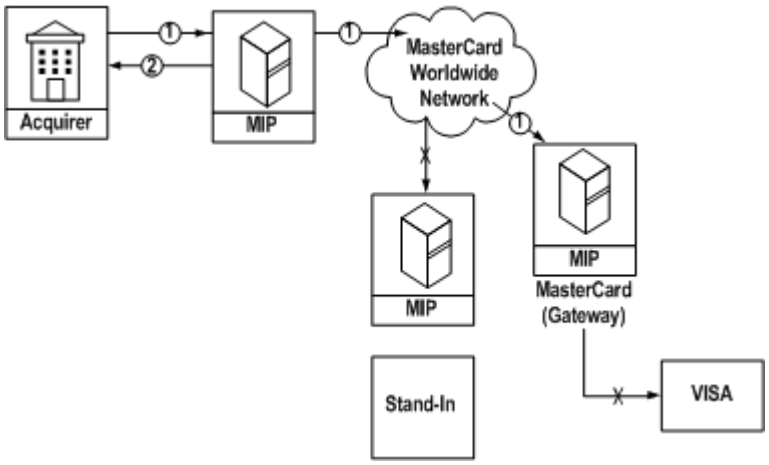


1. The acquirer creates an authorization request conforming to Mastercard specifications for Visa transactions. The Visa authorization request flows through the acquirer MIP to the Mastercard Network.
2. The Authorization Platform routes the request to the Visa network.
3. The Visa network delivers an authorization response to the Mastercard Network.
4. The Authorization Platform delivers the authorization response to the acquirer.
5. The acquirer may return an authorization acknowledgement message.

Secondary Path—Mastercard X-Code Processing

If Mastercard Network connectivity to the Visa network is not functional, Mastercard X-Code processing returns a response of decline.

Authorization Flow Non–Peer-to-Peer Issuer X-Code Processing



1. The acquirer creates an authorization request conforming to Mastercard specifications for Visa transactions. The Visa authorization request flows through the acquirer MIP to the Mastercard Network.
2. The Authorization Platform is unable to route the authorization request to the Visa network or Stand-In processing. X-Code processing at the acquirer MIP returns a response code that indicates, Authorization System or issuer system inoperative and that prompts an acquirer response of decline.

Authorization Flows for Non-Mastercard, Non-Visa Cards

Acquirers can process any of the following card brands via the Mastercard Network.

- American Express
- Diners Club
- Discover
- JCB

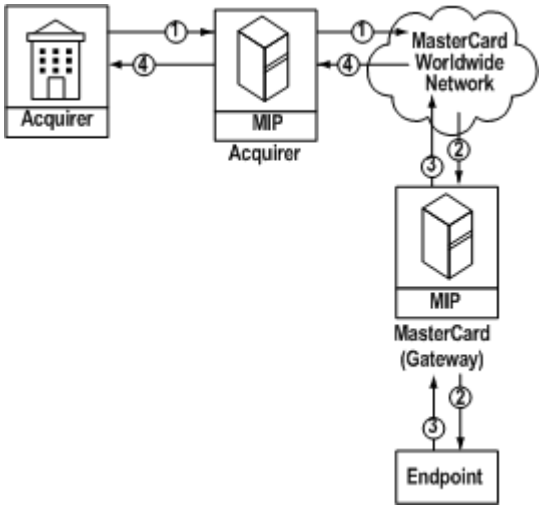
Mastercard also supports processing of a number of private label cards. If the card is among those listed above or one of the supported private label cards, the transaction follows one of the flows depicted in Figure A.10 and Figure A.11.

NOTE: Non-Mastercard ATM transactions are automatically declined at the acquirer MIP.

Primary Path—Direct to Designated Endpoint

The primary path for non-Mastercard, non-Visa transactions always leads directly to the endpoint designated for the specific card brand, as illustrated in the following diagram.

Authorization Flow Direct to Designated Endpoint

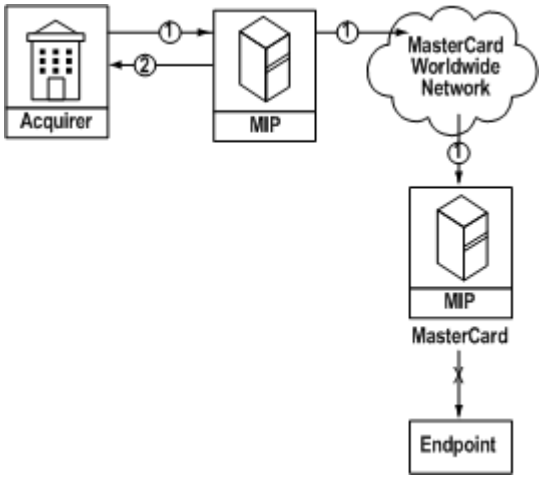


1. The acquirer creates an authorization request conforming to Mastercard specifications for the particular card brand. The request flows through the acquirer MIP to the Mastercard Network.
2. The Authorization Platform routes the authorization request to the appropriate endpoint (such as a processor, card issuer, or other network).
3. The endpoint returns an authorization response to the Mastercard Network.
4. The Authorization Platform delivers the authorization response to the acquirer.

Secondary Path—X-Code Processing

If connectivity to the proper endpoint does not exist, Mastercard performs X-Code processing and issues a refer to card issuer response (except for MO/TO and ATM transactions, which receive a decline response).

Authorization Flow X-Code Processing



1. The acquirer creates an authorization request conforming to Mastercard specifications for the particular card brand. The request flows through the acquirer MIP to the Mastercard Network.
2. The Authorization Platform, unable to route the request to the appropriate endpoint, performs X-Code processing, returning authorization responses as follows:

Response	Transaction Type
Decline	MO/TO, ATM, or merchant suspicious transactions
Refer to Card Issuer	All other transactions

Appendix B Transaction Routing Service

Europe Region. This section explains the transaction routing service functionality on the Mastercard Network.

About Transaction Routing

The Transaction Routing service provides certain routing functionality.

- Allows issuers to define different destination route configurations based on transaction criteria related to an account range.
- Using Network Management Request/0800 messages, supports options to sign on or sign off a single destination route within an account range by group sign-in ID (GSI) or to sign on or sign off an alternate route.
- Supports an account range routing configuration that allows a route to a single destination —the primary issuer.
- Provides extended routing timers for processing Maestro® and Cirrus® transactions on the Mastercard Network.
- Supports routing transactions to an alternate issuer host instead of the Stand-In System.

Transaction-based Routing Preferences

The Authorization Platform allows issuers in the Europe region to configure route destinations at the account range level based on one or more of the following criteria present in the Authorization Request/0100, Authorization Advice/0120—Acquirer-generated, and Reversal Request/0400 messages.

- DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)
- DE 3, subfield 2 (Cardholder "From Account" Type Code)
- DE 3, subfield 3 (Cardholder "To Account" Type Code)
- DE 32 (Acquiring Institution ID Code)
- DE 61 (Point-of-Service [POS] Data), subfield 13 (POS Country Code [or Sub-Merchant Information, if applicable])
- Cardholder verification method based upon the presence of DE 52 (Personal ID Number [PIN] Data) in the incoming message.
  - Signature/offline PIN-based transactions—Authorization requests are categorized as signature/offline PIN when DE 52 (PIN Data) is not present in the Authorization Request/0100 message.
  - Online PIN-based transactions—Authorization requests are categorized as online PIN-based when DE 52 is present in the Authorization Request/0100 message.
- To indicate the appropriate cardholder verification method for Authorization Advice/0120—Acquirer-generated and Reversal Request/0400 messages, acquirers must provide DE 48 (Additional Data—Private Use), subelement 20 (Cardholder Verification Method) and one of the following values:
  - S for a signature/offline PIN-based transaction or if no cardholder verification method (CVM) used.
  - P for an online PIN-based transaction.

- If DE 48, subelement 20 is not present in either the Reversal Request/0400 or Authorization Advice/0120—Acquirer-generated message, the Authorization Platform provides a default value of P (Online PIN-based transaction) to determine the route destination. The Authorization Platform removes DE 48, subelement 20 from the acquirer-generated advice or reversal request message before forwarding the message to the issuer.
- Terminal Type—The Authorization Platform defines transactions as ATM or POS by the values in DE 3, subfield 1 and DE 48, position 1.

The following table shows an example of how different destination routes can be defined for an account range based on transaction criteria. Each destination route is assigned its own Group Sign-in Identifier (GSI), and as a result, a single account range is associated with multiple GSIs.

Destination Route #	Criteria
1 (GSI 1)	Retail and Online PIN-based transactions
2 (GSI 2)	Retail and Signature/Offline PIN-based transactions
3 (GSI 3)	ATM

Network Management Request/0800 Message Sign-On/Sign-Off Options

The Network Management Request/0800 message sign-on and sign-off options include both the Group Sign-in identifier (GSI) and the account range prefix in DE 2. This option allows customers that participate in transaction-based routing to optionally sign on/sign off individual account ranges associated to a group sign-on ID.

Customers that use this option must provide the following values in the Network Management Request/0800 message:

- DE 2 (Primary Account Number [PAN]) with the 5-digit GSI, followed by the 11-digit account range prefix
- DE 70 (Network Management Information Code) with the following values:
  - 063 (Group Sign-On Alternate Issuer Route)
  - 064 (Group Sign-Off Alternate Issuer Route)
  - 065 (Prefix Sign-On by GSI for Primary Route)
  - 066 (Prefix Sign-Off by GSI for Primary Route)
  - 067 (Prefix Sign-On by GSI for Alternate Issuer Route)
  - 068 (Prefix Sign-Off by GSI for Alternate Issuer Route)

DE 70, values 063, 064, 067, and 068 are applicable to customers that use an alternate issuer route instead of the Stand-In System.

The following table shows an example of how different route destinations for an account range can have a different sign-on or sign-off status.

Destination Route #	Criteria	Route Status
1 (GSI 1)	Retail and Online PIN-based transactions	Signed on
2 (GSI 2)	Retail and Signature/Offline PIN-based transactions	Signed on
3 (GSI 3)	ATM	Signed on

Primary Route Only Configuration

The Authorization Platform supports an account range routing configuration that allows a route to a single destination—the primary issuer. When the primary issuer is not available or does not provide a usable response in the allotted time, the Authorization Platform declines authorization request messages with DE 39 (Response Code), value 91 (Authorization System or issuer system inoperative).

Alternate Issuer Host Routing

The Authorization Platform supports alternate issuer host routing that allows issuers to use an alternate issuer authorization route instead of the Stand-In System.

When an alternate issuer host is used instead of the Stand-In System:

- DE 48, subelement 12 (Routing Indicator), value A (Alternate issuer host routing) is present in the Authorization Request/0100 message to indicate that the message has been routed from the Dual Message System, where it was acquired, to the issuer host for alternate route authorization processing.
- DE 48, subelement 12, value P (Primary issuer host routing) is present in the Authorization Request/0100 message to indicate that the message has been routed from the Dual Message System, where it was acquired, to the issuer host for primary route authorization processing.
- DE 121 (Authorizing Agent ID Code), value 000002 is present in the Authorization Advice/0120—System-generated and Reversal Advice/0420 messages to indicate that an alternate issuer route processed the original authorization request.

NOTE: Customers in the Europe region that route to an alternate issuer host for alternate processing, instead of Stand-In processing, will continue to receive advices. Alternate issuer host processing does not send Authorization Advice/0120 or Reversal Request/0400 messages to the alternate host.

Alternate Processing

If an issuer supports an alternate issuer host for alternate route processing and the alternate host is signed out or unavailable, X-Code processing will apply according to product rules.

If X-Code processing is not allowed for a given transaction, response code 91 (Authorization System or Issuer System Inoperative) will be provided in the authorization response to the acquirer.

Routing Timers

The Authorization Platform has a standard, fixed configuration of timers for routing Maestro® and Cirrus® ATM and POS transactions in accordance with the global rules that are published for these brands.

For information about routing timer values, refer to Routing Timer Values.

For More Information

For details about data requirements, refer to the *Customer Interface Specification* manual.

Appendix C File Layouts

This section provides various file layouts.

BIN Table Resource File

The BIN Table Resource File is a fixed-block format with a record size of 150 bytes and a block size of 27900 bytes. The file is identified as MCI.AR.TR52.

Each file consists of the following:

- Header Record
- Detail Record for each account range
- Trailer Record

The BIN Table Resource File is sent to acquirers either as a TR52 production bulk type or as a TR54 test bulk type. Standard Mastercard Global File Transfer methods are used to distribute the BIN Table Resource File.

The BIN Table Resource File layout contains the account ranges (low range and high range) along with the associated issuing member ID (that is, ICA number) and all token account ranges in use.

BIN Table Resource File—File Layout

Field Name	Position	Attribute	Comments/Values
Anonymous Prepaid Indicator	334	ans-1	Valid values: **A** = Anonymous prepaid program and not AMLDS compliant **E** = Anonymous prepaid program and AMLDS compliant **N** = Not prepaid or non-anonymous prepaid program/default **U** = Unknown

BIN Table Resource File Header Record

Field Name	Attribute	Comments
Record Type Identifier	an-1	Code indicating the type of record. Valid value: H (Header)
Transmission Date	n-6	Date the file was created. Format: YYMMDD

Field Name	Attribute	Comments
		YY = Year MM = Month DD = Day
Transmission Time	n-4	Time the file was created. Format: HHMM HH = Hour MM = Minute
Filler	ans-339	Valid values: spaces

BIN Table Resource File Detail Record

Field Name	Attribute	Comments
Record Type Identifier	an-1	Code indicating the type of record. Valid value: D (Detail)
Low Primary Account Range	an-19	The lowest possible account number that would be identified within this authorization account range.
High Primary Account Range	an-19	The highest possible account number that would be identified within this authorization account range.
Acceptance Brand	an-3	Mastercard or other proprietary service mark. Valid values: • MCC (Mastercard® Credit) • DMC (Debit Mastercard®) • MSI (Maestro®) • CIR (Cirrus®) • PVL (Private Label)
Customer ID	n-11	Mastercard ICA number associated with this authorization account range. Format: right justified, leading zeros.
Customer Name	an-70	The customer name.

Field Name	Attribute	Comments
Issuing Country Code	n-3	Licensed Country Code of the account range. Valuable in e-commerce fraud management to help detect inconsistencies between the IP address of the originating purchase and the cardholder billing address that may warrant additional analysis. When used in conjunction with the Local Use flag, a merchant can identify when a card is being used outside of its intended allowed area of use.
Local Use	n-1	Indicates whether cards within the authorization account range may be used outside of the country of issuance. Y = The range is intended for domestic use only. N = The range is intended for use outside the country of issuance.
Authorization only	n-1	Indicates account range is only valid for authorization processing. Y = Authorization only. N = Authorization and Clearing. **NOTE: Accounts identified as Authorization Only that are submitted for clearing will reject with Clearing error code 0011 DE 2 PRIMARY ACCOUNT NUMBER (PAN) ACCOUNT RANGE INVALID. This information is provided in Message Exception/1644-691 messages to the acquirer and reported on report IP857010-AA Error Detail – Input Sequence Report.**
Brand Product Code	ans-3	The Brand Product Code associated with the account range.
Brand Product Description	ans-200	The description of the Brand Product Code named above.

Field Name	Attribute	Comments
Non-reloadable indicator	an-2	Indicates whether the account range is registered as a non-reloadable prepaid card program. Valid values: 01 = non-reloadable prepaid program spaces = reloadable prepaid program or non-prepaid program
Anonymous Prepaid Indicator	ans-1	Valid values: A = Anonymous prepaid program and not AMLDS compliant E = Anonymous prepaid program and AMLDS compliant N = Not prepaid or non-anonymous prepaid program/ default U = Unknown
Filler	ans-18	Valid value: spaces

BIN Table Resource File Trailer Record

Field Name	Attribute	Comments
Record Type Identifier	an-1	Code indicating the type of record. Valid value: T (Trailer)
Number of Records in File	n-12	Total number of records in the file, including header and trailer records. Format: right justified, leading zeros.
Filler	ans-337	Valid values: spaces

PVV/PIN Offset File

The PVV/PIN Offset File has a fixed length of 64 characters.

Each file consists of the following:

- Header Record

- Detail Records
- Trailer Record

Issuers sending their files to the Dual Message System can use Bulk ID RA85 or CONNECT:Direct to send the PVV/PIN Offset file to Mastercard.

Issuers sending their files to the Single Message System can use Bulk ID RM29 (Production), RM31 (MTF), or CONNECT:Direct to send the PVV/PIN Offset file to Mastercard.

PVV/PIN Offset File Header Record

Field Name	Attribute	Length	Comments/Values
Record type ID	Alphanumeric	3	HDR—header record
File version number	Numeric	3	100 (initial version)
Customer ID	Alphanumeric	11	First six digits must contain 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 U: Update (not supported)
Filler	Alphanumeric	20	Spaces

PVV/PIN Offset File Detail Record

Field Name	Attribute	Length	Comments/Values
Record type ID	Alphanumeric	3	DTL—detail record
Update code	Alphanumeric	1	A = add/update

Field Name	Attribute	Length	Comments/Values
			D = delete (not supported)
PAN	Alphanumeric	19	With trailing spaces
Card expiry date	Numeric	4	YYMM (must contain a valid year and month)
Card sequence number	Numeric	1	Must contain the sequence number associated with the PAN or 0. A value of 0 indicates that the card sequence number should not be used as criteria when matching to the PVV file.
PVV/PIN Offset	Numeric	6	Trailing spaces
Filler	Alphanumeric	30	Spaces

PVV/PIN Offset File Trailer Record

Field Name	Attribute	Length	Comments/Values
Record type ID	Alphanumeric	3	TRL—trailer record
Number of detail records	Numeric	11	Detail record count
Filler	Alphanumeric	50	Spaces

In-flight Commerce Blocked Gaming File

The In-flight Commerce (IFC) Blocked Gaming File has the certain specifications.

Frequency:	Generated twice per month
Media:	Bulk File (bulk type T104) or Mastercard File Express (ID AM005)
LRECL:	100
Format:	Fixed block

Block Size: 1,000

Refer to the following file layouts for both bulk file and Mastercard File Express.

IFC Blocked Gaming File Header Record

Field Name	Position	Length	Comments/Valid Values
Record Type	1–3	3	Constant RHD
Processing Date	4–11	8	Date of file creation. Format: = YYYYMMDD YYYY = Year MM = month DD = Day Valid value: Must be numeric
Filler	12–100	89	Valid values: spaces

IFC Blocked Gaming File Financial Detail Record

Field Name	Position	Length	Comments/Valid Values
Record Type	1–3	3	Constant DTL
From BIN	4–22	19	First account number in the BIN range to be blocked. Format: Numeric, left-justified; zero-filled.
To BIN	23–41	19	Last account number in the BIN range to be blocked. Format: Numeric, left-justified; nine-filled.
ICA	42–46	6	ICA number associated with the blocked BIN. Format: Numeric, left-justified; zero-filled.

Field Name	Position	Length	Comments/Valid Values
Effective Date	47–54	8	Date the BIN should begin being blocked. Format: = YYYYMMDD YYYY = year MM = month DD = day Valid value: Must be numeric
Filler	55–100	46	Valid values: spaces

IFC Blocked Gaming File Trailer Record

Field Name	Position	Length	Comments/Valid Values
Record Type	1–3	3	Constant TRL
Record Count	4–12	9	Numeric
Filler	13–100	88	Valid values: spaces

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.