Return to Menu

MasterCard International

Information about this Replacement

Replacement

The October 2005 *MDS Online Specifications* manual replaces your existing manual.

What is in the new version?

This new version reflects changes effective October 2005.

Please refer to:

- "Summary of Changes" for a comprehensive list of changes reflected in this update.
- "Using this Manual" for a complete list of the contents of this manual.

Billing

MasterCard will bill principal members for this document. Please refer to the *MasterCard Consolidated Billing System Manual* for billing-related information.

Questions?

If you have questions about this manual, please contact the Customer Operations Services team or your regional help desk. Please refer to "Using this Manual" for more contact information.

MasterCard is Listening…

Please take a moment to provide us with your feedback about the material and usefulness of the *MDS Online Specifications* manual using the following e-mail address:

publications@mastercard.com

We continually strive to improve our publications. Your input will help us accomplish our goal of providing you with the information you need.

MasterCard International

Summary of Changes

***MDS Online Specifications*, October 2005**

Change Summary	Description of Change	Where to Look
MCCR change to CCA	Replaced references to MCCR with Currency Conversion Assessment	Entire manual
Removed sample of the Implementation Task List form	Removed the Implementation Task List and references to its use from the manual. This form is no longer used.	Chapter 1
Updated key interchange information	Updated Key Exchange interval information	Chapter 2 Chapter 6
Added DE 112 to the 0220 and 0230 messages	Added DE 112 to the 0220 and 0230 messages and updated the comments column to be more descriptive	Chapter 3 Chapter 4
Updated DE 126	Updated DE 126, Switch Private Data, with Cross border acquiring values and information	Chapter 3 Chapter 4
Track 2–DE 35 Discretionary Data	Corrected discretionary data length for ISO DE 35, Track 2 Data	Chapter 4
Updated DE 22	Updated the valid values for DE 22, Point of Service Entry Mode	Chapter 4
Updated DE 39	Removed invalid code 79 for DE 39, Response Code	Chapter 4
Updated DE 43	Updated the valid values for DE 43, Card Acceptor Name and Location	Chapter 4
Updated DE 112	Updated transaction types for DE 112, Additional Data (National Use)	Chapter 4
Updated VPN infrastructure and the MasterCard New York Global Hub	Updated information explaining VPN infrastructure and the MasterCard New York Global Hub	Chapter 5

MasterCard International

MDS Online Specifications

October 2005

Trademarks

Trademark notices and symbols used in this manual reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Media

This document is available:

- On MasterCard OnLine®
- On the *MasterCard Electronic Library* (CD-ROM)
- On the MDS Suite (CD-ROM)

MasterCard International Incorporated
2200 MasterCard Boulevard
O'Fallon MO 63368-7263
USA

1-636-722-6100

www.mastercard.com

Using this Manual

Chapter 1 Implementation Planning

Chapter 3 Message Layouts

Chapter 5 Communication Protocols

Chapter 6 Encryption

Chapter 7 Database Forms

Using this Manual

This chapter contains information that helps you understand and use this document.

Purpose

The MasterCard *MDS Online Specifications* is one of the four manuals comprising the MasterCard® Debit Switch Suite that defines the services and processing requirements for the MasterCard Debit Switch (MDS). The MasterCard® Debit Switch Suite consists of:

- *MDS Online Specifications*
- *MDS Programs and Services*
- *MDS Settlement and Reports*
- *NICS Users' Guide*

The *MDS Online Specifications* manual serves as one of the primary technical references for all debit programs and services supported by MasterCard.

Audience

MasterCard provides this manual for members and their authorized agents. Specifically, the following personnel should find this manual useful:

- MasterCard members directly connected to the MasterCard® Debit Switch
- Third-party processors directly connected to the MasterCard® Debit Switch

Overview

The following table provides an overview of this manual:

Chapter	Description
Table of Contents	A list of the manual's chapters and subsections (each entry references a chapter and page number)
Using this Manual	A description of the manual's purpose and its contents
1 Implementation Planning	An overview of all implementation tasks and testing requirements to aid new participants in planning a successful and timely implementation of services.
2 Transaction Messages	Illustrates and describes the various message types used for transaction processing.
3 Message Layouts	Identifies all of the required, conditional, optional, or switch-generated data elements within each individual ISO 8583–1987 message.
4 Data element Definitions	Provides a detailed definition of all data elements used in online application messages.
5 Communication Protocols	Illustrates and defines options and requirements for establishing a link to the MasterCard® Debit Switch.
6 Encryption	Illustrates and defines procedures and requirements for key generation, key maintenance, and PIN encryption.
7 Database Forms	Defines the procedures for completing the forms required to create and maintain member records in the MasterCard® Debit Switch database.

Oct 2005

Excerpted Text

At times, this document may include text excerpted from another document. A note before the repeated text always identifies the source document. In such cases, we included the repeated text solely for the reader's convenience. The original text in the source document always takes legal precedence.

Language Use

The spelling of English words in this manual follows the convention used for U.S. English as defined in *Merriam-Webster's Collegiate Dictionary*. MasterCard is incorporated in the United States and publishes in the United States. Therefore, this publication uses U.S. English spelling and grammar rules.

An exception to the above spelling rule concerns the spelling of proper nouns. In this case, we use the local English spelling.

Times Expressed

MasterCard is a global company with locations in many time zones. The MasterCard operations and business centers are in the United States. The operations center is in St. Louis, Missouri, and the business center is in Purchase, New York.

For operational purposes, MasterCard refers to time frames in this manual as either "St. Louis time" or "New York time." Coordinated Universal Time (UTC) is the basis for measuring time throughout the world. You can use the following table to convert any time used in this manual into the appropriate time in another time zone:

Oct 2005

	St. Louis, Missouri USA Central Time	Purchase, New York USA Eastern Time	UTC
Standard time (last Sunday in October to the first Sunday in April [a])	09:00	10:00	15:00
Daylight saving time (first Sunday in April to the last Sunday in October)	09:00	10:00	14:00

[a] For Central European Time, the last Sunday in October to the last Sunday in March.

Revisions

MasterCard periodically will issue revisions to this document as we implement enhancements and changes, or as corrections are required.

With each revision, we include a "Summary of Changes" describing how the text changed. Revision markers (vertical lines in the right margin) indicate where the text changed. The month and year of the revision appear at the right of each revision marker.

Occasionally, we may publish revisions or additions to this document in a *Global Deposit Access Operations Bulletin* or other bulletin. Revisions announced in another publication, such as a bulletin, are effective as of the date indicated in that publication, regardless of when the changes are published in this manual. Oct 2005

Related Information

The following documents and resources provide information related to the subjects discussed in this manual. Please refer to the *Quick Reference Booklet* for descriptions of these documents.

- *Chargeback Guide*
- *Cirrus® Worldwide Operating Rules*
- *Data Communications Manual*
- *Global Deposit Access Implementation Guide for Maestro and Cirrus*
- *Maestro® Global Rules*
- *MasterCard Consolidated Billing System Manual*
- *MasterCard Debit Financial Simulator*
- *MasterCard Member ICC Testing Procedures—Debit*
- *MDS Programs and Services*
- *MDS Settlement and Reports*
- *NICS™ Users' Guide*
- *Settlement Manual*

Oct 2005

Debit members that also process transactions using the Authorization (01xx) message format should reference the above manuals and the following manuals:

- *Account Management User Manual*
- *Authorization System Manual*

In addition to the documents listed previously in this chapter, the following international standards publications may also be useful if you are implementing a new ATM or POS program or if you are in the process of converting to the MasterCard® Debit Switch ISO-8583 CIS online message format interface.

- ISO 7810–1985: Identification Cards—Physical Characteristics
- ISO 7811–1985: Identification Cards—Recording Technique
- ISO 7812–1987: Identification Cards—Numbering System and Registration Procedure for Issuer Identifiers
- ISO 7813–1990: Identification Cards—Financial Transaction Cards
- ISO 3166–1988: Codes for the Representation of Names of Countries
- ISO 4217–1990: Codes for the Representation of Currencies and Funds
- ISO 9564–1991: Banking-Personal Identification Number Management and Security Part 1: PIN Protection Principals and Techniques

Members that use the Cirrus® service and logo or that process online debit transactions should refer to the debit processing manuals recommended by the Customer Operations Services team.

For definitions of key terms used in this document, please refer to the *MasterCard Dictionary* available via a link on the Member Publications home page (on MasterCard OnLine® (www.mastercardonline.com), and the *MasterCard Electronic Library* CD-ROM).

Oct 2005

To order MasterCard manuals, please use the Ordering Publications service on MasterCard OnLine®, or contact the Customer Operations Services team.

Support

Please address your questions to the Customer Operations Services team as follows:

Phone: 1-800-999-0363 or 1-636-722-6176

1-636-722-6292 (Spanish language support)

Fax: 1-636-722-7192

E-mail:

Canada, Caribbean, Latin America, South Asia/Middle East/Africa, and U.S.	customer_support@mastercard.com
Asia/Pacific:	
Australia and New Zealand	member_operations@mastercard.com
China, Hong Kong, and Taiwan	helpdesk.gc@mastercard.com
South East Asia	helpdesk.singapore@mastercard.com
Japan/Guam	helpdesk.tokyo@mastercard.com
Korea	korea_helpdesk@mastercard.com
Europe	css@mastercard.com
Spanish language support	lagroup@mastercard.com
Vendor Relations, all regions	vendor.program@mastercard.com

Address: MasterCard International Incorporated
Customer Operations Services
2200 MasterCard Boulevard
O'Fallon MO 63368-7263
USA

Telex: 434800 *answerback*: 434800 ITAC UI

Oct
2005

Member Relations Representative

Member Relations representatives assist U.S. members with marketing inquiries. They interpret member requests and requirements, analyze them, and if approved, monitor their progress through the various MasterCard departments. This does not cover support for day-to-day operational problems, which the Customer Operations Services team addresses.

For the name of your U.S. Member Relations representative, contact your local Member Relations office:

Atlanta	1-678-459-9000
Chicago	1-847-375-4000
Purchase	1-914-249-2000
San Francisco	1-925-866-7700

Regional Representative

The regional representatives work out of the regional offices. Their role is to serve as intermediaries between the members and other departments in MasterCard. Members can inquire and receive responses in their own languages and during their offices' hours of operation.

For the name of the location of the regional office serving your area, call the Customer Operations Services team at:

Phone: 1-800-999-0363 or 1-636-722-6176

1-636-722-6292 (Spanish language support)

1 Implementation Planning

This chapter provides an overview of the project planning and review process for new and existing participants.

Overview

This chapter provides an overview of the project planning and review process for new and existing participants.

An essential component to successful implementation is the review of the project among regional MasterCard, Maestro, and Cirrus staff and all appropriate personnel within your organization. For best results, schedule this review early in the project-planning phase.

Note **Before you initiate the planning process, MasterCard strongly encourages you to contact your MasterCard Regional Office to identify the requirements related to a particular project.**

The following process should occur during the review meeting:

Stage	Description
1.	MasterCard will answer all general questions regarding the MasterCard® Debit Switch (MDS) or this implementation guide.
2.	MasterCard and your organization will establish a detailed project plan to identify due dates and responsibilities and to ensure that all parties agree on the process components.
3.	MasterCard and your organization will review and answer detailed technical questions or operational guidelines and establish specific timeframes for testing.
4.	MasterCard and your organization will schedule additional review sessions, as necessary. These additional review sessions will guarantee consistent, clear communication regarding the status of the implementation project, and generate a timely response to issues that may arise.

Oct
2005

Objectives of Acceptance Testing

System testing of all MDS processors is an integral part of the implementation plan. The MDS, as the provider of routing, message translation, and settlement services, tests all processors' system environments before implementation to ensure the overall integrity of the MDS environment.

Each processor will receive the standard acceptance test scripts from the MasterCard Regional Office and their Customer Implementation Services Specialist. These scripts will assist each processor in complying with the standard processing requirements of the MDS. Using these scripts makes it possible to test all conditions expected in the MDS production environment. MasterCard will review the completed acceptance tests, including receipt of test transactions and the documented results of each test transaction, to ensure that the processor meets all processor testing requirements. Oct 2005

Note **MasterCard will not allow any processor to connect to the MDS unless that processor has completed the minimum acceptance test requirements.**

MasterCard provides processor testing as a continuing service of the MDS. To test each processor's online interface, all processors must accept acquirer and issuer processor functionality. All processors can use the test facilities to re-test their internal system changes and by scheduling convenient times with your MasterCard Regional Office, the Debit Payment Systems— Customer Implementation Services Specialist, or both. Oct 2005

MasterCard Debit Switch Test Environment

The MDS maintains a test platform separate from the production system. This test environment enables processors to perform transaction processing with parameters and timeframes that mirror the production system. Settlement cut-over is included in cycle testing so processors can complete batch processing and balance back to the MDS before going live.

Testing Requirements

To obtain further information on test requirements for implementation, contact your MasterCard Regional Office or the Customer Implementation Services Specialist assigned to your project. Oct 2005

Online Testing

Members use the MDS Test Facility to complete the testing process. After completing the initial testing with the simulator, members should have resolved any message format and procedural issues.

Background

The testing process ensures that online testing with a Customer Implementation Services Specialist focuses on the message routing and processing aspects of testing and testing the member interface to the MDS. Online testing also creates settlement reports and files, allowing members to test file transfer and processing.

Oct 2005

Requirements for New Members

All new members that will have a direct connection to the MDS network must complete online testing with the MDS Test Facility. Required online testing includes:

- Financial functionality for member-supported products and services
- Validation of processing settlement reports and files
- Reject Reason Code Mapping
- Administrative Messages

Warning **During acceptance testing, members must not make changes to their hardware or software environments. Any changes made by members will require members to begin the testing process again.**

Requirements for Existing Members

Existing members may conduct testing with the MDS Test Facility at any time. They can use the test facility to conduct authorization testing for MDS release changes or to test any changes to their authorization interfaces with MasterCard.

Members also can use the MDS Test Facility to test MDS release changes and other file transmissions between members and MasterCard.

Scheduling Test Time

To schedule test time, contact your MasterCard Regional Office or the Customer Implementation Services Specialist assigned to your project.

Note **Simulator testing is required before online testing can occur. For further information on member testing procedures, scheduling, canceling, or pricing, please contact MasterCard Regional Office or the Customer Implementation Services Specialist assigned to your project.**

Canceling Test Time

To cancel scheduled test time, contact your MasterCard Regional Office or the Customer Implementation Services Specialist assigned to your project.

Processor Debit Switch Test Environment

MasterCard highly recommends that processors establish a separate test platform for online testing with the MDS. This platform should consist of the following:

- One of each terminal type supported in the production environment and one host processor.
- A host processor capable of communicating directly with the MDS by using separate telecommunication lines and modems. The MDS can provide separate ports on a member MIP and maintain dial-up modems for testing. All processors must coordinate dial-up testing with MasterCard.
- Terminals and host that have the same functionality as the production system, and the capability to simulate production routing and authorization processes
- Full batch processing functionality to test reconciliation, settlement, and reporting functions

To ensure compliance with any applicable government regulations, MasterCard recommends verification of transaction activity (up to and including a customer's statement).

Electronic Fund Transfer (EFT) Services

As a provider of Electronic Fund Transfer (EFT) services, all processors must successfully meet and complete all test requirements before becoming "live" in the MDS production system.

Acceptance Testing Requirements

Each processor is required to complete acceptance testing successfully as an acquirer processor, an issuer processor, or both. A processor can only process transactions on the production system for which they have completed acceptance testing.

The acceptance process requires two consecutive error-free days of testing; therefore, testing cannot begin on a Friday. If a processor fails any portion of the testing process, the entire testing process must begin again.

The processor must test only those transaction types supported by both the processor and the MDS, before the processor can participate in the MDS production environment.

Simulator Testing Requirements for New Members

New members can use the simulator to test their systems for compliance with the processing requirements of MasterCard. All new members that will have a direct connection to the MDS must purchase the MasterCard Test Simulator—Debit software package.

MasterCard requires members to perform simulator testing before conducting online testing. New members must use the simulator to run predetermined scripts to test their issuing and acquiring host systems.

Members also must submit simulator trace files to Customer Implementation Services Specialist for review. If the trace files are error-free and meet testing requirements, MasterCard Customer Implementation Services staff will confirm the successful completion of simulator testing and arrange for members to conduct online testing.

Oct 2005

New Processor Test Scripts

Processors connecting to the MDS for the first time are required to complete all applicable acceptance test scripts. Members can obtain these scripts during the project planning phase. MasterCard makes every attempt to test the full variety of conditions that will occur in an operations environment in order to minimize production problems when the processor begins "live" processing. Each script requires the processor to accommodate specific conditions.

Personnel assigned to perform acceptance testing should carefully review the appropriate test plan to ensure that all identified conditions can be produced during any given test day. Conditions that cannot be accommodated in a timely manner during the testing process must be brought to the attention of the MasterCard Regional Office and the Customer Implementation Services Specialist.

Oct 2005

The Customer Implementation Services Specialist will determine if the problem identified by the processor makes it unable to satisfy all acceptance testing requirements. The Specialist will document any variances. Significant variances from the approved test plan will be allowed only if the MasterCard Regional Office and the Customer Implementation Services representative give approval.

Note **Members must contact their MasterCard Regional Office and the Customer Implementation Services representative to initiate all scheduled test sessions. Therefore, members must ensure that their testing personnel have the necessary facilities and authority to dial-out from their Test Data Center.**

Simulator Testing Requirements for Existing Members

Existing members already should have the MasterCard Debit Financial Simulator software package. MasterCard strongly encourages members to use the simulator for all optional MDS release testing before conducting any online testing. MasterCard may **require** simulator testing for certain MDS releases.

MasterCard must verify simulator testing for all member-initiated system changes that may affect the member's interface to the MDS. Also, any existing members that implement new products or services, must complete appropriate simulator testing before performing any online testing.

Testing Multiple Terminals

If multiple terminals are available, the processor should perform test transactions simultaneously on multiple terminals to emulate a "live" environment.

Testing Unique Requirements

Testing of all applicable transaction processing scenarios for a specific processor may require the addition, modification, or deletion of test cases. All additions and deletions of test cases must be coordinated with your MasterCard Regional Office or your Customer Implementation Services representative. Your MasterCard contact will generate custom acceptance test scripts for all processors that have unique requirements.

Test Card Requirements

Issuer Processor Testing

The processor must create a series of test card Track 2 data and PINs, to test and analyze multiple test case scenarios (both valid and invalid). Each processor must supply the MDS with a series of test card Track 2 layouts with PINs, for a single financial institution for which it performs issuer processing services.

Note **Processors must block test card information from being used in the production system.**

Oct 2005

Issuer processors should use the sample table included in the Issuer Functionality Form to provide the required Track 2 data to the MDS. Use the following rules to determine the data requirements for a particular card:

- Processors that do not support balance inquiry (BI) transactions should not provide data for any cards whose identifier begins with "BI."
- Processors should not provide test data for cards related to unsupported account types. For example, processors that do not support the savings account type are not required to provide data for any of the test cards with "SAV" in their identifier.

Note **All of the "VALID" cards relate to all account types, and processors must always provide Track-2 data and PINs for these cards.**

- Processors must provide test PINs in the PIN column for each test card required for acceptance testing.

Test Card Master Listing

The master listing describes any special conditions attached to a card. It also lists the type of balance (such as positive or negative, available or ledger account balance) associated with cards to be used for balance inquiry (BI) transactions. Each card, identified by a name, is associated with one or more cardholder account types (such as checking, savings, or credit card accounts), as indicated by the master list. To obtain the master listing of all test cards used to generate transactions during acceptance testing, contact your MasterCard Regional Office.

Acquirer Processor Testing

For acquirer processing systems MasterCard will provide Track 2 information. During the project planning phase, specific information will be available. Processors should contact their MasterCard Regional Office or their Customer Implementation Services representative.

Recommended ATM Screen Sets

The appropriate use of issuer-generated response codes is critical to communicate accurately to the cardholder the reason for the denial. Misrepresentation or a lack of information for the cardholder increases their frustration and affects use. This also affects processor performance because multiple declines occur when the cardholder does not receive meaningful feedback. Issuers should use the mapping of recommended screen messages as shown in Table 1.1.

It is the acquirer's responsibility to describe clearly to the cardholder the intent of the action taken by the issuer. Acquirers should use the following information to ensure that they are interpreting the response codes accurately.

ISO 8583 (1987) Financial Transaction Request/0200 Response Message Format

Response Codes are in DE 39 of the ISO 8583 (1987) Financial Transaction Request/0200 message format. The table below provides the valid response codes for the Financial Transaction Request/0200 message format as used by the MDS. It also lists definitions, expected acquirer actions, and examples of recommended English-language screen messages. Contact your MasterCard Regional Office for examples of screen messages in other languages.

Table 1.1—ISO 8583 (1987) Financial Transaction Request/0200 Format—Financial Transaction Request Response/0210 Messages Response Code Mapping

Code	Response Code Definitions	Issuer Usage	Acquirer Action	Recommended ATM Screen Message
00	Approved or completed successfully	Transaction request approved	Approve	
04	Capture card	Transaction request declined The acquirer should retain the card. No reason is provided for this action.	Capture	• Your card has been retained. Please contact your card issuer. Or, • Your card issuer has declined your request and has instructed me to retain your card. Please contact your card issuer.

Code	Response Code Definitions	Issuer Usage	Acquirer Action	Recommended ATM Screen Message
12	Invalid transaction	Transaction request declined The transaction request is not supported or is not valid for the BIN. The MDS uses this response code exclusively. Card issuers or Intermediate Network Facilities (INFs) should use response code 57.	Decline	• I am sorry you have selected an invalid transaction. Do you want to try another transaction? Or, • I am sorry you have selected an invalid transaction. Please try a different transaction type.
13	Invalid amount	Transaction request declined The requested amount is below the minimum limit set by the issuer for the type of transaction requested.	Decline	• You have selected an invalid amount. Please select amount in multiples of _____ Or, • Your card issuer has declined your request because the amount requested is invalid. Please try a greater amount.
14	Invalid card number	Transaction request declined The presented card number is not valid on the issuer's file.	Decline	• I am sorry I am unable to process your request. Please contact your card issuer. Or, • Your request is declined because your card issuer did not recognize your card number.
15	Invalid issuer	Transaction request declined The transaction request contains a BIN that is unsupported. This response code is valid for MDS usage only.	Decline	• I am sorry I am unable to process your request. Please contact your card issuer. Or, • Your transaction request is declined because your card is not supported at this location.
30	Format error	Transaction request declined Improper format	Decline	I am sorry I am unable to process your request. Please contact your card issuer.

Code	Response Code Definitions	Issuer Usage	Acquirer Action	Recommended ATM Screen Message
41	Lost card	Transaction request declined The acquirer should retain the card. This is a reported lost card.	Capture	• Your card has been retained. Please contact your card issuer. Or, • Your card issuer has declined your request and has instructed me to retain your card because it has been reported lost. Please contact your card issuer.
43	Stolen card	Transaction request declined The acquirer should retain the card. This is a reported stolen card.	Capture	• Your card has been retained. Please contact your card issuer. Or, • Your card issuer has declined your request and has instructed me to retain your card because it has been reported stolen. Please contact your card issuer.
51	Insufficient funds/over credit limit	Transaction request declined The request will result in an over credit limit or insufficient funds condition.	Decline	• I am unable to process for insufficient funds. Please contact your card issuer. Or, • Your request is declined due to insufficient funds. Please contact your card issuer.
54	Expired card	Transaction request declined The card number presented is expired.	Decline	Your request is declined because your card has expired. Please contact your card issuer.
55	Invalid PIN	Transaction request declined The cardholder-entered PIN is incorrect.	Decline	• You have entered your PIN incorrectly. Do you want to try again? Or, • Your request is declined because the PIN you entered is incorrect.

Code	Response Code Definitions	Issuer Usage	Acquirer Action	Recommended ATM Screen Message
57	Transaction not permitted to issuer/ cardholder	Transaction request declined The card issuer or INF declines the transaction request because it is not supported or is not permitted for the card number presented. The MDS generates response code 12 when a transaction is declined for invalid transaction selection.	Decline	• I am sorry you have selected an invalid transaction. Do you want to try another transaction? Or, • Your request is declined because it is not supported. Please try a different transaction type.
61	Exceeds withdrawal amount limit	Transaction request declined The withdrawal amount is in excess of daily defined maximums.	Decline	• You have exceeded the withdrawal limit. Do you want to select another amount? Or, • You have exceeded the daily withdrawal limit. Please contact your card issuer.
62	Restricted card	Transaction request declined The card number has been restricted for the type of use requested.	Decline	• I am sorry I am unable to process your request. Please contact your card issuer. Or, • Your request has been denied by your card issuer because your card has been restricted. Please contact your card issuer.
75	Allowable number of PIN tries exceeded	Transaction request declined The cardholder has incorrectly entered the PIN in excess of the allowable number of tries established by the issuer.	Decline	You have exceeded the amount of times you can enter your PIN. Please contact your card issuer.

Code	Response Code Definitions	Issuer Usage	Acquirer Action	Recommended ATM Screen Message
78	Invalid or nonexistent account specified (general)	Transaction request declined The from (debit) or to (credit) account specified in the transaction is non-existent or is not associated with the card number presented. Issuers should use this response code to decline a transfer request because of a nonexistent or invalid account.	Decline	Your request is declined because the account selected is invalid.
79	Invalid business date	Transaction request declined The business date is not valid. This response code is valid for MDS usage only.	Decline	I am sorry I am unable to process your request. Please contact your card issuer.
80	System not available	Transaction request declined The issuer system is not available. INF can generate this response code when the issuer systems are down, or when it cannot complete a transaction request because the issuer's applications or files are not available.	Decline	• I am sorry I am unable to process your request. Please contact your card issuer. Or, • Your request is declined because your card issuer's systems are not available. Please try again later.
91	Destination processor (customer processor system [CPS] or INF) not available	Transaction request declined The destination processor is not available. The MDS generates this response code when it cannot deliver a transaction request because the destination processor does not have an online connection to the MDS.	Decline	• I am sorry I am unable to process your request. Please contact your card issuer. Or, • Your request is declined because your card issuer's systems are not available. Please try again later.
92	Unable to route transaction	Transaction request declined Insufficient information for routing	Decline	I am sorry I am unable to process your request. Please contact your card issuer.

Code	Response Code Definitions	Issuer Usage	Acquirer Action	Recommended ATM Screen Message
96	System error	Transaction request declined A system failure has occurred or the files required for the authorization are not available.	Decline	I am sorry I am unable to process your request. Please contact your card issuer.

2 Transaction Messages

This chapter provides definitions of all message types used by the MasterCard® Debit Switch (MDS).

Overview

This chapter of the *MDS Online Specifications* provides a definition of all ISO 8583–1987 message types employed by the MasterCard® Debit Switch (MDS). Also included are transaction flow diagrams that illustrate both standard and exception (such as error condition) message processing requirements at the online application programming level.

This chapter also discusses the basic transaction processing techniques employed by the MDS in its implementation of the ISO 8583–1987 message standard. It provides processors with a general overview of the underlying logic for all transaction flow scenarios.

Message Processing Conventions

The ISO 8583–1987 online interface uses several basic processing conventions that are implemented uniformly for all financial products. Review these conventions thoroughly before the development of an ISO 8583–1987 interface, as they provide the foundation from which all transaction flow logic is derived.

Some of the most important ISO 8583–1987 message processing concepts are discussed on the following pages, including:

- Issuer Post-On-Authorization Concept
- Acquirer Response Acknowledgement Concept
- Guaranteed Advice Delivery Concept

Issuer Post-On-Authorization Concept

ISO 8583–1987 online application message processing uses the "post-on-authorization" technique for handling issuer processing system transaction processing for both Authorization/01xx messages and Financial Transaction/02xx messages. This technique ensures MDS integrity and minimizes resource use.

Note

As defined within the ISO 8583–1987 specification, the term "post-on-authorization" does not refer to the actual posting of cardholder accounts for billing purposes. "Post-on-authorization" refers only to the technique used to maintain accurate settlement reconciliation totals between the MDS and any attached issuer or acquirer processing systems. The issuer's cardholder account billing subsystem(s) handles the actual posting of cardholder accounts for billing purposes. The online processing procedures described in this manual do not include the issuer billing function.

The issuer post-on-authorization procedure does not require the use of Completion Confirmation or Completion Response messages for processing of an Authorization Request/0100 messages or Financial Transaction Request/0200 messages at the issuer processing system. This makes it significantly more efficient than the alternative technique known as "post-on-completion." "Post-on-completion" is often used in other EFT environments. It requires Completion Confirmation and Completion Response messages to be transmitted between the acquirer and issuer.

Upon receipt of a Financial Transaction Request Response/0210 message from an issuer, the MDS assumes the transaction approval will affect the cardholder's account and handles any subsequent exception and reversal situations accordingly. The MDS does not return a Financial Transaction Confirmation message back to the issuer. The issuer always assumes that the acquirer normally completed the transaction, **unless otherwise advised** with a Financial Transaction Reversal Advice/0420 message from the MDS or the acquirer processing system.

Late Responses

If the MDS receives a late response from the issuer to an interactive request message (such as a late Financial Transaction Request Response/0210 message), **the MDS will have timed-out the issuer processing system**.

For financial transactions, the MDS responds to the late message, the issuer processing system Financial Transaction Request Response/0210, with an Acquirer Reversal Advice/420 message. This indicates to the issuer that the MDS identified the Financial Transaction Request Response/0210 message as a late response and any financial impact to the cardholder's account must be reversed. Oct 2005

When an Acquirer Reversal Advice/0420 message is received, the issuer processing system must assume that either the MDS timed-out the issuer message and invoked Stand-In processing (if applicable), or sent a denial to the acquirer. The issuer processing system must always **reverse** any previous update to the cardholder's account. The issuer may receive one or more advice messages (for example, Financial Transaction Advice/0220 message or Acquirer Reversal Advice/0420 message, as appropriate) to indicate the specific action taken and the completion status of the transaction. Oct 2005 Oct 2005

If the issuer has not selected Stand-In processing options, the MDS automatically transmits a Financial Transaction Request Response/0210 message to the acquirer with a negative (transaction denied) response code.

If a debit MasterCard issuer does not support an Acquirer Reversal Advice/0420 message, the issuer will receive a Financial Transaction Negative Acknowledgement/0290 message. Oct 2005

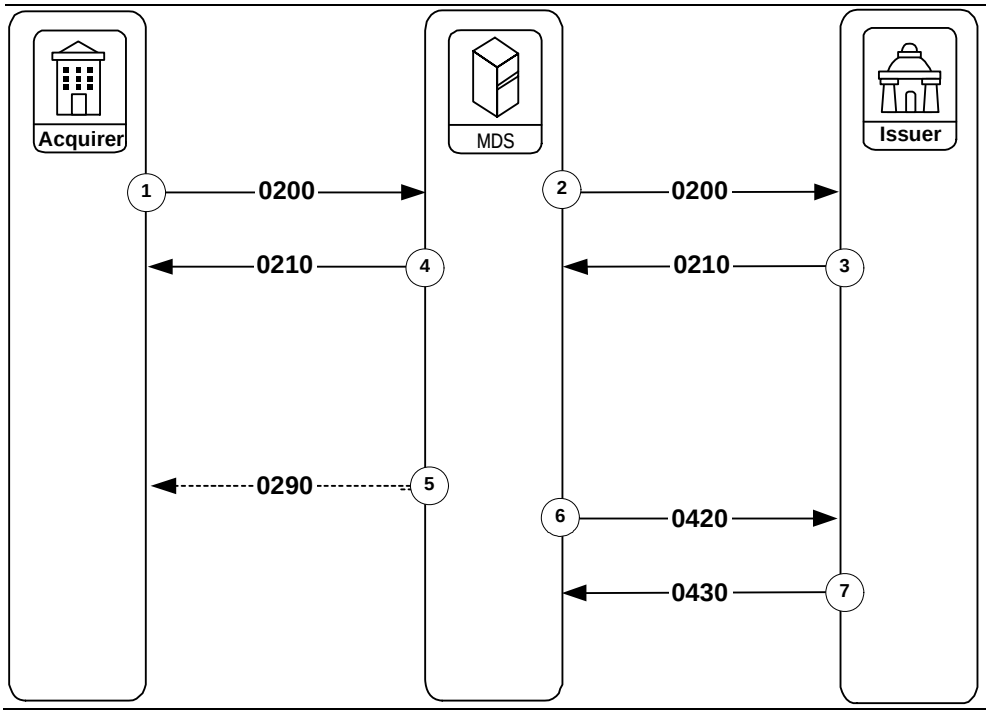
Acquirer Response Acknowledgement Concept

The ISO 8583–1987 online interface optionally supports a positive response acknowledgment technique to help ensure that acquirer processing systems acknowledge receipt of Financial Transaction Request Response/0210 messages at the online application level.

Simple acknowledgment of interactive Financial Transaction messages at the telecommunications protocol level may not provide necessary network integrity for transactions that may be "in progress" when an acquirer processing system fails. Consequently, transaction flows for Financial Transaction/02xx messages may include the option for the acquirer to acknowledge receipt of Financial Transaction Request Response/0210 messages from the MDS.

The following table illustrates the acquirer response acknowledgment concept optionally supported for Financial Transaction/02xx messages.

Acquirer Response Acknowledgement



Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	The issuer generates a Financial Transaction Request Response/0210 message and sends it to the MDS.
4.	The MDS forwards the Financial Transaction Request Response/0210 message to the acquirer.
5.	The MDS sends a Financial Transaction Negative Acknowledgement/0290 message to the acquirer. In this message, DE 39 (Response Code) contains the value 96.
6.	The MDS sends an Acquirer Reversal Advice/0420 message to the issuer.
7.	The issuer responds with an Acquirer Reversal Advice Response/0430 message to the MDS.

Guaranteed Advice Delivery Concept

The ISO 8583–1987 online specification, as implemented on the MDS, employs a guaranteed advice message delivery concept for all advice messages transmitted through the MDS.

The guaranteed advice message delivery facility provides message routing capabilities that, when an advice message is forwarded from any processor (acquirer or issuer) to the MDS, allow the MDS will do the following:

1. Secure the advice message for future delivery.
2. Respond to the originator of the advice message with an Advice Response to indicate that the advice message has been received and secured by the MDS.
3. Forward the advice message to the appropriate receiving entity.

If the MDS cannot deliver an advice message immediately (for example, due to a system or communication failure at the receiving destination) the MDS will store the message using an integrated store-and-forward (SAF) processing facility. The SAF process automatically delivers the message to its proper destination when communication with the endpoint destination has been restored. Thus, the delivery of all advice messages routed through the MDS is **guaranteed**.

Recipients of an advice message must acknowledge receipt with an appropriate Advice Response message. When the MDS has received the appropriate Advice Response message, the MDS considers advice delivery to be complete and removes the advice message from any pending SAF processing queues.

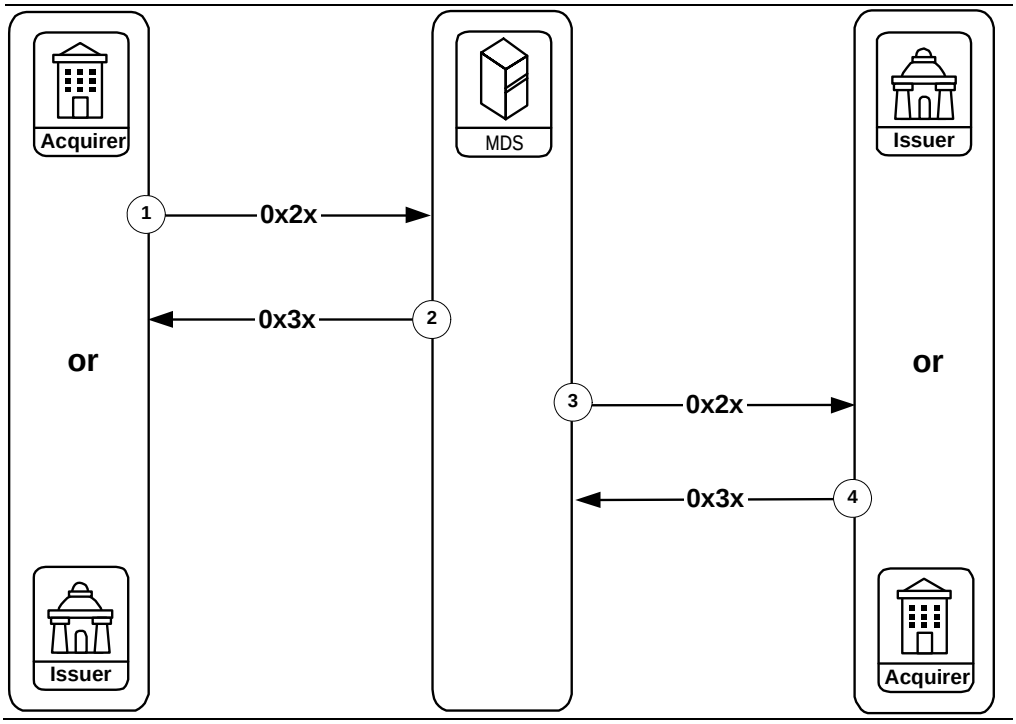
The MDS processes ISO 8583-1987 advice messages using the guaranteed advice delivery technique. These advice messages and their response messages are as follows:

- Financial Transaction Advice/0220
- Financial Transaction Advice Response/0230
- Acquirer Reversal Advice/0420
- Acquirer Reversal Advice Response/0430
- Issuer Reversal Advice/0422
- Issuer Reversal Advice Response/0432

Note **Other ISO 8583 transaction messages have a message type designation of "advice" but are not delivered by the MDS from one processor to another. The description of these other advice message types—0620 and 0820—and their flows are found in the detailed message flow descriptions later in this chapter.**

The following table illustrates the standard transaction flow requirements applicable to advice messages originated by customer processing systems connected to the MDS.

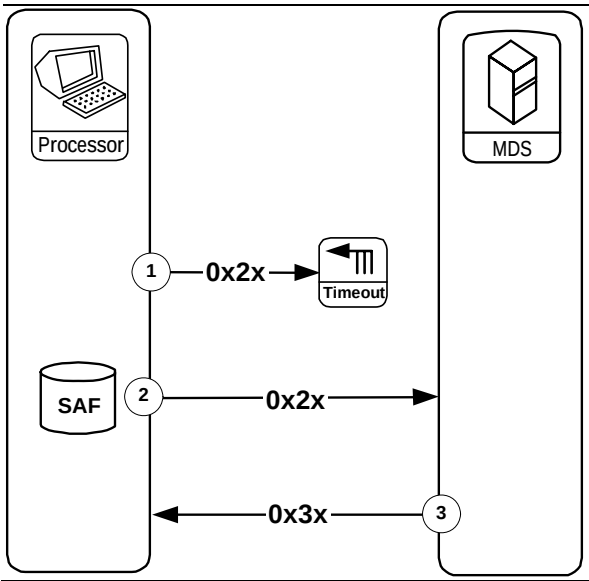
Guaranteed Advice Delivery



Stage	Description
1.	The acquirer or issuer processor forwards an Advice/0x2x message to the MDS.
2.	The MDS returns an Advice Response/0x3x message after it has received the original advice message.
3.	The MDS generates a corresponding Advice/0x2x message to the receiving processor.
4.	The receiving processor returns an Advice Response/0x3x message as positive acknowledgment of receipt after it has received the advice message.

The following table illustrates the exception condition transaction flow scenarios for advice messages with acknowledgments.

Exception, Advice Delivery from Processor Following Timeout



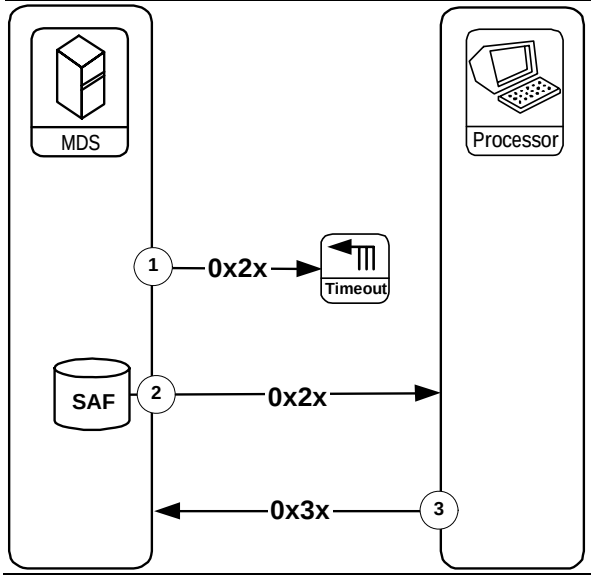
Stage	Description
1.	An issuer or acquirer generates an Advice/0x2x message. If it cannot be transmitted within the processor's configured timeout values, it should be stored by an appropriate store-and-forward (SAF) facility at the customer processing system. The Advice/0x2x message will be transmitted later when communication has been reestablished with the MDS.
2.	When communication is reestablished, the customer processing system forwards the Advice/0x2x message from the SAF facility to the MDS.
3.	The MDS returns an Advice Response/0x3x message after it has received the advice message.

The "Exception, Advice Delivery from Processor Following Timeout" transaction message flow does not illustrate the only scenario for advice messages: The MDS can initiate and send some types of advice messages to an individual processor. An individual processor can initiate and send advice messages to the MDS, and the MDS will forward these messages to another processor. However, the MDS will not forward some types of advice messages initiated by an individual processor to another processor.

The "Exception, Advice Delivery from Processor Following Timeout" transaction message flow description applies to processing during a given settlement period. If an advice message arrives at the MDS following the settlement day of the original transaction, reconciliation should be accomplished using one of the following methods:

- NICS™ (refer to the *NICS Users' Guide* for more information)
- Online adjustment processing (refer to chapter 3 and chapter 4 for more information)
- Manual adjustments (refer to the *NICS Users' Guide* for more information.)

Exception, Advice Delivery from the MDS Following Timeout



Stage	Description
1.	The MDS attempts to deliver the advice message to the intended destination. If it cannot be delivered, it is stored at the MDS SAF facility for later delivery.
2.	The MDS forwards the Advice/0x2x message from the SAF facility to the receiving destination when communication has been reestablished with the receiving processor.
3.	The receiving processor returns an Advice Response/0x3x message after it has received the advice message.

The "Exception, Advice Delivery from the MDS Following Timeout" transaction message flow does not illustrate the only scenario for advice messages: The MDS can initiate and send some types of advice messages to an individual processor. An individual processor can initiate and send some types of advice messages to the MDS and these messages will be forwarded to another processor. However, some types of advice messages initiated by an individual processor will not be forwarded to another processor by the MDS.

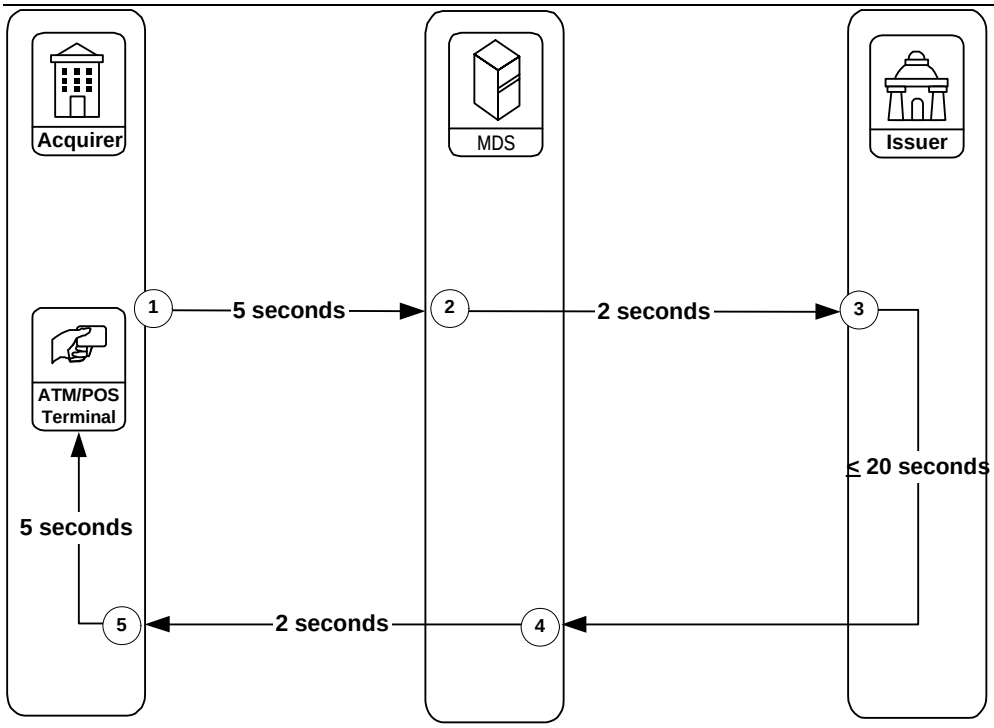
The "Exception, Advice Delivery from the MDS Following Timeout" transaction message description apply to processing during a given settlement period. If an advice message arrives at the MDS following the settlement day of the original transaction, reconciliation should be accomplished using one of the following methods:

- NICS™ (refer to the *NICS Users' Guide* for more information)
- Online adjustment processing (refer to chapter 3 and chapter 4 for more information)
- Manual adjustments (refer to the *NICS Users' Guide* for more information)

Maximum Response Times

The following table illustrates the maximum response time(s) available to each processor.

Maximum Response Times



Once a cardholder initiates a transaction, the MDS expects the following time intervals in processing a transaction:

Stage	Description
1.	The acquirer processor delivers a Financial Transaction Request/0200 ATM or point-of-service (POS) message to the MDS within five seconds.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer processor within two seconds.
3.	The issuer processor generates a Financial Transaction Request Response/0210 message to the MDS. Response is required within the following time intervals: • Maestro ATM (20 seconds) • Maestro POS (10 seconds) • Cirrus (20 seconds) • debit MasterCard (10 seconds)

Stage	Description
4.	The MDS forwards the Financial Transaction Request Response/0210 message to the acquirer processor within two seconds.
5.	The acquirer processor returns a Financial Transaction Request Response/0210 message to the ATM or POS device within five seconds.

The following additional maximum response times apply to other message types processed by the MDS:

- 0430 responses to 0420 adjustment advices (120 seconds)
- 0432 responses to 0422 adjustment advices (120 seconds)
- 0810 responses to 0800 network management requests (60 seconds)

The requirement for MasterCard acquirers is the terminal shall wait for (without timing out) a Financial Transaction Response/0210 message a minimum of 45 seconds after submitting a Financial Transaction Request/0200 message. **MasterCard recommended practice for minimum terminal timeout is 60 seconds.**

Authorization/01xx Messages

Note **This message series is only available for MasterCard credit card issuer-only processors.**

An issuer processing system (IPS) that is not planning on adding acquirer capabilities may choose to have all its transactions processed as credit card "cash advances" using Authorization Request/0100 and Authorization Response/0110 messages.

Authorization/01xx messages do not contain sufficient information to post to a cardholder's account at the IPS. Processors post through receipt of a Global Clearing Management System (GCMS) batch file at the end of the business day.

IPS processors using the Authorization/01xx messages have the option of electing Stand-In PIN verification using the MDS and Stand-In processing authorizations through MasterCard Central Site (available only if PIN verification has been selected). (Refer to the *MDS Programs and Services* manual for further discussion of this option.)

The network will handle any subsequent exception and reversal situations through the GCMS system for MasterCard credit card issuer-only processors.

Note **Authorization/01xx messages may support balance inquiry transactions. The MDS Authorization Request/0100 message interface process (the MDS interface to the Banknet network and its credit processors) does not support Reconciliation Advice messages. Reversal Advice/04xx messages are not sent outbound by the MDS to the 0100 interface; however, reversals can be received inbound by the MDS, through the 0100 interface, from a debit MasterCard acquirer.**

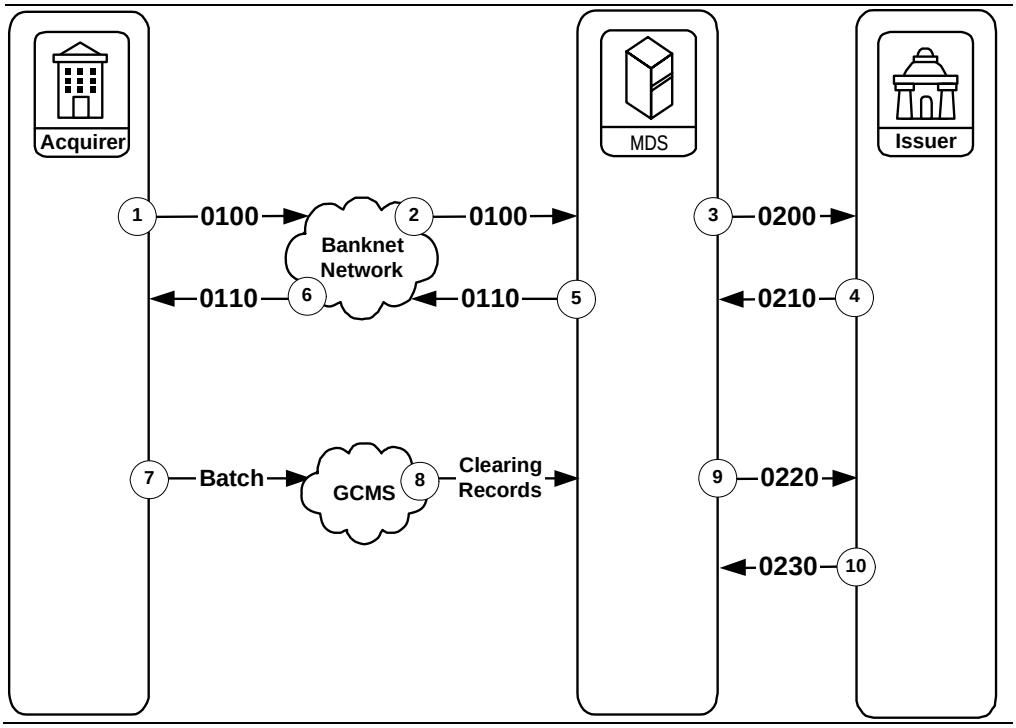
Refer to the *Customer Interface Specification* manual for information about Authorization/01xx messages used by the Authorization System.

Debit MasterCard Pre-authorization and Clearing Processing

The following table illustrates the standard message flow for a debit MasterCard Pre-authorization and clearing transaction when the debit MasterCard issuer is connected to the MDS.

Note **A transaction using debit MasterCard is designed to work like a credit card transaction where the completion occurs following a subsequent-day batch clearing process that is initiated from the acquirer.**

Debit MasterCard Pre-authorization and Clearing Processing



Stage	Description
1.	The acquirer sends the Authorization Request/0100 message to the Banknet network.
2.	The Banknet network forwards the Authorization Request/0100 message to the MDS.

Stage	Description
3.	The MDS converts the Authorization Request/0100 message to a Financial Transaction Request/0200 message and forwards it to the issuer. DE 61 (Point-of-Service Data), subfield 7 (POS Transaction Status Indicator), will contain the value 4 (Pre-authorization Request) that indicating that this is a pre-authorization request.
4.	The issuer responds with a Financial Transaction Request Response/0210 message to the MDS.
5.	The MDS converts the Financial Transaction Request Response/0210 message to an Authorization Request Response/0110 message and sends it to the Banknet network.
6.	The Banknet network forwards the Authorization Request Response/0110 message to the acquirer.
7.	The acquirer processing system batches the clearing records and sends them to the Global Clearing Management System (GCMS) at MasterCard. This typically occurs within 2-5 days of the pre-authorization.
8.	GCMS groups all clearing records bound for the MDS and transmits them to the MDS.
9.	The MDS converts each detail record into a Financial Transaction Advice/0220 clearing message and forwards it to the issuer.
10.	The issuer responds with a Financial Transaction Advice Response/0230 message to the MDS.

Note

The Financial Transaction Request/0200 message must contain the value 4 in subfield 7 of DE 61 for Debit MasterCard pre-authorization transactions. The Financial Transaction Advice/0220 message will contain the value 0 in subfield 7 of DE 61 for a Debit MasterCard pre-authorization completion.

Financial Transaction/02xx Messages

Financial Transaction/02xx messages are used for the following:

- Financial transaction requests
- Financial transaction request responses
- Financial transaction advices
- Financial transaction response acknowledgments

The term "financial transaction" applies when there is sufficient data contained within the individual transaction message to provide actual posting of accounts at the issuer processing system (IPS). The MDS processes all Financial Transaction/02xx messages assuming that when the transaction is completed successfully, no subsequent information (such as "paper" or "transaction tickets") is required to perform actual cardholder account posting and cardholder billing.

The following information lists the definitions of all ISO 8583–1987 Financial Transaction/02xx messages supported for the MDS.

Financial Transaction Request/0200 Message	
Type:	Interactive
Routing:	From an acquirer to the MDS From the MDS to an issuer
Purpose:	Requests approval of a transaction that, if approved, will permit the application of the transaction financial data to the cardholder's account for issuing a bill or statement
Response:	A Financial Transaction Request Response/0210 message is required.

Financial Transaction Request Response/0210 Message	
Type:	Interactive
Routing:	From an issuer to the MDS From the MDS to an acquirer
Purpose:	Must be sent in response to a Financial Transaction Request/0200 message. It carries the response information required to service (such as approve or deny) the request.
Response:	The MDS will provide a Financial Transaction Negative Acknowledgement/0290 message to an issuer when the issuer processing system responds with a late Financial Transaction Response/0210 message to a Financial Transaction Request/0200 message.

Financial Transaction Advice/0220 Message	
Type:	Non-interactive
Routing:	From an acquirer to the MDS From the MDS to an issuer
Purpose:	The MDS forwards a Financial Transaction Advice/0220 message to an affected issuer when: • An authorization of a Maestro or Cirrus transaction request occurrs during Stand-In processing • A debit MasterCard force post transaction message is received from an acquirer • A Maestro pre-authorization completion message is received from an acquirer
Response:	A Financial Transaction Advice Response/0230 message **is required**.

Financial Transaction Advice Response/0230 Message	
Type:	Non-interactive
Routing:	From the MDS to an acquirer From an issuer to the MDS
Purpose:	Must be sent in response to a Financial Transaction Advice/0220 message. Indicates positive receipt of a Financial Transaction Advice/0220 message.
Response:	None

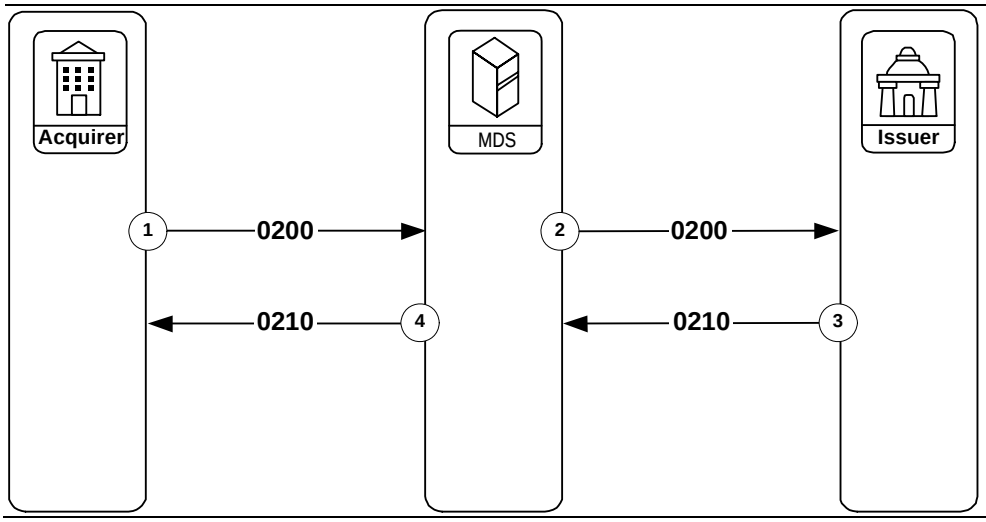
Financial Transaction Negative Acknowledgement/0290 Message	
Type:	Non-interactive
Routing:	From the MDS to an acquirer From the MDS to an issuer
Purpose:	The MDS uses the Financial Transaction Negative Acknowledgement/0290 message primarily to inform an issuer that the MDS did not receive a Financial Transaction Response/0210 from the issuer in the required time interval. The MDS also uses the Financial Transaction Negative Acknowledgement/0290 message to inform an acquirer that the MDS was unable to deliver a Financial Transaction Response/0210 message to the acquirer.
Response:	None

The transaction flows provided throughout the remainder of this chapter define all of the ISO 8583–1987 transaction flow procedures implemented on the MDS. These flows sometimes depict a "timeout" or late response situation.

Financial Transaction Request/0200 and Financial Transaction Request Response/0210

The following table illustrates the standard message flow for interactive financial transaction processing.

Financial Transaction Request/0200 and Financial Transaction Request Response/0210

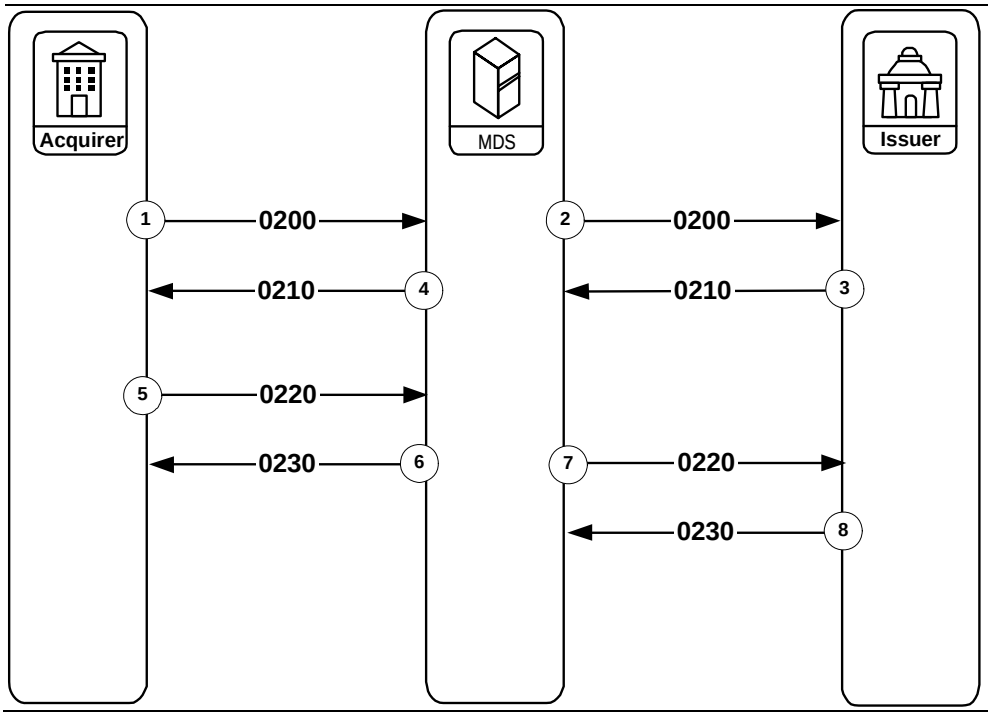


Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	The issuer generates a Financial Transaction Request Response/0210 message and sends it to the MDS.
4.	The MDS forwards the Financial Transaction Request Response/0210 message to the acquirer.

Financial Transaction/02xx—Maestro Pre-authorization and Completion

The following table illustrates a POS pre-authorization and completion transaction.

Financial Transaction/02xx—Maestro Pre-authorization and Completion



Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS. DE 61 (Point-of-Service Data), subfield 7, (POS Transaction Status Indicator), will contain the value 4 (Pre-authorization Request) indicating that this is a pre-authorization request. DE 4 (Amount, Transaction) will contain either the acquirer's standard predetermined requested amount or the cardholder's requested amount.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	If approved, the issuer puts a conditional hold on the cardholder's account and returns a Financial Transaction Request Response/0210 message to the MDS.
4.	The MDS returns the Financial Transaction Request Response/0210 message to the acquirer.

Stage	Description
5.	Within 20 minutes of the original Financial Transaction Request/0200 message, the acquirer must send a Financial Transaction Advice/0220 completion message to the MDS. This completion message must be provided with the actual completed amount of the transaction to be posted to the cardholder's account. This completed amount **must** be provided in DE 95 (Replacement Amounts). DE 61 (Point-of-Service Data), subfield 7 (POS Transaction Status Indicator) and DE 4 (Amount, Transaction) will contain the same values as in the original Financial Transaction Request/0200 message.
6.	The MDS responds with a Financial Transaction Advice Response/0230 message.
7.	The MDS forwards the Financial Transaction Advice/0220 message to the issuer.
8.	The issuer responds with a Financial Transaction Advice Response/0230 message.

Note **Please note that if the MDS does not receive a Financial Transaction Advice/0220 message from the acquirer, the MDS assumes the transaction was not completed and no further message processing occurs.**

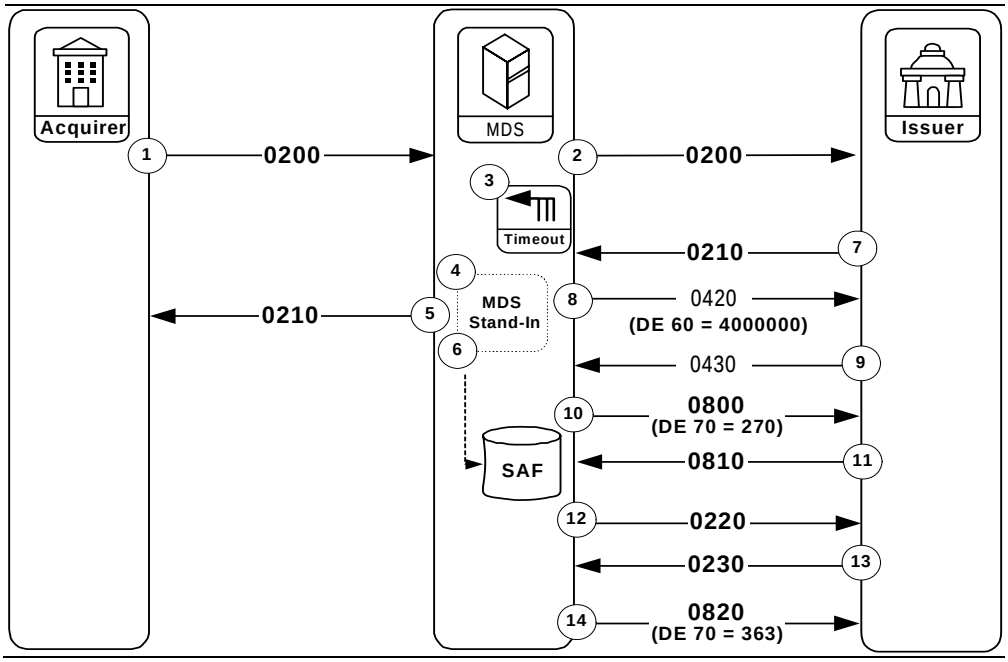
Note **The MDS treats the Maestro pre-authorization and completion cycle as a single transaction. This is unlike the debit MasterCard pre-authorization and completion cycle, which is treated as two separate transactions. This difference is because the Maestro processing cycle is completed within 20 minutes on the same settlement day, while the debit MasterCard completion message is processed within 2–5 calendar days of the pre-authorization message.**

Note **The Financial Transaction Request/0200 message must contain the value 4 in subfield 7 of DE 61 for Maestro pre-authorization transactions. The Financial Transaction Advice/0220 message will contain the value 4 in subfield 7 of DE 61 for a Maestro pre-authorization completion.**

Financial Transaction/02xx—Exception, MDS Stand-In Processing, Late Response from Issuer

The following table illustrates exception condition processing for a late issuer Financial Transaction Request Response/0210 message. This example assumes that the issuer subscribes to the MDS Stand-In processing service.

Financial Transaction/02xx—Exception, MDS Stand-In Processing, Late Response from Issuer



Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	The MDS detects a timeout condition on the Financial Transaction Request Response/0210 message that is expected from the issuer.
4.	If the issuer processor is configured for Stand-In processing at the MDS, the MDS creates an internal financial request message and sends it to Stand-In processing for authorization. The Stand-In processing service validates the request and formulates an internal response message.
5.	The MDS uses the internal response to create a Financial Transaction Request Response/0210 message and sends it to the acquirer.

Stage	Description
6.	A record of the Financial Transaction Request/0220 message is placed in the SAF file on the MDS for later delivery to the issuer.
7.	The MDS receives an unsolicited (late) Financial Transaction Request Response/0210 message from the issuer.
8.	The MDS responds with an Acquirer Reversal Advice/0420 message containing DE 60 (Advice Reason Code) with the value 4000000 (Late response from issuer). This indicates to the issuer that the Financial Transaction Request Response/0210 message is late and rejected. The issuer must assume that the MDS or the acquirer will take appropriate action, and should immediately reverse any impact to the cardholder's account file. OR, If a debit MasterCard issuer does not support an Acquirer Reversal Advice/0420 message, the issuer will receive a Financial Transaction Negative Acknowlegement/0290 message.

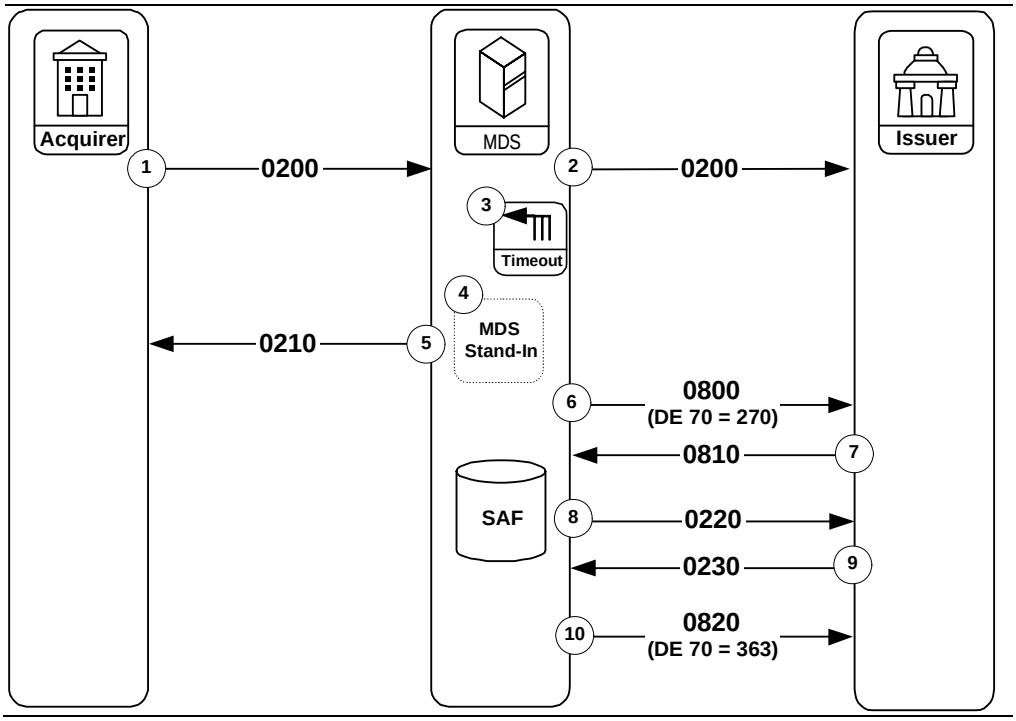
Note **If the late Financial Transaction Request Response/0210 message has a response code indicating a request denial, then the MDS will not take action (the Acquirer Reversal Advice/0420 message is not sent).**

9.	The issuer responds with an Acquirer Reversal Advice Response/0430 message to the MDS.
10.	The MDS initiates, at regular intervals determined programmatically, a Network Management Request/0800 "echo test" message to verify or establish communication with the issuer.
11.	The issuer responds with a Network Management Request Response/0810 message.
12.	When communication is established, the MDS sends a Financial Transaction Advice/0220 authorization completion message with DE 38 (Authorization Identification Response) containing a six digit switch serial number to the issuer from the SAF facility.
13.	The issuer responds with a Financial Transaction Advice Response/0230 message.
14.	Any remaining messages stored in the SAF file for the issuer will also be sent by the MDS. When completed, the MDS will send a Network Management Advice/0820 message to indicate the SAF facility has reached an end-of-file (EOF) condition.

Financial Transaction/02xx—Exception, MDS Stand-In Processing, No Response from Issuer

The following table illustrates the MDS Stand-In processing procedures when the issuer cannot complete the transaction. This example assumes that the issuer has subscribed to the MDS Stand-In processing service.

Financial Transaction/02xx—Exception, MDS Stand-In Processing, No Response from Issuer



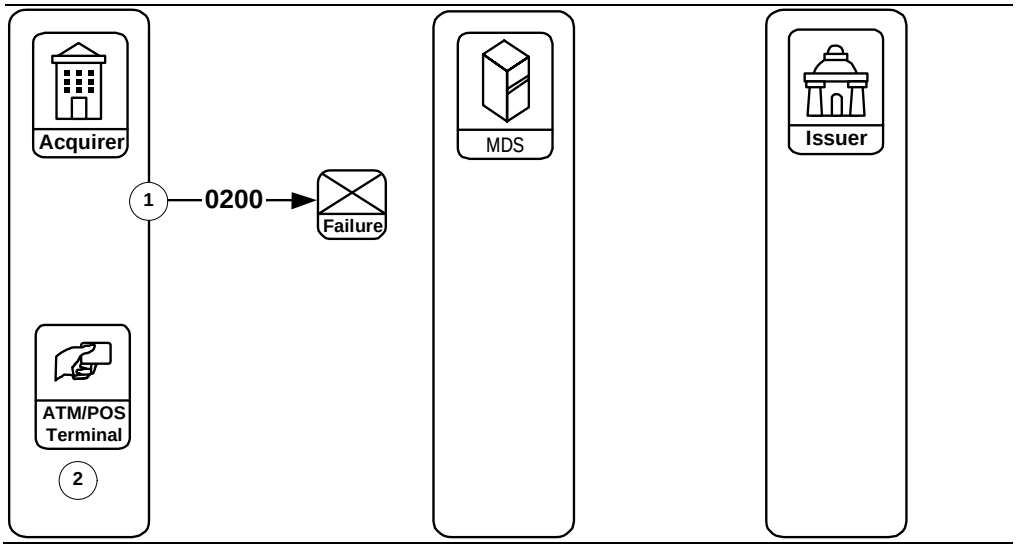
Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	The MDS detects a timeout condition on the Financial Transaction Request Response/0210 message that is expected from the issuer.
4.	If the issuer processor is configured for Stand-In processing at the MDS, the MDS creates an internal financial request message and sends it to Stand-In processing for authorization. The Stand-In processing service validates the request and formulates an internal response message.

Stage	Description
5.	The MDS uses the internal response to create a Financial Transaction Request Response/0210 message, and sends it to the acquirer. The MDS can receive another Financial Transaction Request/0200 message for the issuer. If the issuer processing system is still not online, the MDS repeats stages **4** and **5** above, as additional Financial Transaction Request/0200 messages arrive at the MDS destined for this issuer.
6.	The MDS initiates, at regular intervals determined programmatically, a Network Management Request/0800 "echo test" message to verify or establish communication with the issuer.
7.	The issuer responds with a Network Management Request Response/0810 message.
8.	The MDS sends a Financial Transaction Advice/0220 authorization completion message with DE 38 (Authorization Identification Response) that contains a six-digit switch serial number to the issuer from the SAF facility.
9.	The issuer responds with a Financial Transaction Advice Response/0230 message.
10.	Any remaining messages stored in the SAF file for the issuer also will be sent by the MDS to the issuer. When completed, the MDS will send a Network Management Advice/0820 message to indicate the SAF facility has reached an end-of-file (EOF) condition.

Financial Transaction/02xx—Exception, System Failure during Acquirer Financial Transaction Request/0200

The following table illustrates exception condition processing for a system or communication failure during the transmission of an acquirer Financial Transaction Request/0200 message.

Financial Transaction/02xx—Exception, System Failure during Acquirer Financial Transaction Request/0200

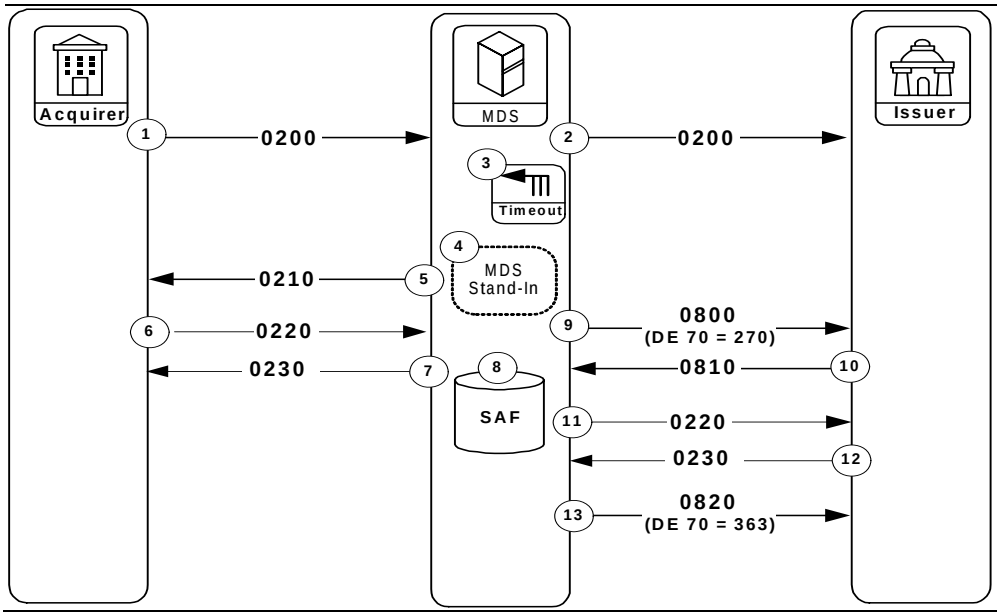


Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message, but it cannot be delivered to the MDS because of system failure.
2.	The acquirer processing system is unable to transmit the Financial Transaction Request/0200 message to the MDS but must complete the transaction at the point of service. The MDS requires that the acquirer deny the transaction request at the point-of-service. Processing terminates.

Financial Transaction/02xx—Exception, Stand-In Maestro Pre-authorization

The following table illustrates a Maestro Pre-authorization transaction if a completion transaction is received by the acquirer.

Financial Transaction/02xx—Exception, Stand-In Maestro Pre-authorization



Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS. DE 61 (Point-of-Service Data), subfield 7 (POS Transaction Status Indicator), will contain the value 4 (Pre-authorization request) that indicates that this is a pre-authorization request. DE 4 (Amount, Transaction) will contain either the acquirer's standard predetermined requested amount or cardholder's requested amount.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	The MDS detects a timeout condition on the Financial Transaction Request Response/0210 message that is expected from the issuer.

Stage	Description
4.	If the issuer processor is configured for Stand-In processing at the MDS, the MDS creates an internal financial request message and sends it to Stand-In processing for authorization. The Stand-In processing service validates the request and formulates an internal response message.
5.	The MDS uses the internal response to create a Financial Transaction Request Response/0210 message, and sends it to the acquirer. The MDS can receive another Financial Transaction Request/0200 message for the issuer. If the issuer processing system is still not online, the MDS repeats stages **4** and **5** above, as additional Financial Transaction Request/0200 messages arrive at the MDS destined for this issuer.
6.	Within 20 minutes of the original Financial Transaction Request/0200 message, the acquirer must send a Financial Transaction Advice/0220 completion message to the MDS. This completion message must be provided with the actual completed amount of the transaction to be posted to the cardholder's account. This completed amount **must** be provided in DE 95 (Replacement Amounts). DE 61 (Point-of-Service Data), subfield 7 (POS Transaction Status Indicator) and DE 4 (Amount, Transaction) will contain the same values as in the original Financial Transaction Request/0200 message.
7.	The MDS responds with a Financial Transaction Advice Response/0230 message.
8.	If the acquirer's Financial Transaction Advice/0220 completion message has passed all MDS edits, it is placed in the SAF file for later delivery to this issuer.

Note **If the acquirer fails to send the Financial Transaction Advice/0220 completion message, it is not placed in the SAF file, and the issuer will not receive an online completion for the transaction.**

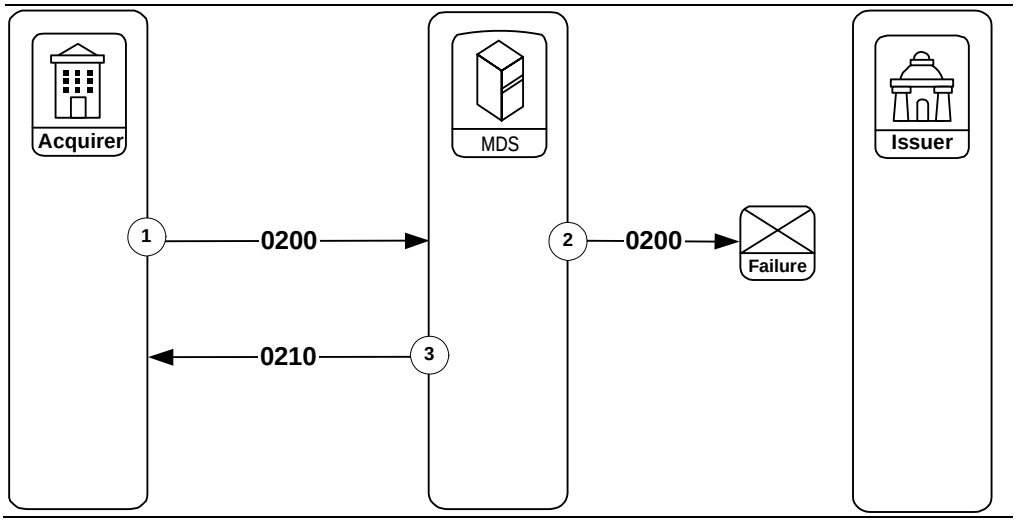
Stage	Description
9.	The MDS initiates, at regular intervals determined programmatically, a Network Management Request/0800 "echo test" message to verify or establish communication with the issuer.
10.	The issuer responds with a Network Management Request Response/0810 message.
11.	The MDS sends a Financial Transaction Advice/0220 authorization completion message with DE 38 (Authorization Identification Response) that contains an MDS-generated six-digit serial number to the issuer from the SAF facility.

Stage	Description
12.	The issuer responds with a Financial Transaction Advice Response/0230 message.
13.	Any remaining messages stored in the SAF file for the issuer also will be sent by the MDS to the issuer. When completed, the MDS will send a Network Management Advice/0820 message to indicate the SAF facility has reached an end-of-file (EOF) condition.

Financial Transaction/02xx—Exception, System Failure during Issuer Financial Transaction Request/0200

The following table illustrates exception procedures for a system or communication failure condition during the transmission of a Financial Transaction Request/0200 message.

Financial Transaction/02xx—Exception, System Failure during Issuer Financial Transaction Request/0200

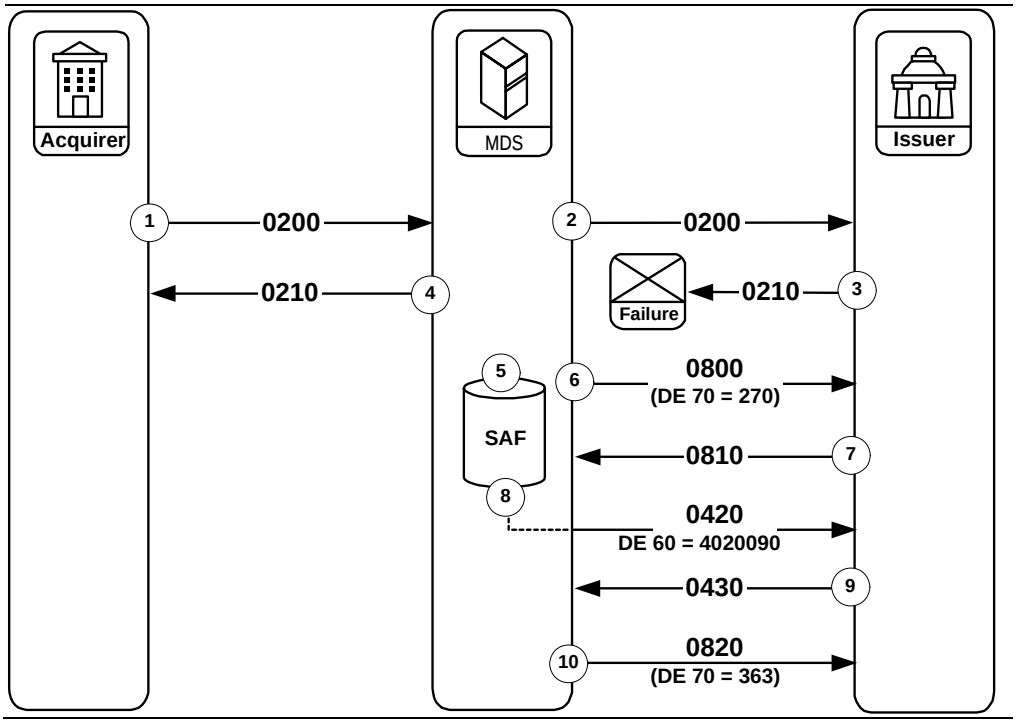


Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS attempts to forward the Financial Transaction Request/0200 message to the issuer but is unable to complete the message transmission due to a communication link failure or other problem at the issuer processing system.
3.	The MDS will generate a Financial Transaction Request Response/0210 message to the acquirer, indicating a request denial.

Financial Transaction/02xx—Exception, System Failure during Issuer Financial Transaction Request Response/0210

The following table illustrates exception condition processing for a system or communication failure during the transmission of an issuer Financial Transaction Request Response/0210 message.

Financial Transaction/02xx—Exception, System Failure during Issuer Financial Transaction Request Response/0210



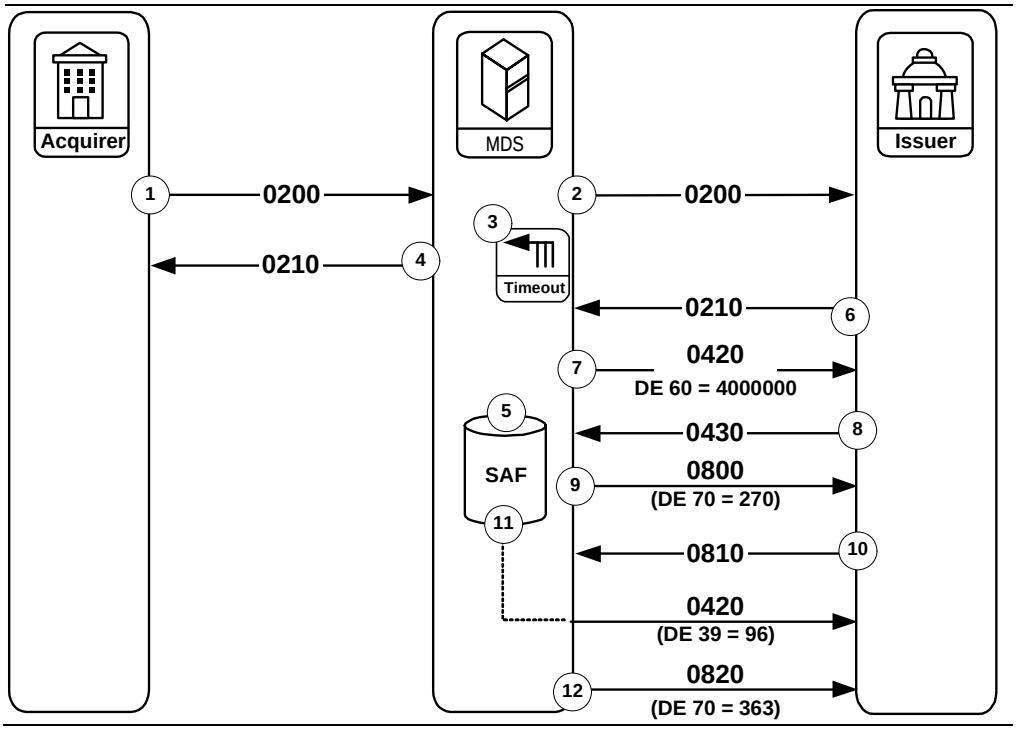
Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	The issuer cannot return the Financial Transaction Request Response/0210 message because of a communication failure between the issuer processing system and the MDS. The issuer must assume that the MDS or the acquirer will take appropriate action and should immediately reverse the impact to the cardholder's account file if the request was approved.

Stage	Description
4.	The MDS detects a timeout condition because of the issuer processing system failure on the Financial Transaction Request Response/0210 message. The MDS generates a Financial Transaction Request Response/0210 message to the acquirer, indicating a request denial.
5.	The MDS also creates a Transaction Negative Acknowledgement/0290 message containing DE 39 (Response Code) with the value 96 (system error or system timer expired on expected CPS message) indicating that no Financial Transaction Request Response/0210 message was received. This message is placed in the SAF file for later delivery to the issuer.
6.	The MDS initiates, at regular intervals determined programmatically, a Network Management Request/0800 "echo test" message to verify or establish communication with the issuer.
7.	The issuer responds with a Network Management Request Response/0810 message.
8.	The MDS sends an Acquirer Reversal Advice/0420 message that contains DE 60 (Advice Reason Code) with the value 4020090 (Network Advice: IPS timeout error not acceptable from acquirer) OR, If a debit MasterCard issuer does not support an Acquirer Reversal Advice/0420 message, the issuer will receive a Financial Transaction Negative Acknowlegement/0290 message.
9.	The issuer responds with an Acquirer Reversal Advice Response/0430 message to the MDS.
10.	The MDS sends a Network Management Advice/0820 message to indicate the SAF facility has reached an end-of-file (EOF) condition.

Financial Transaction/02xx—Exception, Late Issuer Financial Transaction Request Response/0210

The following table illustrates exception condition processing for a late Issuer Financial Transaction Request Response/0210 message.

Financial Transaction/02xx—Exception, Late Issuer Financial Transaction Request Response/0210



Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	The MDS detects a timeout condition on the Financial Transaction Request Response/0210 message that is expected from the issuer.
4.	The MDS then generates a Financial Transaction Request Response/0210 message to the acquirer, indicating a request denial.

Stage	Description
5.	The MDS also creates a Acquirer Reversal Advice/0420 message containing DE 60 (Advice Reason Code) with the value 4020090 (Network Advice: IPS time-out error not acceptable from acquirer) indicating no Financial Transaction Request Response/0210 message was received. This message is placed in the SAF file for later delivery to the issuer. OR, If a debit MasterCard issuer does not support an Acquirer Reversal Advice/0420 message, the issuer will receive a Financial Transaction Negative Acknowlegement/0290 message.
6.	The MDS receives an unsolicited (late) Financial Transaction Response/0210 message from the issuer.
7.	If the late Financial Transaction Request Response/0210 message indicates an approval from the issuer, the MDS responds with an Acquirer Reversal Advice/0420 message containing DE 60 with the value 4000000 (Late response from issuer). This indicates to the issuer that this Financial Transaction Request Response/0210 message is late and rejected. The issuer must assume the MDS or the acquirer will take appropriate action at this point and should immediately reverse any impact to the cardholder's account file. OR, If a debit MasterCard issuer does not support an Acquirer Reversal Advice/0420 message, the issuer will receive a Financial Transaction Negative Acknowlegement/0290 message.

Note **If the late Financial Transaction Request Response/0210 message has a response code indicating a request denial, then the MDS will not take action (that is the Acquirer Reversal Advice/0420 message is not sent).**

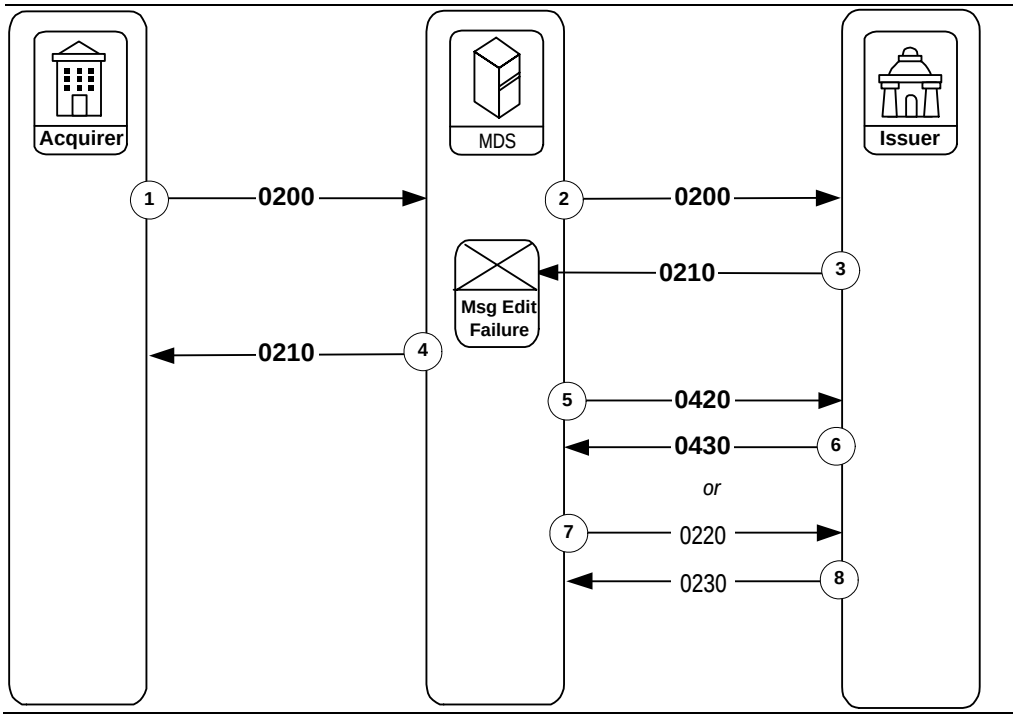
Stage	Description
8.	The issuer responds with an Acquirer Reversal Advice Response/0430 message to the MDS.
9.	The MDS initiates, at regular intervals determined programmatically, a Network Management Request/0800 "echo test" message to verify or establish communication with the issuer.
10.	The issuer responds with a Network Management Request Response/0810 message.

Stage	Description
11.	The MDS sends the Acquirer Reversal Advice/0420 message containing DE 60 (Advice Reason Code) with the value 4020090 (Network Advice: IPS timeout error not acceptable from acquirer) from the SAF file to the issuer. Any remaining messages stored in the SAF file for the issuer also will be sent by the MDS to the issuer. OR, If a debit MasterCard issuer does not support an Acquirer Reversal Advice/0420 message, the issuer will receive a Financial Transaction Negative Acknowlegement/0290 message.
12.	The MDS sends a Network Management Advice/0820 message to indicate the SAF facility has reached an end-of-file (EOF) condition.

Financial Transaction/02xx—Exception, Financial Transaction Request Response/0210 Failure of MDS System Edits

The following table illustrates exception procedures when the MDS processes the Financial Transaction Request Response/0210 message from the issuer, and the message does not pass the MDS system edits.

Financial Transaction/02xx—Exception, Financial Transaction Request Response/0210 Failure of MDS System Edits



Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.

Stage	Description	
3.	The issuer responds with a Financial Transaction Request Response/0210 message and sends it to the MDS. The message does not pass one of several required MDS System edits.	
4.	The MDS then generates a Financial Transaction Request Response/0210 message to the acquirer, indicating a request denial. If the issuer's Financial Transaction Request Response/0210 message fails the MDS System edits:	
	IF...	**THEN...**
5.	The transaction has financial value and DE 39 (Response Code) of the issuer 0210 message contains the value 00 (Approved or completed successfully)	The MDS generates an Acquirer Reversal Advice/0420 message containing DE 60 (Advice Reason Code) with the value 454000 (Network Advice: invalid data) and sends it to the issuer.
6.	The issuer responds by returning a Financial Transaction Advice Response/0430 message to the MDS. OR,	
	If a debit MasterCard issuer does not support an Acquirer Reversal Advice/0420 message, the issuer will receive a Financial Transaction Negative Acknowlegement/0290 message.	The MDS will generate a Financial Transaction Negative Acknowlegement /0290 message and send it to the issuer. DE 63, Network Data, subfield 1, Financial Network code contains the value MD (MasterCard® debit card). The Financial Transaction Negative Acknowlegement/0290 message requires no response from the issuer.
7.	The transaction is a Maestro Pre-authorization, and DE 39 (Response Code) contains the value 00 (Approved or completed successfully)	The MDS sends a Financial Transaction Advice/0220 message to the issuer where DE 60 (Advice Reason Code) contains the value 4540000 (Network Advice: invalid data).

Oct 2005

Oct 2005

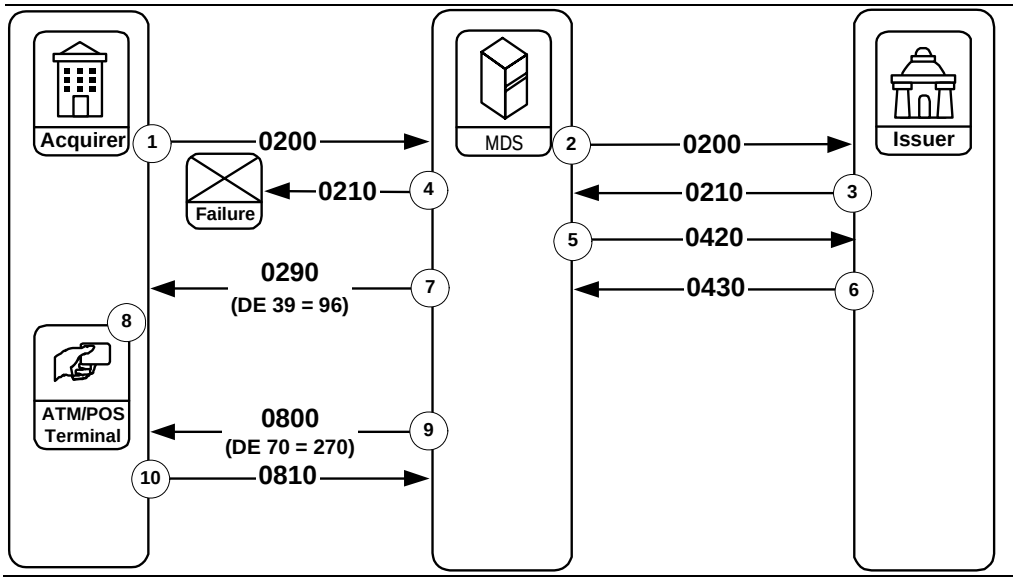
Stage	Description	
	IF…	**THEN…**
8.	The Financial Transaction Request/0220 message sent by the issuer does not contain DE 39 (Response Code) with the value 00 (Approved or completed successfully)	The MDS does not send a Financial Transaction Advice/0220 message to the issuer.

Note **If the MDS cannot parse the Financial Transaction Request Response/0210 message, the MDS generates an Administrative Advice/0620 and sends it to the issuer. Please refer to Administrative Advice/0620 (MDS Initiated).**

Financial Transaction/02xx—Exception, System Failure during Acquirer Financial Transaction Request Response/0210

The following table illustrates exception procedures for a system or communication failure condition encountered during the transmission of a Financial Transaction Request Response/0210 message.

Financial Transaction/02xx—Exception, System Failure during Acquirer Financial Transaction Request Response/0210



Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	The issuer responds with a Financial Transaction Request Response/0210 message and sends it to the MDS.
4.	The MDS attempts to forward the Financial Transaction Request Response/0210 message to the acquirer, but cannot successfully complete the transmission due to a communication failure between the MDS and the acquirer processing system.
5.	The MDS determines that the issuer's Financial Transaction Request Response/0210 message is undeliverable and, only if the response indicates a request approval, immediately generates an Acquirer Reversal Advice/0420 message to the issuer.

Stage	Description
6.	If the issuer receives an Acquirer Reversal Advice/0420 message from the MDS, the issuer responds with a Reversal Advice Response/0430 message to the MDS.
7.	The MDS sends a Financial Transaction Negative Acknowledgement/0290 message containing DE 39 (Response Code) with the value 96 (System error or system timer expired on expected CPS Message) and sends it to the acquirer. This informs the acquirer that the MDS generated a reversal to the issuer for the failed transaction.
8.	If the acquirer processing system is operational, it will detect a timeout condition on the Financial Transaction Request Response/0210 message that it is expecting from the MDS. When the timeout occurs, the MDS requires that the acquirer deny the transaction request at the point-of-service. Processing terminates.
9.	The MDS initiates, at regular intervals determined programmatically, a Network Management Request/0800 "echo test" message to verify or establish communication with the acquirer.
10.	The acquirer responds with a Network Management Request Response/0810 message.

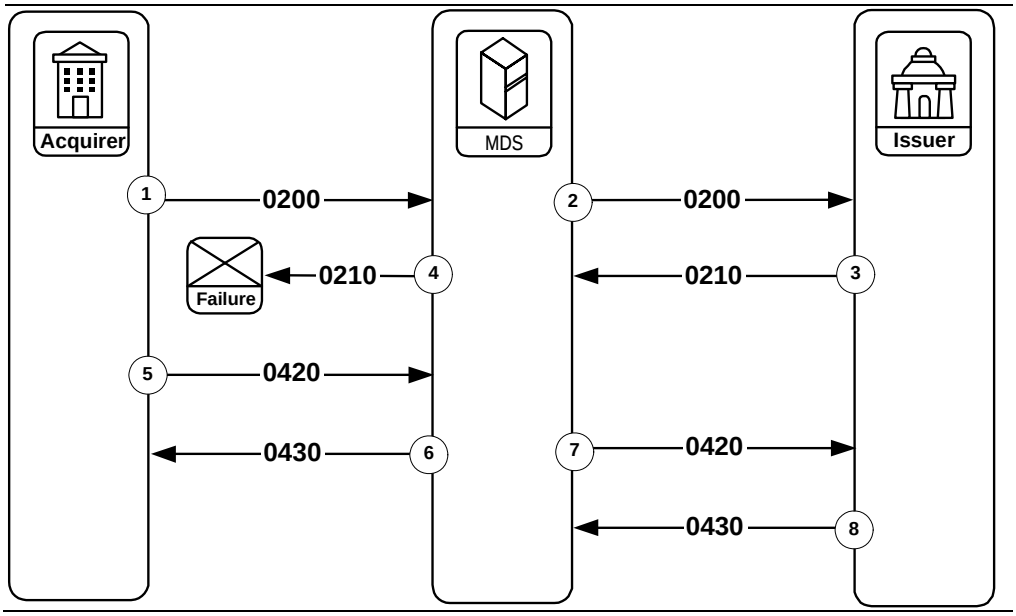
Financial Transaction/02xx—Exception, Timeout of Financial Transaction Request Response/0210 to Acquirer

The following table illustrates exception procedures for a message delivery failure condition encountered on the acquiring side when a Financial Transaction Request Response/0210 message sent to the acquirer by the MDS is not received by the acquirer application.

In this situation, the acquirer's timeout limit (typically in the range of 45-60 seconds) has been exceeded for receiving the Financial Transaction Request Response/0210 message. The acquirer has the option of responding to the timeout by sending a Timeout-Induced Reversal/0420 message to the MDS (for the description and message format, refer to chapter 3).

This Timeout-Induced Reversal/0420 message will not include the DE 15 (Date, Settlement) or DE 63 (Network Data). Further, DE 39 (Response Code), DE 60 (Advice Reason Code), and DE 95 (Replacement Amounts) will have specific requirements as chapter 3 shows in the message format table and usage notes within the data element descriptions of chapter 4.

Financial Transaction/02xx—Exception, Timeout of Financial Transaction Request Response/0210 to Acquirer



Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	The issuer generates a Financial Transaction Request Response/0210 message and sends it to the MDS.
4.	The MDS forwards the Financial Transaction Request Response/0210 message to the acquirer, but the message fails at the acquirer application interface. It fails such that the MDS is not aware of a delivery problem.

Stage	Description
5.	The acquirer times out on receipt of the Financial Transaction Request Response/0210 message [a]. The acquirer sends a Timeout-Induced Reversal/0420 message, also known as an unsolicited message reversal, to the MDS. This reversal is distinct from a normal acquirer-generated reversal in the following manner: • DE 15 (Date, Settlement) is not present in the message from the acquirer • DE 63 (Network Data) is not present in the message from the acquirer • DE 39 (Response Code) contains the value 00 • DE 60 (Advice Reason Code) contains the value 4500018 • DE 95 (Replacement Amounts) contains all zeroes
6.	The MDS responds with an Acquirer Reversal Advice Response/0430 message. **NOTE**: Reversal advice processing is complete when the acquirer receives the Acquirer Reversal Advice Response/0430 message, regardless of DE 39 (Response Code) value contained in the response message. IF DE 39 in the response message contains a value OTHER than 00 (Approved or completed successfully), or DE 39 contains the value 30 (Format Error), the MDS will deny the acquirer's reversal message. In this case, the acquirer should not re-transmit the reversal advice to the MDS. The acquirer must clear their timer for the Acquirer Reversal Advice/0420 message, and consider processing to be complete.
7.	If the Financial Transaction Request Response/0210 message received at step 3 indicates an approval, the MDS generates a standard Acquirer Reversal Advice/0420 message and sends it to the issuer.
8.	The issuer responds with an Acquirer Reversal Advice Response/0430 message.

[a] The acquirer should permit no more than five (5) failures of this type before marking the MDS down and attempting to recover the connection. The acquirer periodically may send Network Management Request/0800 “echo test” messages to the MDS to test its connection and/or it may attempt delivery of the corresponding Timeout-Induced Reversal/0420 message at a later date.

Note

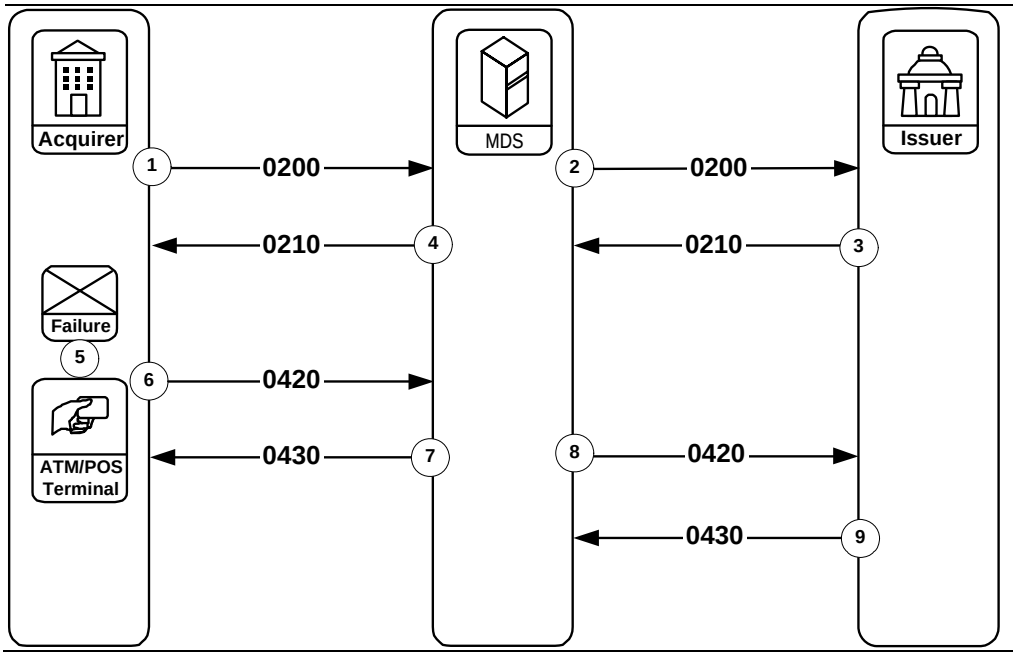
The acquirer should set a 120-second timer on the Timeout-Induced Reversal/0420 message. If an Acquirer Reversal Advice Response/0430 message is not received within 120 seconds, then the acquirer should place the Timeout-Induced Reversal/0420 message into its store-and-forward facility for later delivery to the MDS.

When sending SAF messages, the acquirer should wait for the MDS response to each message before sending the next SAF record. This method of transmission is known as single-threaded mode.

Financial Transaction/02xx—Exception, Acquirer Unable to Complete Transaction

The following table illustrates exception procedures for a situation where the acquirer is not able to complete the cardholder transaction. This situation may develop due to an ATM terminal failure resulting in partial or non-dispense of cash, communication failure within the acquirer's own network, or because a cardholder canceled the transaction prior to receiving a response. In all of these situations, the acquirer's processing system will reverse the transaction to the issuer.

Financial Transaction/02xx—Exception, Acquirer Unable to Complete Transaction



Stage	Description
1.	The acquirer initiates a Financial Transaction Request/0200 message to the MDS.
2.	The MDS forwards the Financial Transaction Request/0200 message to the issuer.
3.	The issuer generates a Financial Transaction Request Response/0210 message and sends it to the MDS.
4.	The MDS forwards the Financial Transaction Request Response/0210 message to the acquirer.

Stage	Description
5.	The acquirer determines the transaction cannot be successfully completed.
6.	The acquirer generates a Financial Transaction Reversal Advice/0420 message and sends it to the MDS. The reversal amount may be for the entire amount of the original transaction or for some partial amount (in the event of an ATM partial dispense).
7.	The MDS responds with an Acquirer Reversal Advice Response/0430 message.
8.	The MDS forwards the Acquirer Reversal Advice/0420 message to the issuer.
9.	The issuer responds with an Acquirer Reversal Advice Response/0430 message. The issuer uses the information in the Acquirer Reversal Advice/0420 message to correctly update the cardholder's account file.

Note

Error condition processing for Reversal Advice/04xx messages is not illustrated. If a reversal advice message does not transmit successfully, it should be re-transmitted. Issuer and acquiring processors must assume the responsibility for identifying any message as a possible "duplicate" transaction.

Acquirer Reversal Advice/0420 and Acquirer Reversal Advice Response/0430 messages are used in conjunction with Financial Transaction/02xx messages when transaction flow exception (error) situations are encountered during financial transaction processing. For specific exception conditions, the MDS may directly generate Acquirer Reversal Advice/0420 messages. Refer to the Financial Transaction/02xx message flow schematics to determine proper use of Acquirer Reversal Advice/0420 and Acquirer Reversal Advice Response/0430 messages in these exception processing situations.

File Update/03xx Messages

Issuers may use file update messages to update individual account files such as "hot card" files or system parameter files defined within the MasterCard Account Management System (AMS) or MDS Stand-In processing. MasterCard uses these account files to control the operation of standard and optional features that members may select when they participate in MasterCard programs.

File Update Request/0302	
Type:	Interactive
Routing:	Directly from an issuer or through NICS™ to the MasterCard AMS. For MDS Stand-In processing, routing is to the MDS. Messages will be routed to both systems if the issuer participates in both services. In cases where the file update request is routed to both AMS and Stand-In, the MDS must receive an approved response from both systems in order to send an approved response to the issuer. If either system does not provide this response, the MDS will return a File Update Request Response/0312 message to the issuer containing a declined/failed response in DE 39 (Response Code).
Purpose:	Requests update of a file, typically a file used to minimize fraudulent usage of, or give preferential treatment to, the financial transaction cards provided by the issuer to its account holders or other customers.
Response:	A File Update Request Response/0312 is **required**.

File Update Request Response/0312	
Type:	Interactive
Routing:	From the MasterCard AMS via the MDS to the issuer. For MDS Stand-In processing, routing is from the MDS to the issuer.
Purpose:	Carries response information to the File Update Request/0312.
Response:	None

The transaction message flows provided throughout the remainder of this chapter define all of the ISO 8583–1987 transaction flow procedures implemented on the MDS. These flows sometimes depict a "timeout" or late response situation.

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

The following tables illustrate the message flow for file update messages. Issuers use file update messages to maintain fraudulent card-use ("hot card") or VIP databases that are available for users at the MDS and at the AMS.

Two file update services are available:

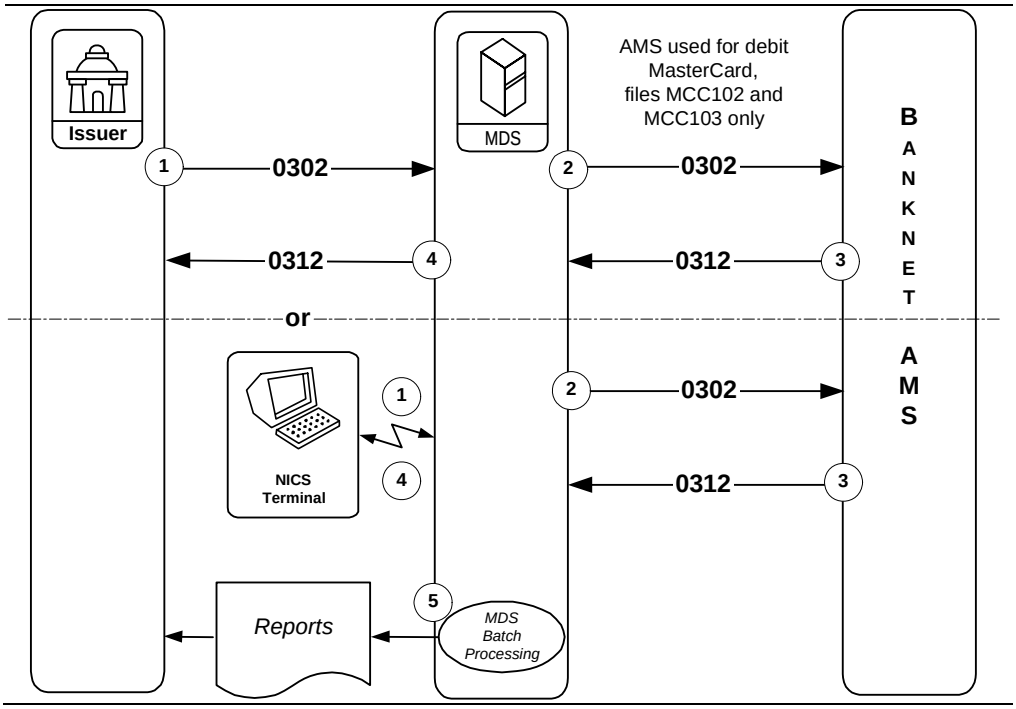
- File Update/0xx, Case 1: For debit MasterCard accounts which require access to AMS through use of MCC102 (Account File) and MCC103 (Account Management File) updates.
- File Update/0xx, Case 2: For Maestro and Cirrus accounts that use the MCCNEG (MDS Stand-In Negative File) updates.

File Update/03xx, Case 1—Debit MasterCard

In File Update/0xx, Case 1, the files being updated are the MCC102 and MCC103 files, which are maintained through the AMS. These updates apply to debit MasterCard cards only. For debit MasterCard issuers participating in the MDS Stand-In service, accepted AMS updates will also be updated in the MCCNEG File.

The following figure shows two separate flows: one originating from the issuer's online transaction processing (OLTP) system and the other from the NICS™ terminal by the issuer or issuer's authorized personnel.

File Update/0xx, Case 1—Debit MasterCard



Stage	Description
1.	Issuers send File Update Request/0302 messages from their OLTP systems or from their NICS™ terminal. When issuers send file updates from their OLTP system, the File Update Request/0302 message is sent to the MDS online interface. When issuers send file updates from a NICS™ terminal, the file update request information is in an internal message format (IMF), but contains the same essential data as the File Update Request/0302 message.
2.	The MDS receives the File Update Request/0302 message through its file update processing facility, which passes the File Update Request/0302 message to the AMS.
3.	The AMS responds to the File Update Request/0302 message with a File Update Request Response/0312 message.
4.	The MDS returns the response to the issuer. For the OLTP connection, the issuer will receive a File Update Request Response/0312 message. For the NICS™ connection, the issuer will obtain a screen image update reflecting the response. (The MDS sends an IMF message, which contains the File Update Request Response/0312 data, to the terminal).

Stage	Description
5.	Before sending the response to the issuer, the update processing facility logs the completed transaction data. From this update log file, the MDS batch processing facility generates update reports and makes them available to the issuer. These reports indicate to the issuer all the file updates that have been processed both through OLTP and NICS™.

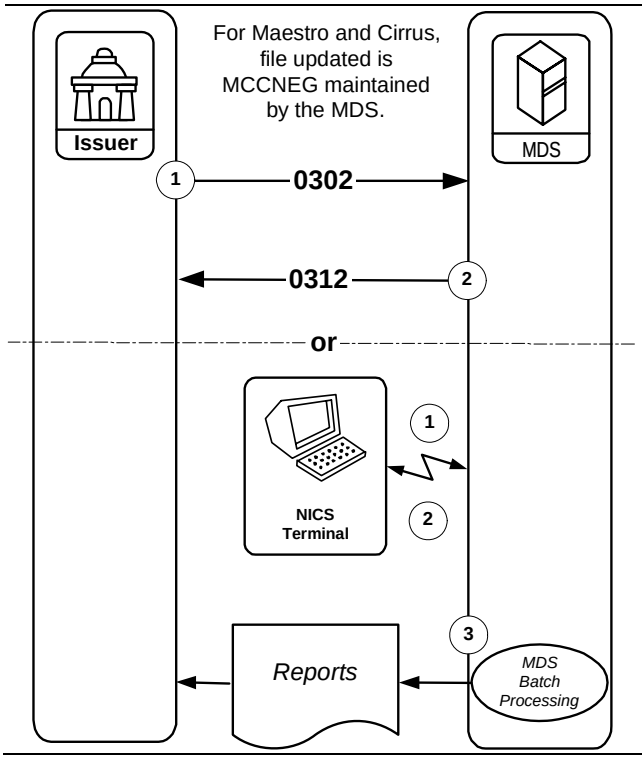
File Update/03xx, Case 2—Maestro and Cirrus

The File Update/03xx, Case 2 transaction flow illustrates the file update process for the Cirrus and Maestro negative card files, which are maintained on behalf of the issuer by the MDS.

In File Update/03xx, Case 2—Maestro and Cirrus, the issuer is updating the negative file that contains card numbers that should not be accepted. The MDS maintains and reads for Stand-In authorization of financial requests. The name of this file is MCCNEG. These updates apply to Maestro and Cirrus cards only.

The following table illustrates two separate flow paths: one originating from the issuer's online transaction processing (OLTP) system and the other from the NICS™ terminal by the issuer or issuer's authorized personnel.

File Update/03xx, Case 2—Maestro and Cirrus



Stage	Description
1.	From the OLTP system, the File Update Request/0302 message is sent to the MDS. From the NICS™ terminal, the file update request information is in an internal message format (IMF), but contains the same essential data as the File Update Request/0302 message.
2.	The MDS receives the File Update Request/0302 message through its file update processing facility, which updates the MCCNEG file. Then the MDS returns a response to the issuer. For the OLTP connection, the issuer will receive a File Update Request Response/0312 message. For the NICS™ connection, the issuer will obtain a screen image update reflecting the response. The MDS sends an IMF message, which contains the File Update Request Response/0312 data, to the terminal.

Stage	Description
3.	Before sending the response to the issuer, the update processing facility logs the completed transaction data. From this update log file, the MDS batch processing facility generates update reports and makes them available to the issuer. These reports indicate to the issuer all the file updates that have been processed both through OLTP and NICS™.

Reversal Advice/04xx Messages

Reversal advice/04xx messages reverse the impact of a previous Authorization/01xx or Financial Transaction/02xx message.

The ISO 8583–1987 online specification employs only "non-interactive" reversal advice messages. These messages come under the general category of "Advice" messages; therefore, they are subject to the guaranteed advice delivery procedures that are standard for all Advice messages.

If, for any reason, these messages cannot be immediately delivered to their intended destination, the MDS automatically assumes responsibility for storing and forwarding them to the proper destination when communication has been reestablished with the appropriate destination processor.

The reversal advice message and its response can be designated Acquirer (0420/0430 sequence) or Issuer (0422/0432 sequence), and the MDS enables several usages within these categories.

Acquirer Reversal Advice/0420 Message	
Type:	Non-interactive
Routing:	From an acquirer to the MDS From the MDS to an issuer
Purpose:	Reverses (partially or wholly) an earlier Authorization/01xx or Financial Transaction/02xx message. The acquirer processing system usually generates this message upon detection of a malfunction at the point-of-interaction (POI). The MDS sends this message to an issuer upon receipt of a reversal or upon receipt of an adjustment from the acquirer. For settlement purposes, this message contains "force-post" information. Thus, the reversal will be processed regardless of message receipt acknowledgment.

Acquirer Reversal Advice/0420 Message	
Purpose:	The Acquirer Reversal Advice/0420 message has four uses: • **Standard Reversal Advice** (before settlement)—most commonly used to correct or cancel the amount dispensed or authorized from the original terminal request. • **Timeout-induced Reversal Advice** (before settlement)—available to acquirers when the Financial Transaction Request Response/0210 does not arrive back to the acquirer in the required time. • **NICS-generated Exception Item** (after settlement)—the acquirer may use NICS™ to make an adjustment to an amount through the MDS Adjustment Manager, which the MDS passes on to the issuer in the form of a 0420 reversal. • **Online Exception** (after settlement)—available to acquirers after the settlement day of the original transaction. This abbreviated 0420 message may be submitted to the MDS through the acquirer's online processing facility, which the MDS will pass to the issuer as a 0420 reversal advice.
Response:	An Acquirer Reversal Advice Response/0430 message is required.

Acquirer Reversal Advice Response/0430 Message	
Type:	Non-interactive
Routing:	From an issuer to the MDS From the MDS to an acquirer
Purpose:	Must be sent in response to an Acquirer Reversal Advice/0420 message, to acknowledge positive receipt of that message.
Response:	None

Issuer Reversal Advice/0422 Message	
Type:	Non-interactive
Routing:	From an issuer to the MDS (for a subsequent day NICS™ adjustment or issuer online adjustment) From the MDS to an acquirer

Issuer Reversal Advice/0422 Message	
Purpose:	Reverses (partially or wholly) an earlier transaction The MDS generates this message upon notice of an adjustment, chargeback, or representment for the acquirer. For settlement purposes, this message contains "force-post" information. Thus, the reversal will be processed regardless of message receipt acknowledgment. The ISO 8583 Issuer Reversal Advice/0422 message has two uses: • **NICS-generated Exception Item** (after settlement)—the issuer uses NICS™ to make a chargeback of a requested amount made in a previous day's Financial Transaction Request/0200 through the MDS Adjustment Manager, which the MDS passes on to the acquirer in the form of a Issuer Reversal Advice/0422 message. • **Online Exception** (after settlement)—for issuers, after the settlement day of the original transaction, an abbreviated Issuer Reversal Advice/0422 message may be submitted to the MDS through the issuer's online processing facility, which the MDS will pass to the acquirer as an Issuer Reversal Advice/0422 message.
Response:	An Issuer Reversal Advice Response/0432 message is required.

Issuer Reversal Advice Response/0432 Message	
Type:	Non-interactive
Routing:	From the MDS to an issuer From the acquirer to the MDS
Purpose:	Must be sent in response to an Issuer Reversal Advice/0422 message, to acknowledge positive receipt of that message.
Response:	None

The transaction flows provided throughout the remainder of this chapter define all of the ISO 8583–1987 transaction flow procedures implemented on the MDS. These flows sometimes depict a "timeout" or late response situation.

Reversal Advice/042x Transaction Exception Processing

MasterCard provides members access to certain functions and data within the MDS application in two ways:

- NICS™—An authorized member representative (or authorized representatives of MasterCard) can use NICS™ to adjust a previous transaction by initiating an exception message. These exceptions are normally performed following the settlement day of the original transaction In the case of the issuer-initiated NICS™ exception, they must be performed following the settlement day of the original transaction.
- Online interface—Processors can access to the MDS transaction exception facility by sending appropriate online Reversal Advice/042x exception messages to the MDS. The functionality is known as online exception processing. Online exceptions are available to the processors on a day following the settlement day.

Each method initiates one of the following types of exception message:

- Chargeback: An issuer-generated reversal advice message that informs an acquirer that a previously completed charge to the cardholder's account is not valid, and that the acquirer will be "charged back" that amount. A chargeback results in a credit to the issuer and a debit to the acquirer.
- Adjustment: An acquirer-generated reversal advice message that corrects the amount settled in a previously completed transaction. An adjustment may result in either a debit or a credit to the issuer.
- Representment: An acquirer-generated reversal advice message that informs an issuer a previous chargeback from the issuer is not valid, and the transaction is being "represented" for settlement. A representment results in a debit to the issuer and a credit to the acquirer.

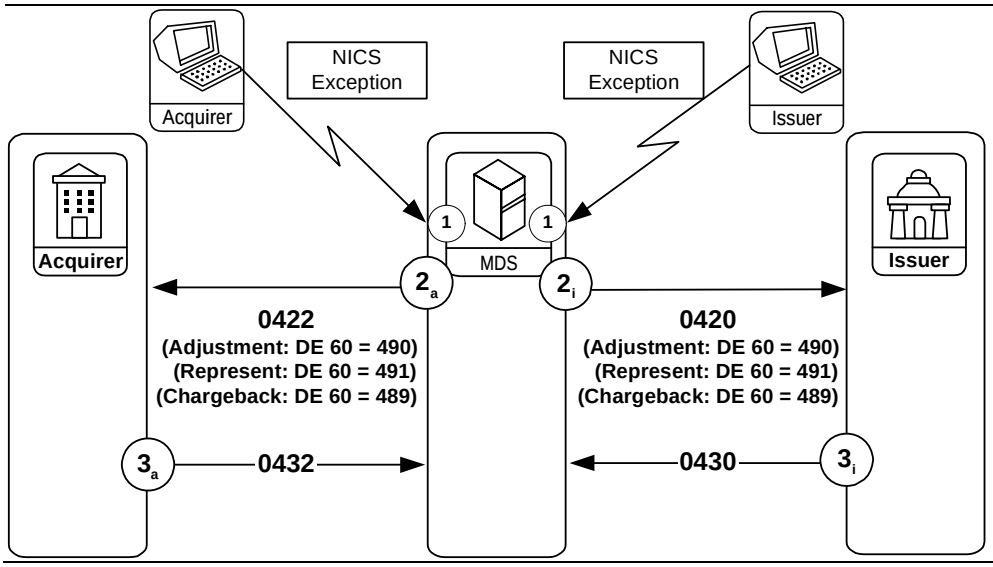
Each of the above forms of a transaction exception-item processing message is represented in an Acquirer Reversal Advice/0420 exception message or an Issuer Reversal Advice/0422 message.

Note **The names of the message types at this point still use "reversal" to indicate the change being made.**

NICS Exception Advice Processing

Past editions referred to these messages as MDS-generated because the external ISO 8583 message is produced by the Adjustment Manager process within the MDS application. The messages are the result of initial request made through the NICS™ terminal. The following table illustrates this processing.

NICS Exception Advice Processing



Stage	Description
1.	Authorized representatives of an acquirer, an issuer, or the MDS use NICS to create one of the following exception items: • Chargeback (originates from issuer) • Adjustment (from acquirer) • Representment (from acquirer)
2.	After the MDS generates a chargeback, adjustment, or representment, it forwards these messages to the issuer and the acquirer processors. The acquirer always receives an Issuer Reversal Advice/0422; the issuer always receives an Acquirer Reversal Advice/0420. Both the Acquirer Reversal Advice/0420 and Issuer Reversal Advice/0422 messages contain DE 90 (Original Data Elements) with the same data elements as the original transaction in order to identify the financial transaction impacted by the reversal advice. • Chargeback: DE 60 = 489nnnn [a] • Reversal: DE 60 = 490nnnn [a] • Representment: DE 60 = 491nnnn [a]

Stage	Description
3.	In all cases, the acquirer's processing system must acknowledge the Issuer Reversal Advice/0422 with an Issuer Reversal Advice Response/0432. Similarly, the issuer's processing system must acknowledge receipt of the Acquirer Reversal Advice Response/0430 message. All reversal advices contain settlement amount and transaction fee data that affect MDS reconciliation and settlement.

[a] nnnn = 4 digit advice detail code in subfield 2 of DE 60.

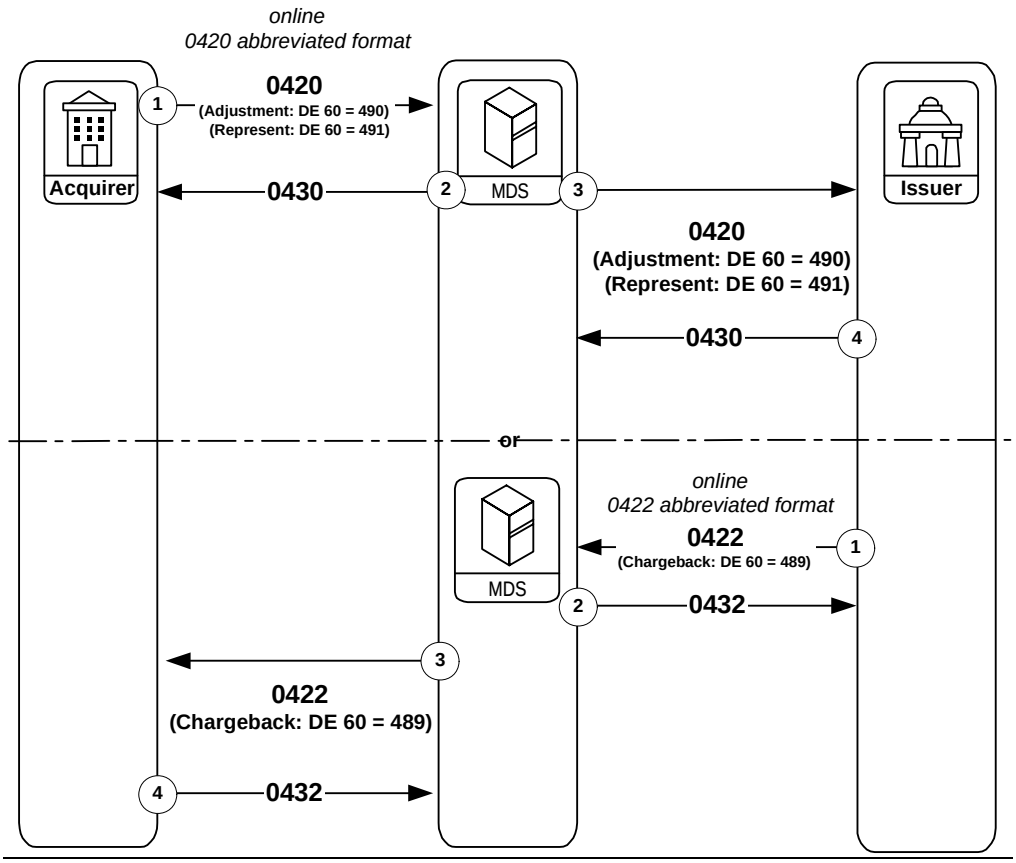
Online Exception Messages

The exception in these circumstances may be an abbreviated set of the normal 0420/0422 reversal advice message. The following data elements are required:

- DE 2 (Primary Account Number [PAN])
- DE 7 (Transmission Date and Time)
- DE 11 (System Trace Audit Number)
- DE 15 (Date, Settlement)
- DE 60 (Advice Reason Code)
- DE 63 (Network Data)
- DE 95 (Replacement Amounts)

Online exceptions are available to the processors on a day following the settlement day. The following table illustrates the basic flow for online exception messages. All Reversal Advices contain settlement amount and transaction fee data that are included with MDS reconciliation and settlement.

Online Exception Processing



Stage	Description
1.	The processor initiates an online exception message • Chargeback/0422 (issuer) • Adjustment/0420 (acquirer) • Representment/0420 (acquirer)
2.	The MDS responds with the appropriate (0430 to an acquirer, 0432 to an issuer) Reversal Advice Response/043x message.

Stage	Description
3.	If the MDS receives a valid adjustment or a representment from the acquirer the MDS creates an Acquirer Reversal Advice/0420–Exception message to the issuer. If the MDS receives a valid chargeback from the issuer, the MDS creates an Issuer Reversal Advice/0422 message to the acquirer. The following advice DE 60 (Reason Codes) apply: • Chargeback: DE 60 = 489nnnn [a] • Adjustment: DE 60 = 490nnnn [a] • Representment: DE 60 = 491nnnn [a]
4.	Issuing processors reply to the Acquirer Reversal Advice/0420 message with an Acquirer Reversal Advice Response/0430 message. Acquiring processors reply to the Issuer Reversal Advice/0422 message with an Issuer Reversal Advice Response/0432 message.

[a] nnnn = 4 digit advice detail code in subfield 2 of DE 60.

Note

Refer to the *NICS Users' Guide* for specific information on the procedures for processing chargebacks, adjustments, and representments.

To use the MDS online exception facility, the processor's online interface application must format and send the appropriate 042x advice message to the MDS online interface. Refer to chapter 3 for the definition of these reversal—exception message records.

Administrative Advice/06xx Messages

The Administrative Advice/06xx messages may be used between any two parties (processors) connected to the MDS.

The originator routes the messages to a destination; no distinction is made as to whether or not the originator or destination is an issuer or an acquirer.

The ISO 8583–1987 online specification employs only "non-interactive" administrative advices. These messages fall under the general category of "advice" messages; therefore, they are subject to the guaranteed advice delivery procedures that are standard for all Advice messages. If for any reason the intended destination does not immediately receive these messages, the MDS will automatically assume responsibility of storing and forwarding them to the proper destination when network delivery-point communication has been reestablished.

The MDS uses Administrative Advice/06xx messages to return indecipherable messages to a message originator with an appropriate error condition code indicating the point at which the MDS terminated message parsing or message processing. The types of messages returned in an Administrative Advice/0620 message would either have, improperly coded Message Type Indicator (MTI) fields or improperly coded bit maps.

Note **In all cases, the Advice Reason Code within the Administrative Advice/0620 message determines the specific reason for the Advice message.**

Administrative Advice/0620 Message	
Type:	Non-interactive
Routing:	Between the MDS and a card payment system, or between any two processors participating on the MDS.
Purpose:	To transmit administrative or informational messages for various reasons, as indicated in the Advice Reason Code of the message.
Response:	An Administrative Advice Response/0630 message is required.

Administrative Advice Response/0630 Message	
Type:	Non-interactive
Routing:	From the receiver to the originator of the related Administrative Advice.
Purpose:	Must be sent in response to an Administrative Advice/0620 message to acknowledge receipt of that message.
Response:	None

Administrative Advice/0644 Message	
Type:	Non-interactive
Routing:	Between the debit Virtual Private Network (VPN) or the Banknet® telecommunications network and a processor connected to the Banknet telecommunications network.
Purpose:	To return undelivered messages to the message originator with an appropriate error condition code.
Response:	None

The transaction flows provided throughout the remainder of this chapter define all of the ISO 8583–1987 transaction flow procedures implemented on the MDS. These flows sometimes depict a "timeout" or late response situation.

Administrative Advice/06xx—MDS Initiated

The MDS uses an Administrative Advice/0620 message to reject invalid messages received from the processor.

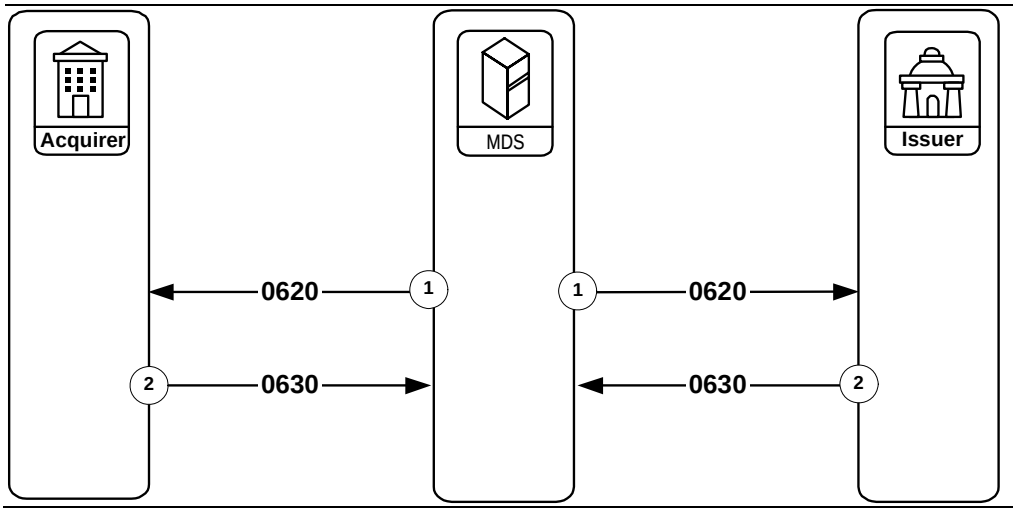
When the processor sends an unrecognizable or incorrectly formatted message to the MDS, the MDS interface process responds by generating an Administrative Advice/0620 message to reject the invalid message. The following table lists all message types that can be rejected using the Administrative Advice/0620 message.

Table 2.1—Rejected Message Types

MTI	Message Name
0200	Financial Transaction Request
0210	Financial Transaction Request Response
0220	Financial Transaction Advice
0230	Financial Transaction Advice Response
0302	File Update Request
0420	Acquirer Reversal Advice
0422	Issuer Reversal Advice
0430	Acquirer Reversal Advice Response
0432	Issuer Reversal Advice Response
0800	Network Management Request
0810	Network Management Request Response

The following table illustrates the message flow for Administrative Advice/06xx messages initiated by the MDS.

Administrative Advice/0620—MDS Initiated

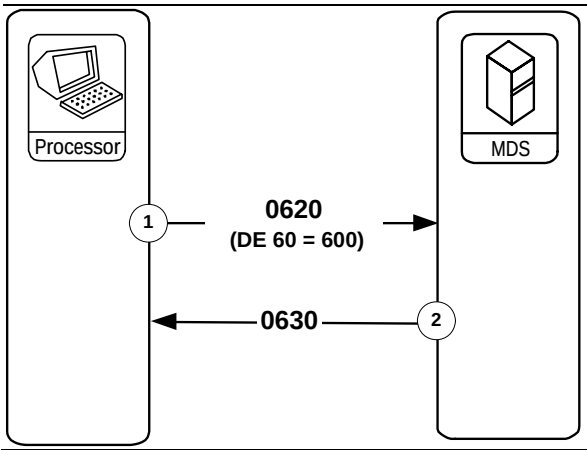


Stage	Description
1.	The MDS sends an Administrative Advice/0620 message to a processor
2.	The processor responds with an Administrative Advice Response/0630 message.

Administrative Advice/06xx—Processor Initiated

The following table illustrates the message flow for Administrative Advice/06xx messages initiated by the Processor to the MDS.

Administrative Advice/0620—Processor Initiated

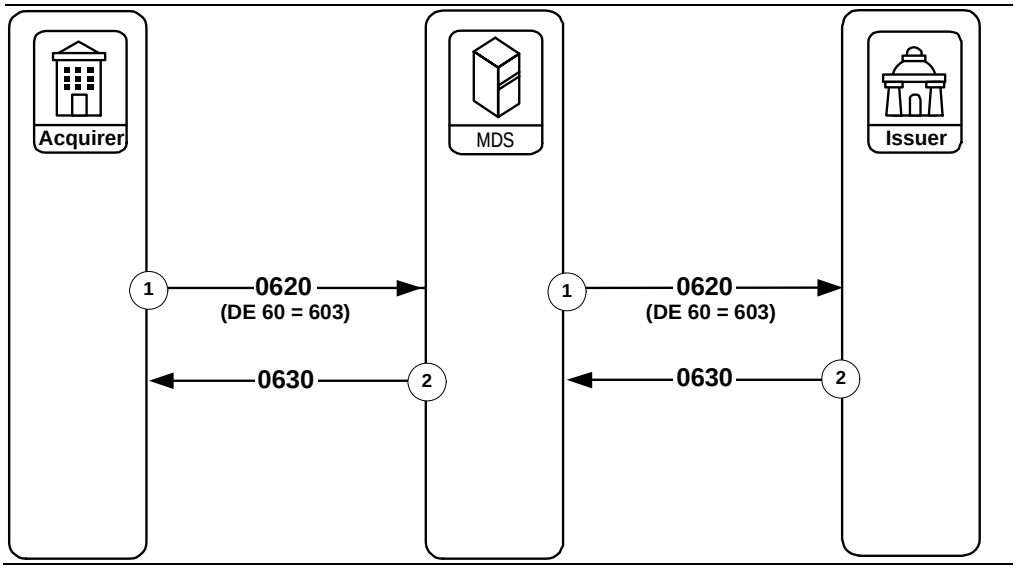


Stage	Description
1.	The acquirer processing system or the issuer processing system originates the Administrative Advice/0620 message to a processor. The Administrative Advice/0620 message contains DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) with the value 600 (Message unreadable/indecipherable/contains invalid data).
2.	The MDS responds to the Administrative Advice Response/0630 message which contains the same value in DE 60 as was received in the Administrative Advice/0620 message.

Administrative Advice/0620—Processor Initiated Time-Based Exception

The following table illustrates the message flow for Administrative Advice/06xx messages initiated by the Processor to the issuer.

Administrative Advice/0620—Processor Initiated Time-Based Exception

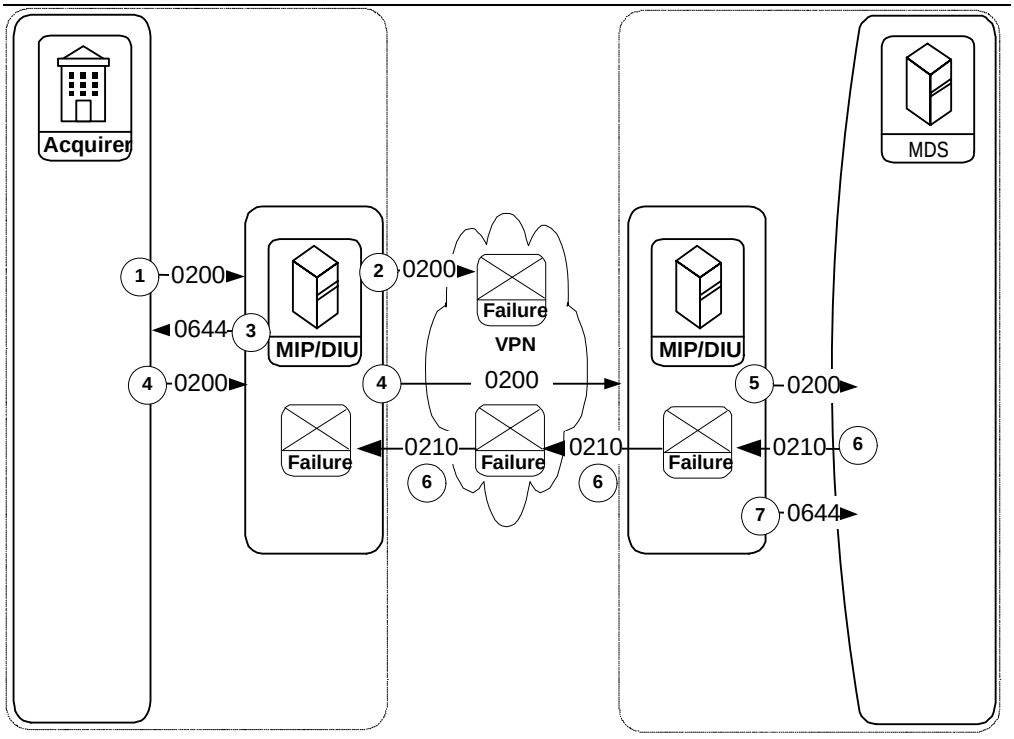


Stage	Description
1.	The acquirer processing system originates the Administrative Advice/0620 message to a processor. The Brazil Time-Based Exception contains DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code) with the value 603 (Message unreadable/indecipherable/contains invalid data).
2.	The Issuer responds to the Administrative Advice Response/0630 message that contains the same value in DE 60 as was received in the Administrative Advice/0620 message.

Administrative Advice/0644 for Virtual Private Network–Connected Acquirers

Processing between the MDS and an acquirer connected through the virtual private network (VPN) is the same as for an issuer connected through the VPN. Acquirers and issuers may be connected through either the debit virtual private network or the Banknet network.

Administrative Advice/0644—VPN Acquirer



Consider the following two scenarios for VPN acquirers:

Administrative Advice/0644—VPN Acquirer

Stage	Description
1.	The acquirer sends a Financial Transaction Request/0200 message to the debit port on the MIP or to the Debit Interface Unit (DIU).
2.	The acquirer's MIP or DIU is unable to deliver the Financial Transaction Request/0200 message to the VPN.
3.	The acquirer's MIP or DIU generates an Administrative Advice/0644 message to the acquirer. The value contained in DE 60 (Advice Reason Code) indicates the reason for the failure. OR,

Administrative Advice/0644—VPN Acquirer	
Stage	**Description**
4.	The acquirer sends a Financial Transaction Request/0200 message to the debit port on the MIP or the DIU, which forwards the message to the VPN.
5.	The VPN forwards the Financial Transaction Request/0200 message to the MDS MIP. These MIPs are found at the site(s) of the MDS application and are known as "Central Site MIPs", which forward the message to the MDS.
6.	If the Financial Transaction Request Response/0210 message indicates an approval and the central-site MIP cannot deliver it [a], then.
7.	The Central Site MIP generates an Administrative Advice/0644 message to the MDS. The value contained in DE 60 (Advice Reason Code) indicates the reason for the failure.

[a] This can occur because of a failure at the central-site VPN interface or at the VPN acquirer interface (typically, the failure would be the MIP does not have confirmation that the remote MIP delivered the 0210 to the acquirer host.)

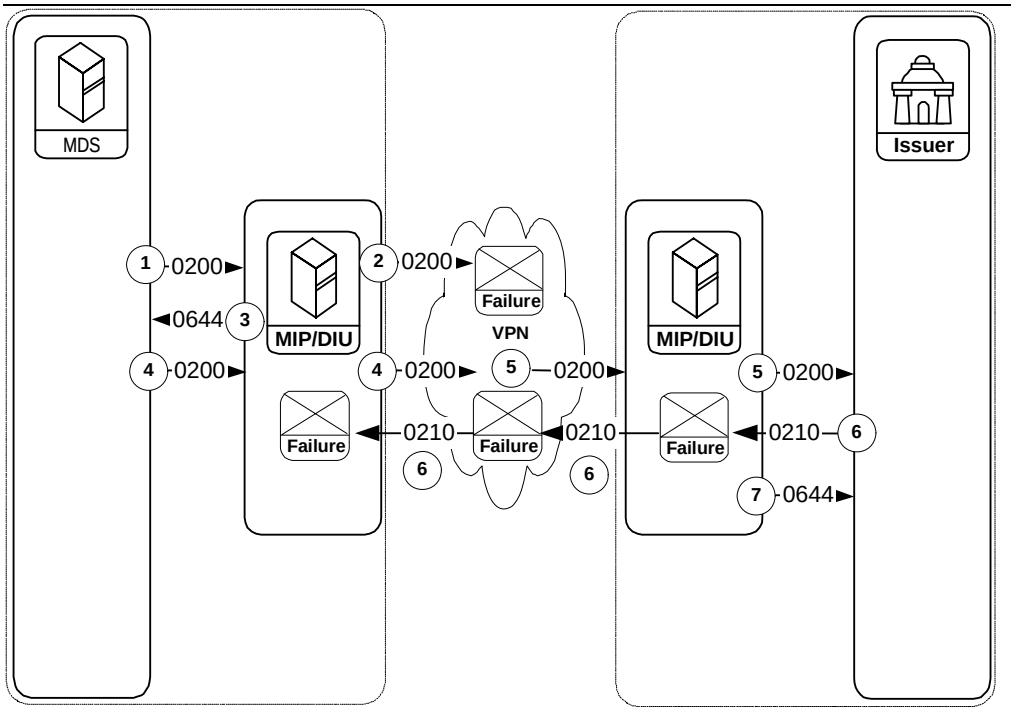
Note

The Administrative Advice/0644—VPN Acquirer transaction message flow shows the internal details of the Administrative Advice/0644 message processing. Following the perceived failure of delivery of the Financial Transaction Response/0210 message by the MDS, the MDS continues to resolve the failure in accordance with normal exception processing.

Administrative Advice/0644 for Virtual Private Network–Connected Issuers

Processing between the MDS and an issuer connected through the VPN is the same as for an acquirer connected through the VPN.

Administrative Advice/0644—VPN Issuer



Consider the following two scenarios for VPN issuers:

Stage	Description
1.	The MDS sends a Financial Transaction Request/0200 message to the MDS MIP—these MIPs located at the site(s) of the MDS application are often referred to as Central Site MIPs.
2.	The Central Site MIP is unable to deliver the Financial Transaction Request/0200 message to the VPN.
3.	The Central Site MIP generates an Administrative Advice/0644 message to the MDS. The value contained in DE 60 (Advice Reason Code) indicates the reason for the failure. OR,
4.	The MDS sends a Financial Transaction Request/0200 message to the Central Site MIP that forwards the message to the VPN.

Stage	Description
5.	The VPN forwards the Financial Transaction Request/0200 message to the issuer. The issuer receives the transaction through the debit port on the MIP or the DIU.
6.	If the Financial Transaction Response/0210 message indicates an approval and the issuer MIP or DIU cannot deliver the Financial Transaction Response/0210 message to the VPN (for example, the issuer MIP or DIU times-out), or because of a failure at the MDS interface to the VPN, then:
7.	The issuer MIP or DIU generates an Administrative Advice/0644 message to the issuer. The value contained in DE 60 (Advice Reason Code) indicates the reason for the failure.

Note

The Administrative Advice/0644—VPN Issuer transaction message flow shows the internal details of the Administrative Advice/0644 message processing. Following the failure of reception of the Financial Transaction Response/0210 message from the issuer by the MDS, the MDS continues to resolve the failure in accordance with normal exception processing.

Network Management/08xx Messages

The MDS, acquirer processing systems, issuer processing systems, or intermediate network facilities use the network management messages to coordinate network events and tasks and to communicate network status conditions.

Typical uses of Network Management/08xx messages include:

- Sign-on/sign-off from the MDS
- Inquire on card payment systems or MDS status
- Perform encryption key management tasks
- Perform communication echo tests
- Advise of store-and-forward (SAF) end-of-file (EOF) condition
- SAF request

Within each Network Management Request/0800 message and Network Management Response/0810 message is a DE 70 (Network Management Information Code) used to determine the specific purpose or function of each Network Management message. Refer to chapter 4 for detailed information on the Network Management codes used within Network Management/08xx messages.

The MDS routes all Network Management/08xx messages from an originator to a destination; no distinction is made as to whether the originator or destination is an issuer or acquirer.

The following information defines all Network Management/08xx messages supported by the MDS.

Network Management Request/0800 Message	
Type:	Interactive
Routing:	Between the MDS and any other party (such as card payment system, acquirer processing system, issuer processing system, or intermediate network facility) communicating directly with the MDS. Either party may originate the message.
Purpose:	To control the interchange network by communicating or coordinating system condition or system security. The Network Management Information Code, a mandatory data element within all Network Management/08xx messages, determines the specific Network Management/08xx messages functions.
Response:	A Network Management Request Response/0810 message is **required**.

Network Management Request Response/0810 Message	
Type:	Interactive
Routing:	From destination to originator of the related Network Management Request/0800 message
Purpose:	Must be sent in response to a Network Management Request/0800 message to acknowledge receipt of that message.
Response:	None

Network Management Advice/0820 Message	
Type:	Non-interactive
Routing:	From the MDS to any other party (such as, card payment system, acquirer processing system, issuer processing system, or intermediate network facility) communicating directly with the MDS. This message originates from the MDS only.
Purpose:	To provide advisory information to processors connected to the MDS.
Response:	None

The transaction flows provided throughout the remainder of this chapter define all of the ISO 8583–1987 transaction flow procedures implemented on the MDS. These flows sometimes depict a "timeout" or late response situation.

Network Management Request/0800 and Network Management Request Response/0810

The MDS system uses Network Management/08xx messages to provide control mechanisms between the MDS and a processor for performing the following actions:

- Signing on and signing off by the processor to/from the MDS
- Establishing that communications exist between a processor and the MDS
- Initiating and concluding sessions for delivery of SAF messages
- Changing a PIN encryption key

Three types of Network Management/08xx messages exist:

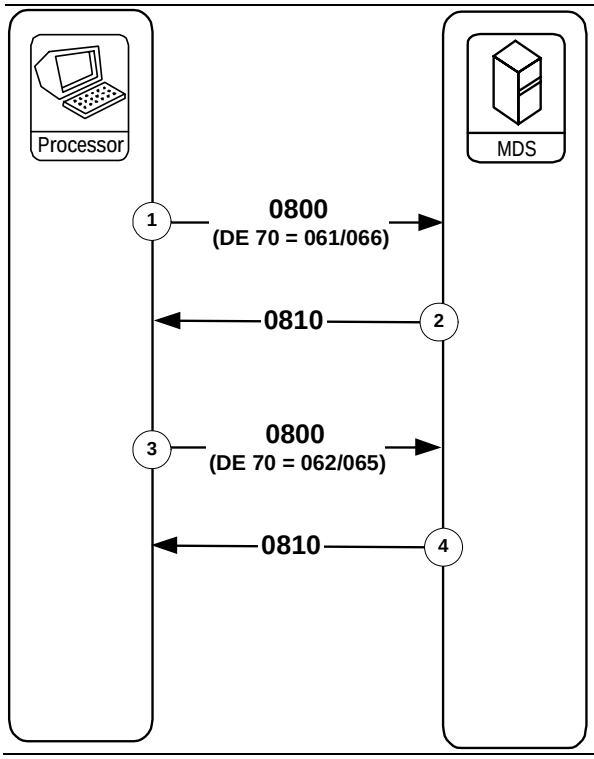
- **Network Management Request/0800**—The initiating message that identifies the purpose of the message.
- **Network Management Request Response/0810**—The response to the Network Management Request/0800, which indicates whether the request was received and approved.
- **Network Management Advice/0820**—A concluding message in some 08xx message processes, which either indicates the end of a store-and-forward file delivery cycle from the MDS, or confirms a PIN encryption key update from the MDS to the processor.

The value in DE 70 (Network Management Information Code) of the initial Network Management Request/0800 message distinguishes the function of the 08xx message process. The following descriptions show how the type of network management process is related to the value in DE 70.

Network Management/08xx—Sign-on and Sign-off

The following table illustrates the processor sign-on to the MDS and sign-off from the MDS.

Network Management/08xx—Sign-on and Sign-off



Stage	Description
1.	The acquirer processing system or the issuer processing system originates the Network Management Request/0800 message for signing-on to the MDS. For a sign-on message, DE 70 (Network Management Information Code) contains one of the following values: • 061 (General sign-on by processor to the MDS) • 066 (Issuer sign-on, directing the MDS to cease Stand-In processing for the issuer)
2.	The MDS responds to the sign-on request with a Network Management Request Response/0810 message, which contains the same value in DE 70 as was received in the Network Management Request/0800 message.

Stage	Description
3.	The acquirer processing system or the issuer processing system originates the Network Management Request/0800 message for signing off the MDS. For a sign-off message, DE 70 contains one of the following values: • 062 (General sign-off by processor off the MDS) • 065 (Issuer sign-off, directing the MDS to begin Stand-In processing for the issuer)
4.	The MDS responds to the sign-off request with a Network Management Request Response/0810 message, which contains the same value in DE 70 as was received in the Network Management Request/0800 message.

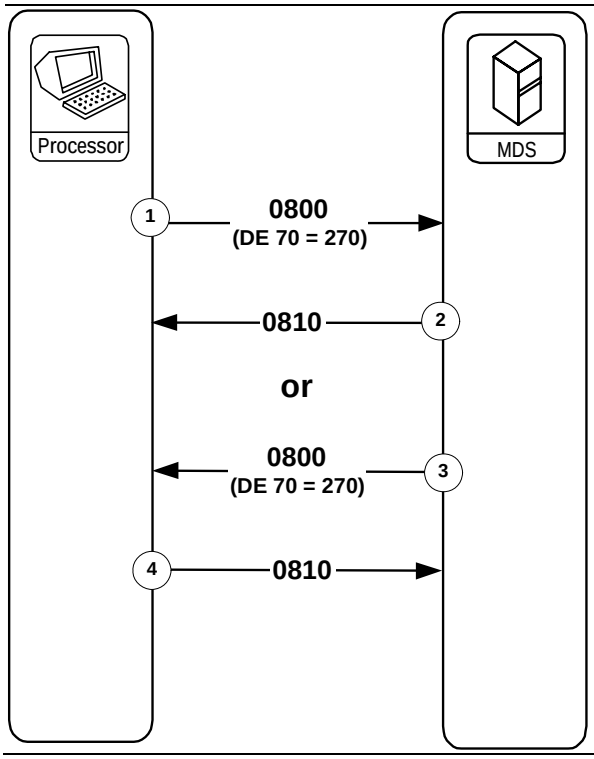
The Network Management Advice/0820 message is not used in any sign-on or sign-off process. The sign-on/sign-off sequence of messages was previously known as "class 0."

Warning **The error condition message flow for Network Management/08xx messages is not illustrated. Unsuccessful Network Management Request/0800 message transmissions should be retransmitted.**

Network Management/08xx—Echo Test

The processor can initiate an echo test to the MDS and the MDS can initiate an echo test to the processor. The echo test is a means of establishing whether a processor or the MDS is connected and available for processing messages.

Network Management/08xx—Echo Test



From the Processor to the MDS

Stage	Description
1.	The acquirer processing system or the issuer processing system initiates a Network Management Request/0800 message where DE 70 (Network Management Information Code) contains the value 270 (Echo Test) and sends it to the MDS.
2.	The MDS responds to the echo test request with a Network Management Request Response/0810 message, which contains the same value in DE 70 as that received from the processor in the Network Management Request/0800 message. Receipt of the Network Management Request Response/0810 message by the processor indicates the MDS is operating and can process message traffic.

Note

After sending the Network Management Request Response/0810 message to the processor, the MDS sends any messages in the SAF file to the processor. The MDS sends a Network Management Advice/0820 message to indicate the final message has been sent. The value for the Network Management Information Code (DE 70) in this 0820 message will be "363", SAF Delivery Complete (refer to Network Management/08xx—SAF Request by Processor to the MDS for additional details.)

From the MDS to the Processor	
Stage	**Description**
1.	The MDS initiates the Network Management Request/0800 message where DE 70 (Network Management Information Code) contains the value 270 (Echo Test) and sends it to the processor.
2.	The processor responds to the echo test request with a Network Management Request Response/0810 message, which contains the same value in DE 70 as that received from the MDS in the Network Management Request/0800 message. Receipt of the Network Management Request Response/0810 message by the processor indicates the processor is operating and can process message traffic. After sending the Network Management Request Response/0810 message to the MDS, the processor must send whatever messages exist for the MDS in the processor's SAF file. The member-initiated echo test sequence of messages was previously known as "class 2," and the MDS-initiated echo test message process was previously known as "class 3."

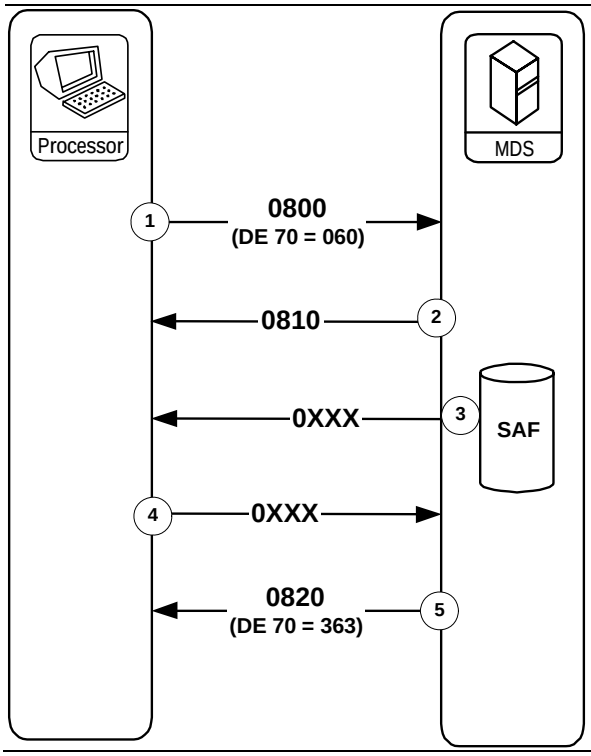
Note

The echo test is also the mechanism by which the MDS requests the processor to send any SAF messages the processor has for the MDS. The MDS will send the appropriate response to each request. When the processor sends these messages, the processor does not have to end the session by delivering a Network Management Advice/0820 message.

Network Management/08xx—SAF Request by Processor to the MDS

The following table illustrates a processor requesting that the MDS deliver the SAF file for the processor.

Network Management/08xx—SAF Request by Processor to the MDS



Stage	Description
1.	The acquirer processing system or the issuer processing system initiates the Network Management Request/0800 message containing DE 70 (Network Management Information Code) with the value 060 (Processor-initiated SAF session request) requesting delivery of messages from the MDS SAF file for the processor.
2.	The MDS responds to the SAF request with a Network Management Request Response/0810 message, which contains the same value in DE 70 as that received in the Network Management Request/0800 message.
3.	If the MDS has any messages for the processor in the SAF file, the MDS delivers these messages.

Stage	Description
4.	The processor responds to each advice, individually, with the appropriate message. • The MDS continues to send SAF messages to the processor until no messages for the processor remain. • Store-and-forward messages to an acquirer processing system may include any of the following message types: – Issuer Reversal Advice/0422 – Administrative Advice/0620 – Financial Transaction Negative Acknowledgement/0290 (special case—even though this is not an advice message) • Store-and-forward messages to an issuer processing system may include any of the following message types: – Financial Transaction Advice/0220 – Acquirer Reversal Advice Response/0420 – Administrative Advice/0620 – Financial Transaction Negative Acknowledgement/0290 (special case—even though this is not an advice message)
5.	The MDS sends to the processor a Network Management Advice/0820 message with DE 70 (Network Management Information Code) containing the value 363 (End-of-File (EOF encountered for SAF traffic. SAF complete).

The member-initiated SAF sequence of messages was previously covered under a designation of "class 2."

Note **The processor can also receive its SAF messages from the MDS by sending an echo test (DE 70 = 270) to the MDS as illustrated in the Network Management/08xx—Echo Test transaction message flow.**

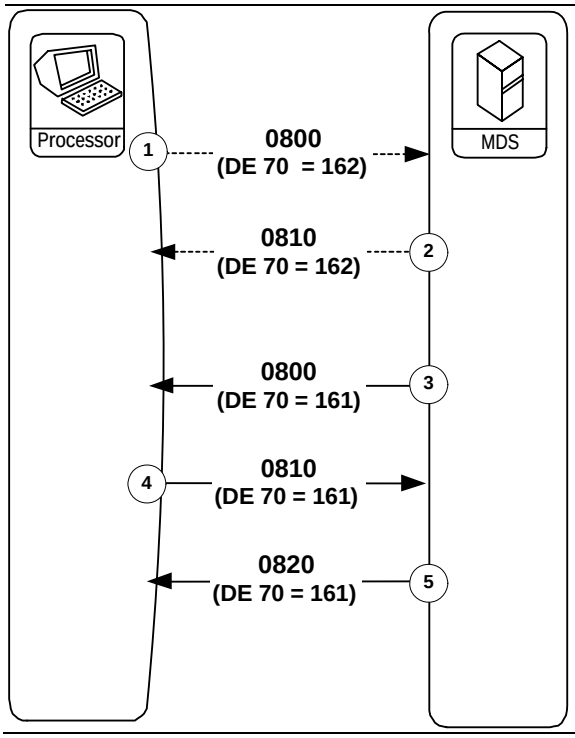
Network Management/08xx—PIN Encryption Key Change

The MDS changes the PIN encryption key used between the MDS and the processor every 12 hours. This key is also referred to as the "working key." Oct 2005

Previously, only the MDS could initiate a PIN Encryption Key Request/0800 message and processors would have to contact the MDS application monitoring group to request the generation of a new PIN encryption key outside of the normal schedule.

Processors can initiate the key change process by sending a Network Management Request/0800 message to the MDS where DE 70 contains the value 162 (Initiate Key Change). This is an optional feature shown with dotted lines as stages 1 and 2 below. When the MDS receives the Network Management Request/0800 message to initiate key change, the MDS responds with a Network Management Request Response/0810 message, then immediately starts the normal key change sequence (stages 3 thru 5 below) as shown in the following table: Oct 2005

Network Management/08xx—PIN Encryption Key Change



Network Management/08xx—PIN Encryption Key Change	
Stage	**Description**
1.	If the processor wants to initiate the key change sequence, the processor sends a Network Management Request/0800 where DE 70 (Network Management Information Code) contains the value 162 (Initiate Encryption Key Change [by processor])
2.	If the processor has initiated a key change sequence by sending an 0800 request with a DE 70 value of 162, the MDS responds with a Network Management Response/0810 with the same value in DE 70.
3.	The MDS originates a Network Management Request/0800 message to change the PIN encryption key (this is sometimes referred to as the "working key"). The 0800 request contains the following data: • DE 70 = 161 (PIN Encryption Key Change Request) • DE 48, subelement 11 (Key Exchange Data Block) contains the MDS Key Exchange Data Block, including the length prefix (indicating whether this is a single, double, or triple-length DES key), key cycle number, the actual PIN encryption key, and a key check value.
4.	The processor responds with a Network Management Request Response/0810 message, which contains the following data: • DE 39 = 00 if the response is an approval (if there is a problem then DE 39 contains "96" indicating a denial). • DE 70 = 161 (PIN Encryption Key Change Response) • DE 48 subelement 11 may be returned at processor's discretion, or some portion of the subelement, but it is not required.
5.	The MDS completes the sequence by sending a Network Management Advice/0820 message to the processor, indicating confirmation of the working key change. This message contains the following data: • DE 70 = 161 (PIN Encryption Key Change Confirmation) • DE 48 subelement 11 contains the first characters of the original Subelement 11 up to the beginning of the actual key.

The key change sequence of messages was previously referred to as "class 1."

Note **If the Network Management Request Response/0810 message indicated a denial, then the Network Management Advice/0820 message will not contain DE 48 and DE 70.**

3 Message Layouts

This chapter describes all required, conditional, optional, or MDS system-provided data element layouts for all messages the MDS supports.

Overview

This chapter describes all ISO 8583–1987 message formats employed by the MasterCard® Debit Switch (MDS).

The MDS supports all of the following ISO 8583–1987 messages. The message format specification charts on the following pages identify all of the required, conditional, optional, or network-generated data elements employed within each individual message.

Data Element Flow

Several entities may insert or modify the data elements in an MDS message as it flows from the message origin to the MDS system and from the MDS system to the message destination. These entities typically include the issuer or acquirer at the origin, the MDS system, and the issuer or acquirer at the destination.

In the message format layouts, the following three columns provide information to the originator, MDS system, and destination related to the data element requirements:

Entity	Description
Org	**Originator Requirements.** The message originator must satisfy this data element's requirements before sending the message. A Financial Transaction Request/0200 from an acquirer is an example of an originator message.
Sys	**MDS System Requirements.** The MDS system may insert, correct, modify, or echo this data element while, for example, routing a message from the origin to the destination. The MDS system may overwrite the data element and thereby destroy any previous content.
Dst	**Destination Requirements.** The message destination must expect this data element (read it) and accept this data element (process it) if the originator requirements are satisfied. A Financial Transaction Request/0210 from an issuer is an example of a destination message.

Data Element Message Format Requirements

The following notations describe the requirements for each data element. These notations appear in the originator (Org), MDS System (Sys), and destination (Dst) entities.

Note **In some cases the MDS system is the originator or the destination of the message.**

The originator or destination can only use the codes in the following table:

Usage Code	Description
M	**Mandatory**. The data element is required in the message.
C	**Conditional**. The data element is required in the message if the conditions described in the accompanying text are applicable.
O	**Optional**. The data element is not required but may be included in the message at the message initiator's option.
•	**Not Required** or **Not Applicable**. The data element is not required or not applicable.

Only the MDS system can use the following codes:

Usage Code	Description
X	**Interaction**. The data element will be accepted, inserted or overwritten by the MDS. Any modification is determined by specific programs and services.
P	**Pass-through**. The data element is forwarded by the MDS to the destination (unmodified).

Summary of Message Type Supported

The MasterCard® Debit Switch (MDS) supports the following ISO 8583–1987 message types.

MTI	Description
Authorization/01xx Messages	
0100	Supported for credit card issuer-only processing. The MDS passes Authorization Request/0100 messages to and from the Banknet network on behalf of Banknet processors; however, the MDS only communicates with MDS processors using the Financial Transaction/02xx message formats.
Financial Transaction/02xx Messages	
0200	Financial Transaction Request
0210	Financial Transaction Request Response
0220	Financial Transaction Advice
0230	Financial Transaction Advice Response
0290	Financial Transaction Negative Acknowledgment
File Update/03xx Messages	
0302	File Update Request
0312	File Update Request Response
Reversal Advice/04xx Messages [a]	
0420	Acquirer Reversal Advice
0422	Issuer Reversal Advice
0430	Acquirer Reversal Advice Response
0432	Issuer Reversal Advice Response
Administrative Advice/06xx Messages	
0620	Administrative Advice
0630	Administrative Advice Response
0644	Administrative Advice [b]

Network Management/08xx Messages	
0800	Network Management Request
0810	Network Management Request Response
0820	Network Management Advice

[a] The word reversal is often used generically to mean any change or exception made to an original transaction, and the name of the 042x message type, i.e., "Reversal Advice," suggests this generic meaning is the appropriate usage. However, a 042x Reversal Advice message can contain one of the following:

- An acquirer-generated reversal due to a terminal error or to cancel a financial request at the terminal.
- An acquirer-generated adjustment to the original request, made on a subsequent day using one of the MDS adjustment processes.
- An issuer-generated chargeback made using one of the MDS adjustment processes.
- An acquirer-generated representment made using one of the MDS adjustment processes.
- The common understanding is a reversal (as a specific kind of transaction exception request) occurs from the acquirer closely following the original transaction, and an adjustment is a non-automatic exception made on a subsequent day by a processor using one of the MDS adjustment processes.

[b] Debit Pass-through only for members connected to the Banknet® telecommunications network.

Financial Transaction Request/0200

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	P	M	Value must be 0200.
-	Bit Map, Primary	M	P	M	Mandatory for all messages
1	Bit Map, Secondary	C	P	C	Required only if any of DE 65 through DE 128 are present in the message
2	Primary Account Number	M	P	M	Contains a cardholder's Primary Account Number (PAN)
3	Processing Code	M	P	M	Indicates type of transaction and the affected cardholder account type
4	Amount, Transaction	M	P	M	Transaction amount in the currency of the acquirer's card acceptor. DE 49 (Currency Code, Transaction) also must be present in conjunction with this data element to identify the currency of the transaction.
5	Amount, Settlement	•	X	C	Transaction amount in the currency of issuer DE 50 (Currency Code, Settlement) [a]. The MDS provides this data element for ISIS transactions, transactions where the currency conversion assessment is applied, and transactions where the issuer settlement currency DE 50 is different from DE 49 (Currency Code, Transaction). DE 5 may include Currency Conversion Assessment. DE 5 will be exclusive of ICCR and fees. When DE 5 is present, DE 9, DE 16, and DE 50 also must be present in the message. Oct 2005
6	Amount, Cardholder Billing	•	X	M	Amount billed to the cardholder in the currency of the cardholder account DE 51 (Currency Code, Cardholder Billing) exclusive of cardholder billing fees, ICCR, and Currency Conversion Assessment. This data element is mandatory and is provided by the MDS for transactions where the currency conversion assessment is applied. In addition, when DE 6 is present, DE 10, DE 16, and DE 51 also must be present in the message. Oct 2005
7	Transmission Date and Time	M	X	M	Date and time, in Universal Time (UTC) that the originator initiates the message. Upon receipt, the MDS updates this data element with its time stamp.

Data Element ID and Name		Org	Sys	Dst	Comments
8	Amount, ICCR	•	X	C	Contains the amount reflecting the ICCR adjustment.
9	Conversion Rate, Settlement	•	X	C	DE 5, DE 9, DE 16, and DE 50 are included when the currency of transaction differs from the currency of settlement.
10	Conversion Rate, Cardholder Billing	•	X	M	Factor used in the conversion from transaction to cardholder billing amount. DE 4 (Amount Transaction) is multiplied by DE 10 to determine DE 6 (Amount, Cardholder Billing).
11	System Trace Audit Number	M	P	M	Transaction trace number. Contents of this data element must be unique for each transaction initiated by a message originator on any single UTC date.
12	Time, Local Transaction	M	P	M	Local time of the transaction at the point-of-service as printed on all cardholder receipts and statements.
13	Date, Local Transaction	M	P	M	Local date of the transaction at the point-of-service as printed on all cardholder receipts and statements.
14	Date, Expiration	C	P	C	May be present in a debit MasterCard manually keyed authorization request.
15	Date, Settlement	•	X	M	Contains the settlement date of the transaction. Remains the same for all subsequent messages.
16	Date, Conversion	•	X	M	This field contains the effective date of any currency conversion performed for this transaction. Must be present in the message whenever the Amount, Settlement (DE 5), or Amount, Cardholder Billing (DE 6) is present.
18	Merchant Type (MCC)	M	P	C	Must be present on all transactions and reflect the business product or service provided.
22	Point-of-Service Entry Mode	M	P	M	Indicates the method used to enter the transaction into the interchange.
23	Card Sequence Number	C	P	C	Must be present for all transactions, which include DE 55 (EMV compliant ICC system related data) and where the ICC provides the application PAN sequence number (tag 5F34) to the terminal.
26	Point-of-Service PIN Capture Code	C	P	C	Required only if PIN data is present and the terminal PIN capture capability is **other than** 12 characters.

Oct 2005

Data Element ID and Name		Org	Sys	Dst	Comments
28	Amount, Transaction Fee	C	P	C	Must contain ATM access fee, if applied.
32	Acquiring Institution Identification Code	M	P	M	Must contain an acquirer's identification number. Acquirer's Federal Reserve Routing and Transit number or a MasterCard assigned pseudo number.
33	Forwarding Institution Identification Code	M	P	M	Must contain the processor ID number of the CPS forwarding this message to the MDS.
35	Track 2 Data	M	P	M	Information encoded on Track 2 of the magnetic stripe. In ICC transactions where sub-field 1 of DE 22 (POS Entry Mode) is 05 or 07, this data element contains 'Track 2 Equivalent data' (EMV tag 57) which is read from the ICC card. This data element is mandatory in transactions where DE 22, subfield 1 is 80 or 91.
37	Retrieval Reference Number	C	P	C	Acquirer may use this as a document retrieval access key. If present, the system must send it back to the acquirer in any subsequent chargeback. DE 37 is mandatory in ICC transactions and proximity transactions (where DE 22, subfield 1 is 05, 07, 80, or 91).
41	Card Acceptor Terminal Identification	M	P	M	Must contain a terminal or merchant number. The member must return it in any subsequent response.
42	Card Acceptor Identification Code	C	P	C	Must contain a merchant identifier for Maestro® ATM/POS and debit MasterCard POS transactions.
43	Card Acceptor Name and Location	M	P	M	Mandatory for all transactions. Provides location data.
45	Track I Data	C	P	C	May be present in debit MasterCard Authorization Request
48	Additional Data	C	P	C	Contains a variety of subelements depending on the card and purpose of the request. Refer to the detailed description in chapter 4.
49	Currency Code, Transaction	M	P	M	Identifies the currency of the transaction, such as the currency used at the point-of-service.
50	Currency Code, Settlement	•	X	C	MDS provided data element. Required if present in the message. Identifies the currency of DE 5 (Amount, Settlement).

Data Element ID and Name		Org	Sys	Dst	Comments
51	Currency Code, Cardholder Billing	•	X	M	Identifies the currency of the cardholder billing amount in DE 6 (Amount, Cardholder Billing), ICCR amount in DE 8 (Amount, ICCR), and the Currency Conversion Assessment amount in DE 111 (Amount, Currency Conversion Assessment).
52	Personal Identification Number (PIN) Data	C	P	C	Used to contain encrypted PIN information. Required for Maestro, Cirrus, and ATM Gateway transactions. Not present for debit MasterCard POS transactions.
54	Additional Amounts	C	P	C	If used may contain cash back amount.
55	Integrated Circuit Card (ICC) System-Related Data	C	P	C	Must be present in ICC or proximity M/Chip full grade transactions (refer to the M/Chip Functional Architecture document for additional information).
58	Authorizing Agent Institution ID	•	X	C	Provided by the MDS for members using the enhanced issuer identification (EII) service Contains the issuing processor's financial institution routing and transit number.
61	POS Data	M	P	M	Describes the conditions present at the point-of-service at the time the originator initiates the transaction.
62	INF Data	O	P	C	If used, may contain INF network information for use in any future on-line retrieval request, chargeback transaction, or both. When present in a request message, the destination must return it in the subsequent response message.
63	Network Data	•	X	M	Provided by the MDS. Contains the financial network code and the switch serial number for the transaction. For debit MasterCard transactions, the Banknet reference number is also included.
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service. Contains the issuer processor number.
110	Additional Data - 2	C	X	C	Contains a variety of subelements depending on the card and purpose of the request. Refer to the detailed description in chapter 4.

Oct 2005

Data Element ID and Name		Org	Sys	Dst	Comments	
111	Amount, Currency Conversion Assessment	•	X	C	Contains the amount reflecting the Currency Conversion Assessment adjustment. This amount is expressed in DE 51 (Currency, Cardholder Billing). When present in the message, this amount is reflected in DE 5 (Amount, Settlement).	Oct 2005
112	Additional Data (National Use)	C	P	C	Reserved for national organizations to define data unique to specific networks or specific programs and services.	Oct 2005
120	Record Data	C	P	C	May contain billing address data for debit MasterCard Address Verification Service (AVS) request.	
124	Member-defined Data	O	P	O	The MDS enables processors to pass data to each other in this data element.	
126	Switch Private Data	•	X	M	Will contain settlement service and cross border indicators, along with MDS symbolic network information.	Oct 2005
127	Private Data	O	X	•	Available for private use by the message originator. The data does not pass through the MDS. The MDS returns this data to the request/advice message originator (with contents intact) in any subsequent response message.	

[a] The processor may elect to receive batch settlement in one of the MasterCard supported settlement currencies, and receive DE 5 (Amount, Settlement) and DE 50 (Currency Code, Settlement) reflected in US dollars.

Financial Transaction Request Response/0210

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	P	M	Value must be 0210.
-	Bit Map, Primary	M	P	M	Mandatory for all messages.
1	Bit, Map Secondary	C	P	C	Required only if any of DE 65 through DE 128 are present in the message.
2	Primary Account Number(PAN)	M	P	M	Must contain the same value from the original request message.
3	Processing Code	M	P	M	May contain the same value from the original request message. Refer to detailed description in chapter 4.
4	Amount, Transaction	M	P	M	Must contain the same value from the original request message.
5	Amount, Settlement	C	P	C	**Issuer 0210 message:** Must contain the same value from the original request (if present) **and** the destination approved the transaction. **Acquirer 0210 message:** MDS provided data element. DE 4 (Amount, Transaction) converted to the acquirer's DE 50 (Currency, Settlement).
7	Transmission Date and Time	M	X	M	With limited exceptions, contains the same value from the original request message.
9	Conversion Rate, Settlement	C	P	C	**Issuer 0210 message:** Must contain the same value from the original request (if present) **and** the destination approved the transaction. **Acquirer 0210 message:** MDS provided data element. The factor used in the conversion from DE 4 (Amount, Transaction) to DE 5 (Amount, Settlement).
11	System Trace Audit Number	M	P	M	Must contain the same value from the original request message.
12	Time, Local Transaction	M	P	M	Must contain the same value from the original request message.
13	Date, Local Transaction	M	P	M	Must contain the same value from the original request message.
15	Date, Settlement	M	P	M	Must contain the same value from the original request message.

Data Element ID and Name		Org	Sys	Dst	Comments
16	Date, Conversion	C	P	C	Must contain the same value from the original request (if present) **and** the destination approved the transaction. Required if DE 5, DE 9, or DE 50 are present in the 0210 message.
20	Primary Account Number (PAN) Country Code	O	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
28	Amount, Transaction Fee	C	P	C	Must contain the same value from the original request message.
32	Acquiring Institution Identification Code	M	P	M	Must contain the same value from the original request message.
33	Forwarding Institution Identification Code	M	P	M	Must contain the same value from the original request message.
37	Retrieval Reference Number	C	P	C	Must contain the same value from the original request message (if present).
38	Authorization Identification Response	C	P	C	May contain an Authorization ID code generated by an IPS.
39	Response Code	M	P	M	Response Code for this message.
41	Card Acceptor Terminal	M	P	M	Must contain the same value from the original request message.
44	Additional Response Data	C	X	C	Refer to detailed description in chapter 4.
48	Additional Data	C	P	C	Some subelements are returned with the same value as in original request message. Refer to detailed description in chapter 4.
49	Currency Code, Transaction	M	P	M	Must contain the same value from the original request message.
50	Currency Code, Settlement	C	P	C	**Issuer 0210 message:** Contains the currency code for issuer settlement in DE 5 (Amount, Settlement). Must contain the same value from the original request (if present) **and** the destination approved the transaction. **Acquirer 0210 message:** MDS provided data element. Contains the currency code for the acquirer settlement in DE 5.
54	Additional Amounts	C	P	C	May contain balance inquiry and account information for Maestro and Cirrus transactions.

Data Element ID and Name		Org	Sys	Dst	Comments	
55	Integrated Circuit Card (ICC) System-related Data	C	P	C	Present if the Integrated Circuit Card (ICC) System-related Data was included in the original 0200 request and issuer data is to be returned to the ICC (otherwise not present). May be present for Chip Card transactions and must **not** contain the same value from the original request message.	
62	INF Data	C	P	C	Must contain the same value from the original request message (if present).	
63	Network Data	M	P	M	Must contain the same value (provided by the MDS) in the original request message. This value must be retained throughout the life cycle of the transaction.	Oct 2005
100	Receiving Institution Identification Code	C	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service. Must contain the same value from the original request message (if present).	
102	Account Identification-1	C	P	C	May contain the actual "FROM" account number.	
103	Account Identification-2	C	P	C	May contain the actual "TO" account number.	
112	Additional Data (National Use)	C	P	C	Reserved for national organizations to define data unique to specific networks or specific programs and services.	Oct 2005
120	Record Data	C	P	C	Must contain the same value from the original request message.	
124	Member-Defined Data	O	P	O	The MDS enables processors to pass data to each other in this data element.	
126	Switch Private Data	C	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service or cross border indicators. Must contain the same value from the original request message.	Oct 2005
127	Private Data	O	X	C	Available for private use by the message originator. The data does not pass through the MDS. The MDS returns this data to the request/advice message originator (with contents intact) in any subsequent response message.	

Financial Transaction Advice/0220

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	P	M	Value must be 0220.
-	Bit Map, Primary	M	P	M	Mandatory for all messages.
1	Bit Map, Secondary	C	P	C	Required only if any of DE 65 through DE 128 are present in the message.
2	Primary Account Number (PAN)	M	P	M	Must contain the same value from the original (PAN) request message.
3	Processing Code	M	P	M	Must contain the same value from the original request message.
4	Amount, Transaction	M	P	M	Must contain the same value from the original request message.
5	Amount, Settlement	C	P	C	**Issuer 0220 message:** Must contain the same value from the original request message (if present). **Acquirer 0220 message:** Must contain the same value from the 0210 message.
6	Amount, Cardholder Billing	•	X	M	Contains the same value as the original request.
7	Transmission Date and Time	M	X	M	Date and time, in Universal Time (UTC) that the originator initiates the message. Upon receipt, the MDS updates this data element with its time stamp.
8	Amount, ICCR	•	X	C	Contains the amount reflecting the ICCR adjustment.
9	Conversion Rate, Settlement	C	P	C	**Issuer 0220 message:** Must contain the same value from the original settlement request message (if present). **Acquirer 0220 message:** Must contain the same value from the 0210 message.
10	Conversion Rate, Cardholder Billing	•	X	M	Contains the same value from the original request message.
11	System Trace Audit Number	M	P	M	Transaction trace number.
12	Time, Local Transaction	M	P	M	Must contain the same value from the original request message.
13	Date, Local Transaction	M	P	M	Must contain the same value from the original request message.

Data Element ID and Name		Org	Sys	Dst	Comments
14	Date, Expiration	C	P	C	Must contain the same value from the original request message (if present).
15	Date, Settlement	M	P	M	Must contain the same value from the original request message.
16	Date, Conversion	C	P	C	Must contain the same value from the original request message (if present).
18	Merchant Type (MCC)	M	P	C	Must be present on all transactions and reflect the business product or service provided.
22	Point-of-Service Entry Mode	M	P	M	Must contain the same value from the original request message.
23	Card Sequence Number	C	P	C	Present only for ICC Full Grade transactions, where DE 55 was included in the original 0200 message. If so, DE 55 will carry the same information as in the original 0200 message.
26	Point-of-Service PIN Capture Code	C	P	C	Must contain the same value from the original request message (if present).
28	Amount, Transaction Fee	C	P	C	Must contain the same value from the original message (if present).
32	Acquiring Institution Identification Code	M	P	M	Must contain the same value from the original request message.
33	Forwarding Institution Identification Code	M	P	M	Must contain the same value from the original request message (if present).
35	Track 2 Data	C	P	C	DE 35 will be present in the issuer bound 0220 message for: • Maestro "MS" preauthorization completion 0220 messages. • "Chip Clearing" 0220 messages, if present in the 0220 message from the acquirer.
37	Retrieval Reference Number	C	P	C	Must contain the same value from the original request message (if present).
38	Authorization Identification Response	C	P	C	Must contain the same value from the original response message (if present).
39	Response Code	M	P	M	Must contain the same value from the original response message.
41	Card Acceptor Terminal Identification	M	P	M	Must contain the same value from the original request message.
42	Card Acceptor Identification Code	C	P	C	Must contain a merchant name for ATM/POS and debit MasterCard POS transactions.

Data Element ID and Name		Org	Sys	Dst	Comments
43	Card Acceptor Name and Location	M	P	M	Must contain the same value from the original request message.
44	Additional Response Data	C	X	C	Indicates the data element where the field edit error occurred.
48	Additional Data	•	X	C	Conditionally required, based on individual program or service agreement between the MDS and the issuer. The MDS sends subelement 71 and subelement 72 in MDS Stand-In Advice 0220 messages, if the issuer participates in On-behalf Service 02 or 03. Refer to chapter 4 for additional information.
49	Currency Code, Transaction	M	P	M	Must contain the same value from the original request message.
50	Currency Code, Settlement	C	P	C	**Issuer 0220 message:** Must contain the same value from the original settlement request message (if present). **Acquirer 0220 message:** Must contain the same value from the 0210 message.
51	Currency Code, Cardholder Billing	•	X	M	Identifies the currency of the cardholder billing amount in DE 6 (Amount, Cardholder Billing).
54	Additional Amounts	C	P	C	May contain cash back amount.
55	Integrated Circuit Card (ICC) System-Related Data	C	P	C	Present only for ICC or proximity M/Chip Full Grade transactions, where DE 55 was included in the original 0200 message. If so, DE 55 will carry the same information as in the original 0200 message.
58	Authorizing Agent Institution ID	•	X	C	Provided by the MDS for members who participate in the enhanced issuer identification (EII) service. Contains the issuing processor's financial institution routing and transit number.
60	Advice Reason Code	M	P	M	The Advice Reason Code (ARC) indicates the specific purpose of this advice message.
61	POS Data	C	P	C	Must contain the same value from the original request message, except for debit MasterCard force post messages.
62	INF Data	C	P	C	Must contain the same value from the original request message (if present).
63	Network Data	M	P	M	Must contain the same value from the original response message.

Data Element ID and Name		Org	Sys	Dst	Comments
90	Original Data Elements	M	P	M	Mandatory for all MDS 0220 Advices. The system uses subfields within this data element to identify the original referenced transaction.
95	Replacement Amounts				Required for partial completions only.
	Subfield				
	1 Actual Amount, Transaction	C	P	C	Actual completion or adjusted amount.
	2 Actual Amount, Settlement	•	X	C	Actual Settlement Amount in the issuer's settlement currency.
	3 Actual Amount, Cardholder Billing	•	X	C	Actual cardholder billing amount in the cardholder billing currency.
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
102	Account Identification-1	C	P	C	Must contain the same value from the original response message (if present).
103	Account Identification-2	C	P	C	Must contain the same value from the original response message (if present).
110	Additional Data - 2	C	X	C	Contains a variety of subelements depending on the card and purpose of the request. Refer to the detailed description in chapter 4.
111	Amount, Currency Conversion Assessment	•	X	C	Contains the amount reflecting the Currency Conversion Assessment adjustment. Oct 2005
112	Additional Data	C	P	C	Reserved for national organizations to define data unique to specific networks or specific programs and services.
124	Member-Defined Data	O	P	O	The MDS enables processors to pass data to each other in this data element.
126	Switch Private Data	C	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service, cross border, or currency conversion. Oct 2005 Must contain the same value from the original request message.
127	Private Data	O	X	•	Available for private use by the message originator. The data does not pass through the MDS. The MDS returns this data to the request/advice message originator (with contents intact) in any subsequent response message.

Financial Transaction Advice Response/0230

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	P	M	Value must be 0230.
-	Bit Map, Primary	M	P	M	Mandatory for all messages.
1	Bit Map, Secondary	C	P	C	Required only if any data elements in the range DE 65 through DE 128 are present.
2	Primary Account Number (PAN)	M	P	M	Must contain the same value from the original advice message.
3	Processing Code	M	P	M	Must contain the same value from the original advice message.
4	Amount, Transaction	M	P	M	Must contain the same value from the original advice message.
5	Amount, Settlement	C	P	C	Must contain the same value from the original advice message (if present).
7	Transmission Date and Time	M	X	M	With limited exceptions, will contain the same value from the original advice message.
9	Conversion Rate, Settlement	C	P	C	Must contain the same value from the original advice message (if present).
11	System Trace Audit Number	M	P	M	Must contain the same value from the original advice message.
12	Time, Local Transaction	M	P	M	Must contain the same value from the original advice message.
13	Date, Local Transaction	M	P	M	Must contain the same value from the original advice message.
15	Date, Settlement	M	P	M	Must contain the same value from the original advice message.
16	Date, Conversion	C	P	C	Must contain the same value from the original advice message (if present).
20	Primary Account Number (PAN) Country Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
28	Amount, Transaction Fee	C	P	C	Must contain the same value from the original request message (if present).
32	Acquiring Institution Identification Code	M	P	M	Must contain the same value from the original advice message.
33	Forwarding Institution Identification Code	M	P	M	Must contain the same value from the original advice message.

Data Element ID and Name		Org	Sys	Dst	Comments
37	Retrieval Reference Number	C	P	C	Must contain the same value from the original advice message (if present).
39	Response Code	M	P	M	Response code for this message.
41	Card Acceptor Terminal Identification	M	P	M	Must contain the same value from the original advice message.
44	Additional Response Data	C	X	C	Indicates the data element where the field edit error occurred.
49	Currency Code, Transaction	M	P	M	Must contain the same value from the original advice message.
50	Currency Code, Settlement	C	P	C	Must contain the same value from the original advice message (if present).
54	Additional Amounts	C	P	C	May contain balance inquiry and account information for Maestro® and Cirrus® transactions.
62	INF Data	C	P	C	Must contain the same value from the original advice message (if present).
63	Network Data	M	P	M	Must contain the same value from the original advice message.
95	Replacement Amounts				Required if present in original advice message:
	Subfield				
	1 Actual Amount, Transaction	C	P	C	Actual completion or adjusted amount in local currency.
	2 Actual Amount, Settlement	•	X	C	**Acquirer 0230 message:** Actual Settlement Amount in the acquirer's settlement currency.
	3 Actual Amount, Cardholder Billing	•	X	C	Actual Cardholder Billing Amount in the cardholder billing currency.
100	Receiving Institution Identification Code	C	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
112	Additional Data	C	P	C	Reserved for national organizations to define data unique to specific networks or specific programs and services.

Oct 2005

Data Element ID and Name		Org	Sys	Dst	Comments
126	Switch Private Data	C	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service or cross border indicators. Must contain the same value from the original request message.
127	Private Data	O	X	C	Available for private use by the message originator. The data does not pass through the MDS. The MDS returns this data to the request/advice message originator (with contents intact) in any subsequent response message.

Oct 2005

Financial Transaction Negative Acknowledgment/0290

Note **The MDS can send the Financial Transaction Negative Acknowledgment/0290 Message to either the issuer or the acquirer.**

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value must be 0290.
-	Bit Map, Primary	•	X	M	Mandatory for all messages.
1	Bit Map, Secondary	•	X	C	Required if any data elements in the range DE 65 through DE 128 are present in the message.
7	Transmission Date and Time	•	X	M	Must contain the same value from the original response message.
11	System Trace Audit Number	•	X	M	Must contain the same value from the original response message.
32	Acquiring Institution Identification Code	•	X	M	Must contain the same value from the original response message.
33	Forwarding Institution Identification Code	•	X	M	Must contain the same value from the original response message.
39	Response Code	•	X	M	Response code for this message.
44	Additional Response Data	•	X	C	Used to indicate the data element location where the edit error or format error occurred.
63	Network Data	•	X	M	Must contain the same value from the original response message.
127	Private Data	•	X	C	Available for private use by the message originator. The data does not pass through the MDS.

File Update Request/0302

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI) [a]	M	P	M	Value must be 0302.
-	Bit Map, Primary	M	P	M	Mandatory.
1	Bit Map, Secondary	M	P	M	Mandatory.
2	Primary Account Number (PAN)	M	P	M	Contains the primary account number to be listed by the issuer.
7	Transmission Date and Time	M	P	M	The transmission date and time expressed in Universal Time (UT).
11	System Trace Audit Number	M	P	M	Transaction trace number that must have a unique value for each transaction initiator within each UT day.
33	Forwarding Institution Identification Code	M	P	M	Contains the MasterCard customer ID number that identifies the entity to which this file update action applies.
91	File Update Code	M	P	M	File function code that describes appropriate action: add, change, delete, or inquire.
96	Message Security Code	C	P	C	File update password or security code that can be required to enable the file update.
101	File Name	M	P	M	Name of the file to be updated. Refer to chapter 4 description of DE 101 for file names, descriptions, and permissible updates.
120	Record Data	M	P	M	Contains record location for file update action, and if file add/change, contains new/changed data. Refer to chapter 4, DE 120 for a detailed description.
127	Private Data	O	X	•	Available for private use by the message originator. The data does not pass through the MDS. The MDS returns this data to the request/advice message originator (with contents intact) in any subsequent response message.

[a] File update messages may originate from the issuer's online transaction processing system or the issuer's authorized representative via NICS™.

File Update Request Response/0312

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI) [a]	M	P	M	Value must be 0312.
-	Bit Map, Primary	M	P	M	Mandatory.
1	Bit Map, Secondary	M	P	M	Mandatory.
2	Primary Account Number (PAN)	M	P	M	Contains the primary account number to be listed by the issuer.
7	Transmission Date and Time	M	P	M	Must contain the same value from the original request message.
11	System Trace Audit Number	M	P	M	Must contain the same value from the original request message.
33	Forwarding Institution Identification Code	M	P	M	Must contain the same value from the original request message.
39	Response Code	M	P	M	Indicates whether the file update was successful. Refer to chapter 4 for a description of valid values for DE 39.
44	Additional Response Data	C	X	C	Provides additional information in the event of a format error. Refer to chapter 4 for a description of valid values for DE 44.
63	Network Data	M	P	M	Banknet reference number.
91	File Update Code	M	P	M	Must contain the same value from the original request message.
96	Message Security Code	C	P	C	Must contain the same value from the original request message.
101	File Name	M	P	M	Must contain the same value from the original request message.
120	Record Data	M	P	M	Must contain the same value from the original request message.
122	Additional Record Data	C	P	C	A free form field used to return additional data as a result of a file inquiry. Refer to chapter 4, DE 122 for a detailed record description and valid values.

Data Element ID and Name	Org	Sys	Dst	Comments
127 Private Data	O	X	C	Available for private use by the message originator. The data does not pass through the MDS. The MDS returns this data to the request/advice message originator (with contents intact) in any subsequent response message.

[a] File update response messages originate at the MasterCard Account Management System or, in the case of MDS Stand-In, from the MDS. The responses are ultimately returned to the issuer.

Acquirer Reversal Advice/0420—Acquirer Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	P	M	Value must be 0420. Type "A" format: Generated by APS only.
-	Bit Map, Primary	M	P	M	Mandatory.
1	Bit Map, Secondary	M	P	M	Mandatory.
2	Primary Account Number (PAN)	M	P	M	Must contain the same value from the original financial message.
3	Processing Code	M	P	M	Must contain the same value from the original financial message.
4	Amount, Transaction	M	P	M	Must contain the same value from the original financial message.
5	Amount, Settlement	•	X	C	Must contain the same value from the original financial message (if present).
6	Amount, Cardholder Billing	•	X	M	Contains the same value from the original financial message.
7	Transmission Date and Time	M	X	M	Date and time, in Universal Time (UTC) that the originator initiates the message. Upon receipt, the MDS updates this data element with its time stamp.
8	Amount, ICCR	•	X	C	Contains the amount reflecting the ICCR adjustment.
9	Conversion Rate, Settlement	•	X	C	Required if DE 5 is present. If present, Must contain the same value from the original financial message.
10	Conversion Rate, Cardholder Billing	•	X	M	Contains the same value from the original financial message.
11	System Trace Audit Number	M	P	M	Must contain the same value as the original message.
12	Time, Local Transaction	M	P	M	Must contain the same value from the original financial message.
13	Date, Local Transaction	M	P	M	Must contain the same value from the original financial message.
15	Date, Settlement	M	X	M	Contains the settlement date of this transaction from original message, if available.

Data Element ID and Name		Org	Sys	Dst	Comments
16	Date, Conversion	•	X	C	Required if DE 5 is present. If present, Must contain the same value from the original financial message.
28	Amount, Transaction Fee	C	P	C	Must contain the same value from the original financial message (if present).
32	Acquiring Institution Identification Code	M	P	M	Must contain the same value from the original financial message.
33	Forwarding Institution Identification Code	M	P	M	Must contain the same value from the original financial message.
37	Retrieval Reference Number	C	P	C	Must contain the same value from the original financial message (if present).
38	Authorization ID Response	C	P	C	From original response, if available.
39	Response Code	M	P	M	Must contain the same value from the original transaction response message.
41	Card Acceptor Terminal Identification	M	P	M	Must contain the same value from the original financial message.
49	Currency Code, Transaction	M	P	M	Must contain the same value from the original financial message.
50	Currency Code, Settlement	•	X	C	Required if present in the message. If present, Must contain the same value from the original financial message.
51	Currency Code, Cardholder Billing	•	X	M	Identifies the currency of the cardholder billing amount in DE 6.
54	Additional Amounts	C	P	C	Must be present if contained in the original cash back transaction.
58	Authorizing Agent Institution ID	•	X	C	Provided by the MDS for members using the enhanced issuer identification (EII) service Contains the issuing processor's financial institution routing and transit number.
60	Advice Reason Code	M	P	M	Indicates the specific reason for this Reversal message. The system uses the three-digit Advice Reason Code and four-digit MDS Advice Detail Code.
62	INF Data	C	P	C	Must contain the same value from the original financial message (if present).
63	Network Data	M	P	M	Must contain the same value from the original transaction response message.

Data Element ID and Name		Org	Sys	Dst	Comments
90	Original Data Elements	M	P	M	Mandatory for all Acquirer Reversal Advice/0420 reversals. The system uses the subfields within this data element to identify the original reversed transaction.
95	Replacement Amounts	M	X	M	Actual amount of the transaction. Contains all zeroes for full reversals.
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
111	Amount, Currency Conversion Assessment	•	X	C	Contains the amount reflecting the Currency Conversion Assessment adjustment. Oct 2005
126	Switch Private Data	C	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service or cross border indicators. Oct 2005 Must contain the same value from the original financial message.
127	Private Data	O	X	•	Available for private use by the message originator. Does not pass through the MDS.

Acquirer Reversal Advice/0420—Timeout-induced, Acquirer Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	P	M	Value must be 0420. Type "A" format: Generated by APS only.
-	Bit Map, Primary	M	P	M	Mandatory.
1	Bit Map, Secondary	M	P	M	Mandatory.
2	Primary Account Number (PAN)	M	P	M	Must contain the same value from the original request message.
3	Processing Code	M	P	M	Must contain the same value from the original request message.
4	Amount, Transaction	M	P	M	Must contain the same value from the original request message.
5	Amount, Settlement	•	X	C	The MDS supplies currency conversion data, if required.
6	Amount, Cardholder Billing	•	X	M	Contains the same value from the original request message.
7	Transmission Date and Time	M	X	M	Date and time, in Universal Time (UTC) that the originator initiates the message. Upon receipt, the MDS updates this data element with its time stamp.
8	Amount, ICCR	•	X	C	Contains the amount reflecting the ICCR adjustment.
9	Conversion Rate, Settlement	•	X	C	Required if DE 5 is present.
10	Conversion Rate, Cardholder Billing	•	X	M	Contains the same value from the original request message.
11	System Trace Audit Number	M	P	M	Must contain the same value as the original request message.
12	Time, Local Transaction	M	P	M	Must contain the same value from the original request message.
13	Date, Local Transaction	M	P	M	Must contain the same value from the original request message.
15	Date, Settlement	•	X	M	Provided by MDS in the message to the issuer.
16	Date, Conversion	•	X	C	Required if DE 5 is present.

Data Element ID and Name		Org	Sys	Dst	Comments
28	Amount, Transaction Fee	C	P	C	Must contain the same value from the original request message (if present).
32	Acquiring Institution Identification Code	M	P	M	Must contain the same value from the original request message.
33	Forwarding Institution Identification Code	M	P	M	Must contain the same value from the original request message.
37	Retrieval Reference Number	C	P	C	Must contain the same value from the original request message (if present).
38	Authorization ID Response	C	P	C	From original response, if available.
39	Response Code	M	P	M	Contains the code 00 for the Timeout-Induced Reversal message.
41	Card Acceptor Terminal Identification	M	P	M	Must contain the same value from the original request message.
49	Currency Code, Transaction	M	P	M	Must contain the same value from the original request message.
50	Currency Code, Settlement	•	X	C	Required if DE 5 is present.
51	Currency Code, Cardholder Billing	•	X	M	Identifies the currency of the cardholder billing amount in DE 6.
54	Additional Amounts	C	P	C	Must be present if contained in the original cash back transaction.
58	Authorizing Agent Institution ID	•	X	C	Provided by the MDS for members using the enhanced issuer identification (EII) service. Contains the issuing processor's financial institution routing and transit number.
60	Advice Reason Code	M	P	M	Has the value 4500018 for the Timeout-Induced Reversal message.
62	INF Data	C	P	C	Must contain the same value from the original request message (if present).
63	Network Data	•	X	M	Provided by the MDS in the message to the issuer.
90	Original Data Elements	M	P	M	Mandatory for all Acquirer Reversal Advice/0420 reversals. The system uses the subfields within this data element to identify the original reversed transaction.
95	Replacement Amounts	M	X	M	Contains all zeroes for the Timeout-Induced Reversal message.
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.

Data Element ID and Name		Org	Sys	Dst	Comments	
111	Amount, Currency Conversion Assessment	•	X	C	Contains the amount reflecting the Currency Conversion Assessment adjustment.	Oct 2005
126	Switch Private Data	C	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service or cross border indicators. Must contain the same value from the original request message.	Oct 2005
127	Private Data	O	X	•	Available for private use by the message originator. Does not pass through the MDS.	

Acquirer Reversal Advice/0420—Timeout-Induced, System Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value must be 0420. Type "S" format: Generated by the MDS only.
-	Bit Map, Primary	•	X	M	Mandatory.
1	Bit Map, Secondary	•	X	M	Mandatory.
2	Primary Account Number (PAN)	•	X	M	Must contain the same value from the original request message.
3	Processing Code	•	X	M	Must contain the same value from the original request message.
4	Amount, Transaction	•	X	M	Must contain the same value from the original request message.
5	Amount, Settlement	•	X	C	The MDS supplies currency conversion data, if required..
6	Amount, Cardholder Billing	•	X	M	Contains the same value from the original request message.
7	Transmission Date and Time	•	X	M	Date and time, in Universal Time (UTC) that the originator initiates the message. Upon receipt, the MDS updates this data element with its time stamp.
8	Amount, ICCR	•	X	C	Contains the amount reflecting the ICCR adjustment.
9	Conversion Rate, Settlement	•	X	C	Required if DE 5 is present.
10	Conversion Rate, Cardholder Billing	•	X	M	Contains the same value from the original request message.
11	System Trace Audit Number	•	X	M	Must contain the same value as the original request message.
12	Time, Local Transaction	•	X	M	Must contain the same value from the original request message.
13	Date, Local Transaction	•	X	M	Must contain the same value from the original request message.
15	Date, Settlement	•	X	M	Provided by MDS in the message to the issuer.
16	Date, Conversion	•	X	C	Required if DE 5 is present.

Data Element ID and Name		Org	Sys	Dst	Comments
28	Amount, Transaction Fee	•	X	C	Must contain the same value from the original request message (if present).
32	Acquiring Institution Identification Code	•	X	M	Must contain the same value from the original request message.
33	Forwarding Institution Identification Code	•	X	M	Must contain the same value from the original request message.
37	Retrieval Reference Number	•	X	C	Must contain the same value from the original request message (if present).
38	Authorization ID Response	•	X	C	From original response, if available.
39	Response Code	•	X	M	Contains the code 00 for the Timeout-Induced Reversal message.
41	Card Acceptor Terminal Identification	•	X	M	Must contain the same value from the original request message.
49	Currency Code, Transaction	•	X	M	Must contain the same value from the original request message.
50	Currency Code, Settlement	•	X	C	Required if DE 5 is present.
51	Currency Code, Cardholder Billing	•	X	M	Identifies the currency of the cardholder billing amount in DE 6.
54	Additional Amounts	•	X	C	Must be present if contained in the original cash back transaction.
58	Authorizing Agent Institution ID	•	X	C	Provided by the MDS for members using the enhanced issuer identification (EII) service Contains the issuing processor's financial institution routing and transit number.
60	Advice Reason Code	•	X	M	Has the value 4010080 for the Timeout-Induced Reversal message.
62	INF Data	•	X	C	Must contain the same value from the original request message (if present).
63	Network Data	•	X	M	Provided by the MDS in the message to the issuer.
90	Original Data Elements	•	X	M	Mandatory for all Acquirer Reversal Advice/0420 reversals. The system uses the subfields within this data element to identify the original reversed transaction.
95	Replacement Amounts	•	X	M	Contains all zeroes for the Timeout-Induced Reversal message.

Data Element ID and Name		Org	Sys	Dst	Comments
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
111	Amount, Currency Conversion Assessment	•	X	C	Contains the amount reflecting the Currency Conversion Assessment adjustment.
126	Switch Private Data	•	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service or cross border indicators. Must contain the same value from the original request message.
127	Private Data	•	X	•	Available for private use by the message originator. Does not pass through the MDS.

Oct 2005

Oct 2005

Acquirer Reversal Advice/0420—NICS Exception, System Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value must be 0420. Type "S" format: generated by MDS only.
-	Bit Map, Primary	•	X	M	Mandatory.
1	Bit Map, Secondary	•	X	M	Mandatory.
2	Primary Account Number (PAN)	•	X	M	Must contain the same value from the original financial message[a].
3	Processing Code	•	X	M	Must contain the same value from the original financial message [a].
4	Amount, Transaction	•	X	M	Must contain the same value from the original financial message [a].
5	Amount, Settlement	•	X	C	MDS supplies currency conversion data, if required [b].
6	Amount, Cardholder Billing	•	X	M	MDS recalculates the original cardholder billing amount using the conversion rate in effect on the adjustment processing data [b].
7	Transmission Date and Time	•	X	M	The system initiates the date and time, in UTC format of this message.
8	Amount, ICCR	•	X	C	Contains the amount reflecting the ICCR adjustment.
9	Conversion Rate, Settlement	•	X	C	Required if DE 5 is present [b].
10	Conversion Rate, Cardholder Billing	•	X	M	Factor used in the conversion from transaction to cardholder billing amount [b].
11	System Trace Audit Number	•	X	M	Transaction trace number. The contents of this data element must be unique for each transaction initiated by a message originator on any single UTC date [a.]
12	Time, Local Transaction	•	X	M	Must contain the same value from the original financial message [a.]
13	Date, Local Transaction	•	X	M	Must contain the same value from the original financial message [a.]
15	Date, Settlement	•	X	M	Contains the settlement date of this transaction.
16	Date, Conversion	•	X	C	Required if DE 5 is present.

Data Element ID and Name		Org	Sys	Dst	Comments
32	Acquiring Institution Identification Code	•	X	M	Must contain the same value from the original financial message [a].
33	Forwarding Institution Identification Code	•	X	M	Must contain the same value from the original financial message [a].
37	Retrieval Reference Number	•	X	C	Must contain the same value from the original financial message, if present [a].
39	Response Code	•	X	M	Must contain the same value from the original financial message [a].
41	Card Acceptor Terminal Identification	•	X	M	Must contain the terminal ID to which this transaction applies [a].
49	Currency Code, Transaction	•	X	M	Must contain the same value from the original financial message [a].
50	Currency Code, Settlement	•	X	C	Required if present in the message [a].
51	Currency Code, Cardholder Billing	•	X	M	Identifies the currency of the cardholder billing amount in DE 6 (Amount, Cardholder Billing), DE 8 (Amount, ICCR), and DE 111 (Amount, Currency Conversion Assessment) [a]. Oct 2005
58	Authorizing Agent Institution ID	•	X	C	Provided by the MDS for members using the enhanced issuer identification (EII) service Contains the issuing processor's financial institution routing and transit number.
60	Advice Reason Code	•	X	M	Indicates the specific reason for this reversal message. The system uses the 3-digit Advice Reason Code and 4-digit MDS Advice Detail Code.
62	INF Data	•	X	C	Must contain the same value from the original financial message, if present [a].
63	Network Data	•	X	M	Must contain the same value from the original transaction response message [a].
90	Original Data Elements	•	X	M	Mandatory for all Acquirer Reversal Advice/0420 reversals. The system uses subfields within this data element to identify the original reversed transaction [a].
95	Replacement Amounts	•	X	M	Mandatory for all MDS 0420 Reversals [a].
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
111	Amount, Currency Conversion Assessment	•	X	C	Contains the amount reflecting the Currency Conversion Assessment adjustment. Oct 2005

Data Element ID and Name		Org	Sys	Dst	Comments
126	Switch Private Data	•	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service or cross border indicators. Must contain the same value from the original financial message.
127	Private Data	•	X	C	Available for private use by the message originator. Does not pass through the MDS [a].

Oct 2005

a The system populates this DE data (from the previous message).

b The MDS applies the conversion rate in effect for the date the adjustment is processed. The exchange rate applied to the adjustment may vary from the one applied to the original transaction.

Acquirer Reversal Advice/0420—Acquirer Initiated Exception

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	P	M	Value must be 0420.
-	Bit Map, Primary	M	P	M	Mandatory.
1	Bit Map, Secondary	M	P	M	Mandatory.
2	Primary Account Number (PAN)	M	P	M	Must contain the same value from the original financial message.
3	Processing Code	O	X	M	Must contain the same value from the original financial message.
4	Amount, Transaction	O	X	M	Must contain the same value from the original financial message.
5	Amount, Settlement	•	X	C	MDS supplies currency conversion data, if required [b].
6	Amount, Cardholder Billing	•	X	M	MDS recalculates the original cardholder billing amount using the conversion rate in effect on the adjustment processing date [b].
7	Transmission Date and Time	M	X	M	Date and time, in Universal Time (UTC) that the originator initiates the message. Upon receipt, the MDS updates this data element with its time stamp.
8	Amount, ICCR	•	X	C	Contains the amount reflecting the ICCR adjustment [b].
9	Conversion Rate, Settlement	•	X	C	Present if DE 5 is present [b].
10	Conversion Rate, Cardholder Billing	•	X	M	Factor used in the conversion from transaction to cardholder billing amount [b].
11	System Trace Audit Number	M	P	M	Transaction trace number. The contents of this data element must be unique for each transaction initiated by a message originator on any single UTC date [a].
12	Time, Local Transaction	O	X	M	Will contain the same value from the original financial message.
13	Date, Local Transaction	O	X	M	Will contain the same value from the original financial message.
15	Date, Settlement	M	X	M	Contains the settlement date of this transaction. From original message, if available.

Data Element ID and Name		Org	Sys	Dst	Comments
16	Date, Conversion	•	X	C	Present if DE 5 is present [a].
32	Acquiring Institution Identification Code	O	X	M	Must contain the same value from the original financial message.
33	Forwarding Institution Identification Code	M	P	M	Must contain the same value from the original financial message.
37	Retrieval Reference Number	O	X	C	Must contain the same value from the original financial message (if present).
39	Response Code	•	X	M	Will contain the same value from the original transaction response message.
41	Card Acceptor Terminal Identification	O	X	M	Must contain the same value from the original financial message.
49	Currency Code, Transaction	•	X	M	Will contain the same value from the original financial message.
50	Currency Code, Settlement	•	X	C	Required if present in the message. If present, must contain the same value from the original financial message.
51	Currency Code, Cardholder Billing	•	X	M	Identifies the currency of the cardholder billing amount in DE 6 (Amount, Cardholder Billing), DE 8 (Amount, ICCR), and DE 111 (Amount, Currency Conversion Assessment) [a].
58	Authorizing Agent Institution ID	•	X	C	Provided by the MDS for members using the enhanced issuer identification (EII) service Contains the issuing processor's financial institution routing and transit number.
60	Advice Reason Code	M	P	M	Indicates the specific reason for this Reversal message. The system uses the three-digit Advice Reason Code and four-digit MDS Advice Detail Code.
62	INF Data	O	X	C	Must contain the same value from the original financial message (if present).
63	Network Data	M	P	M	Must contain the same value from the original transaction response message.

Oct 2005

Data Element ID and Name		Org	Sys	Dst	Comments
90	Original Data Elements	O	X	M	Mandatory for all Acquirer Reversal Advice/0420 reversals. The system uses the subfields within this data element to identify the original reversed transaction.
95	Replacement Amounts	M	P	M	Contains all zeroes for acquirer generated full reversals.
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
111	Amount, Currency Conversion Assessment	•	X	C	Contains the amount reflecting the Currency Conversion Assessment adjustment [b]. Oct 2005
126	Switch Private Data	C	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service or cross border indicators. Oct 2005 Must contain the same value from the original financial message.
127	Private Data	O	X	•	Available for private use by the message originator. Does not pass through the MDS.

[a] The system populates this DE data (from the previous message).

[b] The MDS applies the conversion rate in effect for the date the adjustment is processed. The exchange rate applied to the adjustment may vary from the one applied to the original transaction.

Issuer Reversal Advice/0422—NICS Exception, System Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value Must be 0422. Type "S" format: generated by MDS only.
-	Bit Map, Primary	•	X	M	Mandatory.
1	Bit Map, Secondary	•	X	M	Mandatory.
2	Primary Account Number (PAN)	•	X	M	Must contain the same value from the original financial message [a].
3	Processing Code	•	X	M	Must contain the same value from the original financial message [a].
4	Amount, Transaction	•	X	M	Must contain the same value from the original financial message [a].
5	Amount, Settlement	•	X	C	The MDS supplies currency conversion data, if required [b].
6	Amount, Cardholder Billing	•	X	C	MDS recalculates the original cardholder billing amount using the conversion rate in effect on the adjustment processing date [b].
7	Transmission Date and Time	•	X	M	The system initiates the date and time in UTC format of this message.
9	Conversion Rate, Settlement	•	X	C	Required if DE 5 is present.[b]
10	Conversion Rate, Cardholder Billing	•	X	C	Factor used in the conversion from transaction to cardholder billing amount [b].
11	System Trace Audit Number	•	X	M	Transaction trace number. Contents of this data element must be unique for each transaction initiated by a message originator on any single UTC date.
12	Time, Local Transaction	•	X	M	Will contain the same value from the original financial message [a].
13	Date, Local Transaction	•	X	M	Must contain the same value from the original financial message [a].
15	Date, Settlement	•	X	M	Contains the settlement date of this transaction.
16	Date, Conversion	•	X	C	Required if DE 5 is present.
20	Primary Account Number (PAN) Country Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.

Data Element ID and Name		Org	Sys	Dst	Comments
32	Acquiring Institution Identification Code	•	X	M	Must contain the same value from the original financial message [a].
33	Forwarding Institution Identification Code	•	X	M	Must contain the same value from the original financial message [a].
37	Retrieval Reference Number	•	X	C	Must contain the same value from the original financial message, if present.
39	Response Code	•	X	M	Will contain the same value from the original transaction response message [a].
41	Card Acceptor Terminal Identification	•	X	M	Must contain the same value from the original financial message [a].
49	Currency Code, Transaction	•	X	M	Must contain the same value from the original financial message [a].
50	Currency Code, Settlement	•	X	C	Required if present in the message.
51	Currency Code, Cardholder Billing	•	X	C	Identifies the currency of the cardholder billing amount in DE 6 (Amount, Cardholder Billing), DE 8 (Amount, ICCR), and DE 111 (Amount, Currency Conversion Assessment).
58	Authorizing Agent Institution ID	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
60	Advice Reason Code	•	X	M	Indicates the specific reason for this reversal message. The system uses the 3-digit Advice Reason Code and 4-digit MDS Advice Detail Code.
62	INF Data	•	X	C	Must contain the same value from the original financial message, if present [a].
63	Network Data	•	X	M	Must contain the same value from the original transaction response message [a].
90	Original Data Elements	•	X	M	The system uses subfields within this data element to identify the original reversed transaction.
95	Replacement Amounts	•	X	M	
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.

Oct 2005

Data Element ID and Name		Org	Sys	Dst	Comments
126	Switch Private Data	•	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service or cross border indicators. Must contain the same value from the original financial message.
127	Private Data	•	X	C	Available for private use by the message originator. Does not pass through the MDS.

Oct 2005

a The system populates this DE data (from the previous message).

b The MDS applies the conversion rate in effect for the date the adjustment is processed. The exchange rate applied to the adjustment may vary from the one applied to the original transaction.

Issuer Reversal Advice/0422—Exception, Issuer Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	P	M	Value must be 0420.
-	Bit Map, Primary	M	P	M	Mandatory.
1	Bit Map, Secondary	M	P	M	Mandatory.
2	Primary Account Number (PAN)	M	P	M	Must contain the same value from the original financial message.
3	Processing Code	O	X	M	Must contain the same value from the original financial message.
4	Amount, Transaction	O	X	M	Must contain the same value from the original financial message.
5	Amount, Settlement	•	X	C	MDS supplies currency conversion data, if required [b].
6	Amount, Cardholder Billing	•	X	C	MDS recalculates the original cardholder billing amount using the conversion rate in effect on the adjustment processing date [b].
7	Transmission Date and Time	M	X	M	Date and time, in Universal Time (UTC) that the originator initiates the message. Upon receipt, the MDS updates this data element with its time stamp.
9	Conversion Rate, Settlement	•	X	C	Present if DE 5 is present [b].
10	Conversion Rate, Cardholder Billing	•	X	C	Factor used in the conversion from transaction to cardholder billing amount [b].
11	System Trace Audit Number	M	P	M	Transaction trace number. The contents of this data element must be unique for each transaction initiated by a message originator on any single UTC date [a].
12	Time, Local Transaction	O	X	M	Will contain the same value from the original financial message.
13	Date, Local Transaction	O	X	M	Will contain the same value from the original financial message.
15	Date, Settlement	M	X	M	Contains the settlement date of this transaction. From original message, if available.
16	Date, Conversion	•	X	C	Present if DE 5 is present [a].
20	Primary Account Number (PAN) Country Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.

Data Element ID and Name		Org	Sys	Dst	Comments
32	Acquiring Institution Identification Code	O	X	M	Must contain the same value from the original financial message.
33	Forwarding Institution Identification Code	M	P	M	Must contain the same value from the original financial message.
37	Retrieval Reference Number	O	X	C	Must contain the same value from the original financial message (if present).
39	Response Code	•	X	M	Will contain the same value from the original transaction response message.
41	Card Acceptor Terminal Identification	O	X	M	Must contain the same value from the original financial message.
49	Currency Code, Transaction	•	X	M	Will contain the same value from the original financial message.
50	Currency Code, Settlement	•	X	C	Required if present in the message. If present, must contain the same value from the original financial message.
51	Currency Code, Cardholder Billing	•	X	C	Will contain the same value from the original financial message, if present [a].
58	Authorizing Agent Institution ID	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
60	Advice Reason Code	M	P	M	Indicates the specific reason for this Reversal message. The system uses the three-digit Advice Reason Code and four-digit MDS Advice Detail Code.
62	INF Data	O	X	C	Must contain the same value from the original financial message (if present).
63	Network Data	M	P	M	Must contain the same value from the original transaction response message.
90	Original Data Elements	O	X	M	Mandatory for all Acquirer Reversal Advice/0420 reversals. The system uses the subfields within this data element to identify the original reversed transaction.
95	Replacement Amounts	M	P	M	Contains all zeros for acquirer generated full reversals.
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.

Data Element ID and Name		Org	Sys	Dst	Comments
126	Switch Private Data	C	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service or cross border indicators. Must contain the same value from the original financial message.
127	Private Data	O	X	•	Available for private use by the message originator. Does not pass through the MDS.

Oct 2005

a The system populates this DE data (from the previous message).

b The MDS applies the conversion rate in effect for the date the adjustment is processed. The exchange rate applied to the adjustment may vary from the one applied to the original transaction.

Acquirer Reversal Advice Response/0430—System Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value Must be 0430. (Response to acquirer-generated 0420 advice).
-	Bit Map, Primary	•	X	M	Mandatory.
1	Bit Map, Secondary	•	X	M	Mandatory.
2	Primary Account Number (PAN)	•	X	M	Must contain the same value from the original financial message.
3	Processing Code	•	X	M	Must contain the same value from the original financial message.
4	Amount, Transaction	•	X	M	Must contain the same value from the original financial message.
5	Amount, Settlement	•	X	C	Must contain the same value from the original financial message (if present).
6	Amount, Cardholder Billing	•	X	C	Contains the same value from the original financial message (if present).
7	Transmission Date and Time	•	X	M	With limited exceptions, will contain the same value from the original financial message.
9	Conversion Rate, Settlement	•	X	C	The MDS will provide currency conversion data, if required.
10	Conversion Rate, Cardholder Billing	•	X	C	Will contain the same value from the original financial message, if present [a].
11	System Trace Audit Number	•	X	M	Must contain the same value from the original financial message.
12	Time, Local Transaction	•	X	M	Must contain the same value from the original financial message.
13	Date, Local Transaction	•	X	M	Must contain the same value from the original financial message.
15	Date, Settlement	•	X	M	Must contain the same value from the original financial message.
16	Date, Conversion	•	X	C	Must contain the same value from the original financial message (if present).
20	Primary Account Number (PAN) Country Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.

Data Element ID and Name		Org	Sys	Dst	Comments
32	Acquiring Institution Identification Code	•	X	M	Must contain the same value from the original financial message.
33	Forwarding Institution Identification Code	•	X	M	Must contain the same value from the original financial message.
37	Retrieval Reference Number	•	X	C	Must contain the same value from the original financial message (if present).
39	Response Code	•	X	M	Response code for this message.
41	Card Acceptor Terminal ID	•	X	M	Must contain the same value from the original financial message.
44	Additional Response Data	•	X	C	Indicates the data element location where the field edit error occurred.
49	Currency Code, Transaction	•	X	M	Must contain the same value from the original financial message.
50	Currency Code, Settlement	•	X	C	Must contain the same value from the original financial message (if present).
51	Currency Code, Cardholder Billing	•	X	C	Will contain the same value from the original financial message, if present [a].
54	Additional Amounts	•	X	C	If used, may contain balance inquiry and account information for Maestro® and Cirrus® transactions.
62	INF Data	•	X	C	Must contain the same value from the original financial message (if present).
63	Network Data	•	X	M	Must contain the same value from the original financial message.
95	Replacement Amounts	•	X	M	Contains the same subelement values from the original message.
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
126	Switch Private Data	•	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor chooses to receive the settlement service or cross border indicators. Must contain the same value from the original financial message.
127	Private Data	•	X	C	Available for private use by the message originator. Does not pass through the MDS.

Oct 2005

Acquirer Reversal Advice Response/0430—Issuer Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	X	•	Value must be 0430.
-	Bit Map, Primary	M	X	•	Mandatory for all messages.
1	Bit Map, Secondary	M	X	•	Mandatory.
2	Primary Account Number (PAN)	M	X	•	Must contain the same value from the original financial message.
3	Processing Code	M	X	•	Must contain the same value from the original financial message.
4	Amount, Transaction	M	X	•	Must contain the same value from the original financial message.
5	Amount, Settlement	C	X	•	Must contain the same value from the original financial message, if present.
6	Amount, Cardholder Billing	C	X	•	Must contain the same value from the original financial message, if present.
7	Transmission Date and Time	M	X	•	Must contain the same value from the original financial message.
9	Conversion Rate Settlement,	O	X	•	The MDS provides currency conversion data, if required.
10	Conversion Rate, Cardholder Billing	C	X	•	Must contain the same value from the original financial message, if present.
11	System Trace Audit Number	M	X	•	Must contain the same value from the original financial message.
12	Time, Local Transaction	M	X	•	Must contain the same value from the original financial message.
13	Date, Local Transaction	M	X	•	Must contain the same value from the original financial message.
15	Date, Settlement	M	X	•	Must contain the same value from the original financial message.
16	Date, Conversion	C	X	•	Must contain the same value from the original financial message, if present.
20	Primary Account Number (PAN) Country Code	C	X	•	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
32	Acquiring Institution Identification Code	M	X	•	Must contain the same value from the original financial message.

Data Element ID and Name		Org	Sys	Dst	Comments
33	Forwarding Institution Identification Code	M	X	•	Must contain the same value from the original financial message.
37	Retrieval Reference Number	C	X	•	Must contain the same value from the original financial message, if present.
39	Response Code	M	X	•	Response code for this message.
41	Card Acceptor Terminal ID	M	X	•	Must contain the same value from the original financial message.
44	Additional Response Data	C	X	•	Indicates the data element location where the field edit error occurred.
49	Currency Code, Transaction	M	X	•	Must contain the same value from the original financial message.
50	Currency Code, Settlement	C	X	•	Must contain the same value from the original financial message, if present.
51	Currency Code, Cardholder Billing	C	X	•	Must contain the same value from the original financial message, if present.
62	INF Data	C	X	•	Must contain the same value from the original financial message, if present.
63	Network Data	M	X	•	Must contain the same value from the original financial message.
95	Replacement Amounts	M	X	•	Contains the same subelement values from the original message.
100	Receiving Institution Identification Code	C	X	•	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
126	Switch Private Data	C	X	•	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor chooses to receive the settlement service or cross border indicators. Must contain the same value from the original financial message.
127	Private Data	O	X	•	Available for private use by the message originator. Does not pass through the MDS.

Oct 2005

Issuer Reversal Advice Response/0432—Exception, Acquirer Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	X	•	Value must be 0432. (Response to MDS generated 0422 advice).
-	Bit Map, Primary	M	X	•	Mandatory.
1	Bit Map, Secondary	M	X	•	Mandatory.
2	Primary Account Number (PAN)	M	X	•	Must contain the same value from the original financial message.
3	Processing Code	M	X	•	Must contain the same value from the original financial message.
4	Amount, Transaction	M	X	•	Must contain the same value from the original financial message.
5	Amount, Settlement	C	X	•	Must contain the same value from the original 0422 message.
6	Amount, Cardholder Billing	C	X	•	Must contain the same value from the original 0422 message.
7	Transmission Date and Time	M	X	•	Must contain the same value from the original financial message.
9	Conversion Rate, Settlement	O	X	•	Must contain the same value from the original 0422 message.
10	Conversion Rate, Cardholder Billing	C	X	•	Must contain the same value from the original 0422 message.
11	System Trace Audit Number	M	X	•	Must contain the same value from the original financial message.
12	Time, Local Transaction	M	X	•	Must contain the same value from the original financial message.
13	Date, Local Transaction	M	X	•	Must contain the same value from the original financial message.
15	Date, Settlement	M	X	•	Must contain the same value from the original financial message.
16	Date, Conversion	C	X	•	Must contain the same value from the original 0422 message.
20	Primary Account Number (PAN) Country Code	C	X	•	Only present if the processor participates in Enhanced Issuer Identification (EII) service.

Data Element ID and Name		Org	Sys	Dst	Comments
32	Acquiring Institution Identification Code	M	X	•	Must contain the same value from the original financial message.
33	Forwarding Institution Identification Code	M	X	•	Must contain the same value from the original financial message.
37	Retrieval Reference Number	C	X	•	Must contain the same value from the original financial message (if present).
39	Response Code	M	X	•	Response code for this message.
41	Card Acceptor Terminal ID	M	X	•	Must contain the same value from the original financial message.
44	Additional Response Data	C	X	•	Indicates the data element location where the field edit error occurred.
49	Currency Code, Transaction	M	X	•	Must contain the same value from the original financial message.
50	Currency Code, Settlement	C	X	•	Must contain the same value from the original financial message, if present.
51	Currency Code, Cardholder Billing	C	X	•	Must contain the same value from the original financial message, if present.
62	INF Data	C	X	•	Must contain the same value from the original financial message, if present.
63	Network Data	M	X	•	Must contain the same value from the original financial message.
95	Replacement Amounts	M	X	•	Contains the same subelement values from the original message.
100	Receiving Institution Identification Code	C	X	•	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
126	Switch Private Data	C	X	•	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor chooses to receive the settlement service or cross border indicators. Must contain the same value from the original financial message.
127	Private Data	O	X	•	Available for private use by the message originator. Does not pass through the MDS.

Oct 2005

Issuer Reversal Advice Response/0432—Exception, System Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value must be 0432.
-	Bit Map, Primary	•	X	M	Mandatory.
1	Bit Map, Secondary	•	X	M	Mandatory.
2	Primary Account Number (PAN)	•	X	M	Must contain the same value from the original 0200 message.
3	Processing Code	•	X	M	Must contain the same value from the original 0200 message.
4	Amount, Transaction	•	X	M	Must contain the same value from the original 0200 message.
5	Amount, Settlement	•	X	C	MDS supplies currency conversion data, if required [b].
6	Amount, Cardholder Billing	•	X	C	MDS recalculates the original cardholder billing amount using the conversion rate in effect on the adjustment processing date [b].
7	Transmission Date and Time	•	X	M	Must contain the same value from the original financial message.
9	Conversion Rate, Settlement	•	X	C	Required if DE 5 is present [a].
10	Conversion Rate, Cardholder Billing	•	X	C	Factor used in the conversion from transaction to cardholder billing amount [b].
11	System Trace Audit Number	•	X	M	Must contain the same value from the online exception request.
12	Time, Local Transaction	•	X	M	Must contain the same value from the original financial message.
13	Date, Local Transaction	•	X	M	Must contain the same value from the original 0200 message.
15	Date, Settlement	•	X	M	Must contain the value from the exception request.
16	Date, Conversion	•	X	C	Required if DE 5 is present.
20	Primary Account Number (PAN) Country Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.
32	Acquiring Institution Identification Code	•	X	M	Must contain the same value from the original 0200 message.

Data Element ID and Name		Org	Sys	Dst	Comments
33	Forwarding Institution Identification Code	•	X	M	Must contain the same value from the original 0200 message.
37	Retrieval Reference Number	•	X	C	If DE 63 is not present, DE 37 from original transaction must be present.
39	Response Code	•	X	M	Status of the exception request.
41	Card Acceptor Terminal ID	•	X	M	Must contain the same value from the original 0200 message.
44	Additional Response Data	•	X	C	If exception request is denied, contain the denial reason in four-digit numeric format.
49	Currency Code, Transaction	•	X	M	Must contain the same value from the original 0200 message.
50	Currency Code, Settlement	•	X	C	Required if DE 5 is present.
51	Currency Code, Cardholder Billing	•	X	C	Must contain the same value from the original financial message, if present.
58	Authorizing Agent Institution ID	•	X	C	Provided by the MDS for members using the enhanced issuer identification (EII) service Contains the issuing processor's financial institution routing and transit number.
60	Advice Reason Code	•	X	M	Must contain the same value from the online exception request.
62	INF Data	•	X	C	Must contain the same value from the original 0200 message (if present).
63	Network Data	•	X	M	Must contain the same value from the original 0200 message.
90	Original Data Elements	•	X	M	Must contain the same value from the original 0200 message.
95	Replacement Amounts	•	X	M	Subfield 1 contains the actual completed amount in local currency (from the original exception request). Subfield 2 (provided by the MDS) contains the actual settlement amount. Subfield 3 (provided by the MDS) contains the actual cardholder billing amount, if applicable. Subfield 4 is zero filled.
100	Receiving Institution Identification Code	•	X	C	Only present if the processor participates in Enhanced Issuer Identification (EII) service.

Data Element ID and Name		Org	Sys	Dst	Comments
126	Switch Private Data	•	X	C	Conditionally required, based on individual program or service agreement between the MDS and the processor. Must be present if processor opts to receive the settlement service or cross border indicators. Must contain the same value from the original financial message.
127	Private Data	•	X	C	Available for private use by the message originator. Does not pass through the MDS.

Oct 2005

a The system populates this DE data (from the previous message).

b The MDS applies the conversion rate in effect for the date the adjustment is processed. The exchange rate applied to the adjustment may vary from the one applied to the original transaction.

Administrative Advice/0620—MDS Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value must be 0620.
-	Bit Map, Primary	•	X	M	Mandatory.
1	Bit Map, Secondary	•	X	M	Mandatory.
7	Transmission Date and Time	•	X	M	The system transmits the date and time, in UTC format, of this message.
11	System Trace Audit Number	•	X	M	Transaction trace number; must be unique value for transaction initiator within each UTC day.
33	Forwarding Institution Identification Code	•	X	M	Contains the processor ID of the CPS or NCID originating this message (The value will be 9000000000 for MDS-generated 0620 messages).
60	Advice Reason Code	•	X	M	Indicates the specific reason for this message. 600 = rejected message
63	Network Data	•	X	M	Provided by the MDS. Contains the MDS reference number for this transaction.
100	Receiving Institution Identification Code	•	X	M	Must contain the processor ID of the network destination for this message.
120	Record Data	•	X	C	If ARC = 600, this data element may be used to contain the original (rejected) message.

Administrative Advice/0620—Processor Initiated

Note **The MDS will not respond to an Administrative Advice/0620 Message with an Administrative Advice Response/0630 Message.**

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	X	•	Value must be 0620.
-	Bit Map, Primary	M	X	•	Mandatory.
1	Bit Map, Secondary	C	X	•	Mandatory.
7	Transmission Date and Time	M	X	•	Date and time, in Universal Time (UTC) that the originator initiates the message.
11	System Trace Audit Number	M	X	•	Transaction trace number; must be unique value for transaction initiator within each UTC day.
33	Forwarding Institution Identification Code	M	X	•	Contains the processor ID of the CPS or NCID originating this message.
60	Advice Reason Code	M	X	•	Indicates the specific reason for this message. 600 = Rejected message 603 = Time Based exception
63	Network Data	•	X	M	Provided by the MDS. Contains the MDS reference number for this transaction.
100	Receiving Institution Identification Code	O	X	•	Must contain the processor ID of the network destination for this message.
112	Additional Data (National Use)	C	C	C	Must contain the same values from the original Time-Based request message, with the exception of subfield 24 which is optionally populated by the originator.
120	Record Data	C	X	•	If DE 60 = 600, this data element may be used to contain the original (rejected) message.
127	Private Data	O	X	•	Available for private use by the message originator. Does not pass through the MDS.

Administrative Advice/0620—Processor Initiated Time-Based Exception

Note **The Time-based payments service is currently available for members in Brazil only.**

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	P	M	Value must be 0620.
-	Bit Map, Primary	M	P	M	Mandatory.
1	Bit Map, Secondary	C	P	M	Mandatory.
7	Transmission Date and Time	M	P	M	Date and time, in Universal Time (UTC) that the originator initiates the message.
11	System Trace Audit Number	M	P	M	Transaction trace number; must be unique value for transaction initiator within each UTC day.
33	Forwarding Institution Identification Code	M	P	M	Contains the processor ID of the CPS or NCID originating this message.
60	Advice Reason Code	M	P	M	Indicates the specific reason for this message. 603 = Time Based exception.
63	Network Data	•	X	M	Provided by the MDS. Contains the MDS reference number for this transaction.
100	Receiving Institution Identification Code	O	P	M	Must contain the processor ID of the network destination for this message.
120	Record Data	C	P	C	If DE 60 = 600, this data element may be used to contain the original (rejected) message.
112	Additional Data (National Use)	C	P	C	Must contain the same values from the original Time-based request message, with the exception of subfield 24 which is optionally populated by the originator.
127	Private Data	O	X	•	Available for private use by the message originator. Does not pass through the MDS.

Administrative Advice Response/0630—MDS Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	X	•	Value must be 0630.
-	Bit Map, Primary	M	X	•	Mandatory.
1	Bit Map, Secondary	M	X	•	Mandatory.
7	Transmission Date and Time	M	X	•	Must contain the same value from the original advice message.
11	System Trace Audit Number	M	X	•	Must contain the same value from the original advice message.
33	Forwarding Institution Identification Code	M	X	•	Must contain the same value from the original advice message.
39	Response Code	M	X	•	Response code for this message.
44	Additional Response Data	C	X	•	May contain data element number where edit error occurred in a rejected message.
63	Network Data	M	X	•	Must contain the same value from the original advice message.
100	Receiving Institution Identification Code	M	X	•	Must contain the processor ID of the network destination for this message.
127	Private Data	O	X	•	Available for private use by the message originator. This data does not pass through the MDS.

Administrative Advice Response/0630—Processor Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	X	•	Value must be 0630.
-	Bit Map, Primary	M	X	•	Mandatory.
1	Bit Map, Secondary	M	X	•	Mandatory.
7	Transmission Date and Time	M	X	•	Must contain the same value from the original advice message.
11	System Trace Audit Number	M	X	•	Must contain the same value from the original advice message.
33	Forwarding Institution Identification Code	M	X	•	Must contain the same value from the original advice message.
39	Response Code	M	X	•	Response code for this message.
44	Additional Response Data	C	X	•	May contain data element number where edit error occurred in a rejected message.
63	Network Data	M	X	•	Must contain the same value from the original advice message.
100	Receiving Institution Identification Code	M	X	•	Must contain the processor ID of the network destination for this message.
127	Private Data	O	X	•	Available for private use by the message originator. This data does not pass through the MDS.

Administrative Advice/0644

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value must be 0644.
-	Bit Map, Primary	•	X	M	Mandatory.
1	Bit Map, Secondary	•	X	M	Mandatory.
7	Transmission Date and Time	•	X	M	The system transmits the date and time, in UTC format of this message.
11	System Trace Audit Number	•	X	M	Must contain the same value from the original message.
33	Forwarding Institution Identification Code	•	X	M	Must contain the same value from the original message.
60	Advice Reason Code	•	X	M	Indicates the specific reason for this message. 690x = rejected message
63	Network Data	•	X	M	Contains the Banknet reference number. The interface replaces this number with the MDS switch serial number.
100	Receiving Institution Identification Code	•	X	M	Must contain the Processor ID of the CPS or Network destination for this message.
120	Record Data	•	X	C	If ARC = 690x, this data element may be used to contain the original (rejected) message.
127	Private Data	•	X	C	Available for private use by the message originator. Does not pass through the MDS.

Network Management Request/0800—Acquirer or Issuer Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	X	•	Value must be 0800 for all Network Management Request/0800 messages.
-	Bit Map, Primary	M	X	•	Mandatory.
1	Bit Map, Secondary	M	X	•	Mandatory.
2	Primary Account Number	M	X	•	For **debit** processors, this data element must contain the originating processor ID for sign–on/sign-off by group NCID network management codes (see DE 70, below). For **credit** customers, this data element must contain the Group Sign-on ID (GSI) number.
7	Transmission Date and Time	M	X	•	The system transmits the date and time (in UTC format) of the message.
11	System Trace Audit Number	M	X	•	Transaction trace number; must be unique value for transaction initiator within each UTC day.
33	Forwarding Institution Identification Code	M	X	•	For **debit** processors, DE 33 contains the processor ID of the CPS or NCID originating this message. For **credit** customers, DE 33 contains the MasterCard customer ID number of the CPS or INF originating this message.
48	Additional Data	C	X	•	Key data for PIN encryption key exchange messages only, where DE 70 = 161.
63	Network Data	O	X	•	The MDS will overwrite the contents of DE 63, and return the MDS-generated network reference number in the 0810 response message.

Data Element ID and Name		Org	Sys	Dst	Comments
70	Network Management Information Code	M	X	•	Indicates the specific purpose of this 0800 message. Valid values are as follows: 060 = Store and Forward session request 061 = Sign-on by processor to the MDS 062 = Sign-off by processor from the MDS 065 = Sign-off by processor from the MDS, MDS to begin Stand-In processing 066 = Sign-on by processor to the MDS, MDS to cease Stand-In processing 161 = PIN encryption key change 162 = Processor-initiated key change 270 = Echo Test
96	Message Security Code	C	X	•	Contains a MDS Password security code to verify that the originator of the Sign-on Request is allowed access to the requested functions.
127	Private Data	O	X	•	Available for private use by the message originator. Does not pass through the MDS.

Network Management Request/0800—System Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value must be 0800 for all Network Management Request/0800 messages.
-	Bit Map, Primary	•	X	M	Mandatory.
1	Bit Map, Secondary	•	X	M	Mandatory.
2	Primary Account Number	•	X	M	Required for 0800 messages destined for the Banknet credit card system. Must contain the Group Sign-on ID of the key exchange recipient. DE 2 is not sent in the 0800 message to **debit** processors.
7	Transmission Date and Time	•	X	M	The system transmits the date and time (in UTC format) of the message.
11	System Trace Audit Number	•	X	M	Transaction trace number; must be unique value for transaction initiator within each UTC day.
33	Forwarding Institution Identification Code	•	X	M	For **debit** processors, DE 33 contains the processor ID of the CPS or NCID to whom this message is destined. For **credit** customers, DE 33 contains MDS ICA number 002202.
48	Additional Data	•	X	C	Key data for PIN encryption key exchange messages only, where DE 70 = 161.
63	Network Data	•	X	M	Provided by the MDS. Includes a network reference number for this transaction.
70	Network Management Information Code	•	X	M	Indicates the specific purpose of this 0800 message. Valid values are as follows: 060 = Store and Forward session request 061 = Sign-on by processor to the MDS 062 = Sign-off by processor from the MDS 065 = Sign-off by processor from the MDS, MDS to begin Stand-In processing 066 = Sign-on by processor to the MDS, MDS to cease Stand-In processing 161 = PIN encryption key change 162 = Processor-initiated key change 270 = Echo Test

Network Management Request Response/0810—Acquirer or Issuer Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	M	X	•	Value must be 0810 for all Network Management Request/0810 messages.
-	Bit Map, Primary	M	X	•	Mandatory.
1	Bit Map, Secondary	M	X	•	Mandatory.
7	Transmission Date and Time	M	X	•	Must contain the same value from the original request message.
11	System Trace Audit Number	M	X	•	Must contain the same value from the original request message.
33	Forwarding Institution Identification Code	M	X	•	Must contain the same value from the original request message.
39	Response Code	M	X	•	Response code for this message.
44	Additional Response Data	C	X	•	May contain additional response or diagnostic information when DE 39 (Response Code) is 30.
48	Additional Data	C	X	•	For key change messages (DE 70 = 161), this field may contain the PIN encryption key.
63	Network Data	M	X	•	Must contain the same value from the original request message.
70	Network Management Information Code	M	X	•	Must contain the same value from the original request message.
127	Private Data	O	X	•	Available for private use by the message originator. Does not pass through the MDS.

Network Management Request Response/0810—System Initiated

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value must be 0810 for all Network Management Request/0810 messages.
-	Bit Map, Primary	•	X	M	Mandatory.
1	Bit Map, Secondary	•	X	M	Mandatory.
7	Transmission Date and Time	•	X	M	Must contain the same value from the original request message.
11	System Trace Audit Number	•	X	M	Must contain the same value from the original request message.
33	Forwarding Institution Identification Code	•	X	M	Must contain the same value from the original request message.
39	Response Code	•	X	M	Response code for this message.
44	Additional Response Data	•	X	C	May contain additional response or diagnostic information when DE 39 (Response Code) is 30.
48	Additional Data	•	X	C	For key change messages (DE 70 = 161), this field may contain the PIN encryption key.
63	Network Data	•	X	M	Provided by the MDS. Includes a network reference number for this transaction.
70	Network Management Information Code	•	X	M	Must contain the same value from the original request message.
127	Private Data	•	X	C	Available for private use by the message originator. Does not pass through the MDS.

Network Management Advice/0820

Note **The MDS-generated Network Management Advice/0820 messages do not require a subsequent response message.**

Data Element ID and Name		Org	Sys	Dst	Comments
-	Message Type Identifier (MTI)	•	X	M	Value must be 0820 for all Network Management Advice /0820 messages.
-	Bit Map, Primary	•	X	M	Mandatory.
1	Bit Map, Secondary	•	X	M	Mandatory.
7	Transmission Date and Time	•	X	M	The system transmits the date and time (in UTC format) of the message.
11	System Trace Audit Number	•	X	M	Transaction trace number. When the 0820 message is sent to a **credit** customer, DE 11 will contain the same value as the original 0800 message. When it is sent to a **debit** processor, DE 11 will contain a newly-generated value, different from what was sent in the original 0800 message.
33	Forwarding Institution Identification Code	•	X	M	Contains the same value as in the original 0800 message.
48	Additional Data	•	X	C	For key change messages (DE 70 = 161), this field will be present. Will not be present when the 0810 message is denied.
63	Network Data	•	X	M	Provided by the MDS. When the 0820 message is sent to a **credit** customer, DE 63 will contain the same value as in the original 0800 message. When it is sent to a **debit** processor, DE 63 will contain a newly-generated value, different from what was sent in the original 0800 message.
70	Network Management Information Code	•	X	C	Indicates the specific purpose of this 0820 message. Will not be present when the 0810 message is denied. Valid values are as follows: 161 = Encryption key change confirmed 363 = Store and Forward complete
127	Private Data	•	X	C	Available for private use by the message originator. Does not pass through the MDS.

4 Data Element Definitions

This chapter provides a detailed definition of all data elements used within MasterCard® Debit Switch (MDS) System application messages.

Overview

This chapter provides a detailed definition of all data elements that are used within ISO 8583–1987 bank card message types. Information is presented in the following order:

1. Explanation of the notation used throughout this chapter to describe all data element attributes.
2. Summary list of all ISO 8583–1987 data elements in the order of their ISO-assigned bit map numbers, including annotation of those data elements which are currently **not implemented** within the ISO 8583–1987 specification.
3. Detailed definition of each message data element, presented in the order of the data element bit map number. Information provided for each data element includes the following:
   - Data element definition
   - Data element usage
   - Data element formats, including data representation attributes, data field format, and data field length
   - Data element values or field edits indicating the specific value(s) or permissible range of values that may be present within the data element
   - Product application notes, where applicable, that detail unique, product-specific, or message-specific usage of the data element

Annotation Conventions for Data Element Attributes

The following notation conventions are used throughout this chapter to describe the attributes of ISO 8583–1987 message data elements:

Conventions for Data Representation

The data encoding conventions listed below have been adapted for all ISO 8583–1987 messages:

- The system aligns all message data element fields on byte boundaries; for example; a data field cannot begin with the low order "nibble" or any bit other than the high-order bit of any byte.
- All of the data types listed in Table 4.1, are encoded for transmission between the MDS and processor systems using EBCDIC display character representation:
- All of the valid special character symbols listed in Table 4.2 are used in mapping un-printable characters provided in DE 43, Card Acceptor Name and Location, to printable characters.

Oct 2005

- All numeric (attribute **n**) data elements are **right justified** with **leading zeroes** unless otherwise specified in the individual data element definitions. All other data elements are **left justified** with **trailing blanks** unless otherwise specified.
- All binary (attribute **b**) data elements are constructed of bit-strings which have lengths that are an integral number of 8-bit bytes. No binary data element has a length of less than eight bits (one byte).
- All track-2 or track-3 (attribute **z**) data elements are encoded as EBCDIC representations of the hexadecimal data specified in ISO specification 7811 and 7812. Thus, a hex "D" (binary "1101") is encoded as an EBCDIC "D" character, and so on. The LLVAR or LLLVAR length specification associated with these data elements specifies the field length in number of bytes.
- The system encodes all length subfields as numeric EBCDIC, right justified with leading zeroes.
  - Fields designated LL are 2-character numeric fields with values from "01" to "99".
  - Fields designated LLL are 3-character numeric fields with values from "001" to "999".

General Representation

Table 4.1—Data Types

Notation	Description
a	alphabetic characters only (MUST USE UPPERCASE LETTERS) [a]
n	numeric characters only
s	special characters only
an	alpha and numeric characters
as	alpha and special characters
ns	numeric and special characters
ans	alpha, numeric, and special characters
b	binary data
z	magnetic stripe track-2 or track-3 data
x	character "C" or "D" to indicate "credit" or "debit" value of a dollar amount

[a] The MDS application requires use of uppercase letters in data specifying state and country codes. Thus, safe, general practice is to code alpha data as uppercase.

Special Character Values

Oct 2005

Table 4.2—Special Character Values

Extended Character	ASCII Hex	EBCDIC Hex	Description	Mapped to	Note
â	E2	42	Latin small letter a with circumflex	a	
ä	E4	43	Latin small letter a with diaeresis	a	
à	E0	44	Latin small letter a with grave	a	
á	E1	45	Latin small letter a with acute	a	
ã	E3	46	Latin small letter a with tilde	a	
å	E5	47	Latin small letter a with ring above	a	
ç	E7	48	Latin small letter c with cedilla	c	
ñ	F1	49	Latin small letter n with tilde	n	

Extended Character	ASCII Hex	EBCDIC Hex	Description	Mapped to	Note
¢	A2	4a	Cent sign	N/A	Default to blank
é	E9	51	Latin small letter e with acute	e	
ê	EA	52	Latin small letter e with circumflex	e	
ë	EB	53	Latin small letter e with diaeresis	e	
è	E8	54	Latin small letter e with grave	e	
í	ED	55	Latin small letter i with acute	i	
î	EE	56	Latin small letter i with circumflex	i	
ï	EF	57	Latin small letter i with diaeresis	i	
ì	EC	58	Latin small letter i with grave	i	
ß	DF	59	Latin small letter sharp s (German)	B	
Â	C2	62	Latin capital letter A with circumflex	A	
Ä	C4	63	Latin capital letter A with diaereses	A	
À	C0	64	Latin capital letter A with grave	A	
Á	C1	65	Latin capital letter A with acute	A	
Ã	C3	66	Latin capital letter A with tilde	A	
Å	C5	67	Latin capital letter A with ring above	A	
Ç	C7	68	Latin capital letter C with cedilla	C	
Ñ	D1	69	Latin capital letter N with tilde	N	
¦	A6	6A	Broken bar	|	
ø	F8	70	Latin small letter o with stroke	o	
É	C9	71	Latin capital letter E with acute	E	
Ê	CA	72	Latin capital letter E with circumflex	E	
Ë	CB	73	Latin capital letter E with diaereses	E	
È	C8	74	Latin capital letter E with grave	E	
Í	CD	75	Latin capital letter I with acute	I	
Î	CE	76	Latin capital letter I with circumflex	I	
Ï	CF	77	Latin capital letter I with diaereses	I	
Ì	CC	78	Latin capital letter I with grave	I	
Ø	D8	80	Latin capital letter O with stoke	0	

Oct 2005

Oct 2005

Extended Character	ASCII Hex	EBCDIC Hex	Description	Mapped to	Note
«	AB	8A	Left-pointing double angle quotation mark	<	
»	BB	8B	Right-pointing double angle quotation mark	>	
ð	F0	8C	Latin small letter ETH (Icelandic)	o	
ý	FD	8D	Latin small letter y with ACUTE	y	
þ	FE	8E	Latin small letter THORN (Icelandic)	p	
±	B1	8F	Plus-minus sign	N/A	
°	B0	90	Degree sign	N/A	
ª	AA	9A	Feminine ordinal indicator	a	
º	BA	9B	Masculine ordinal indicator	o	
æ	E6	9C	Latin small ligature AE	N/A	
¸	A8	9D	Cedilla	N/A	
Æ	C6	9E	Latin capital ligature AE	N/A	
¤	A4	9F	Currency sign	N/A	
µ	B5	A0	Micro sign	N/A	
¡	A1	AA	Inverted exclamation mark	N/A	
¿	BF	AB	Inverted question mark	N/A	
Ð	D0	AC	Latin capital letter ETH (Icelandic)	N/A	
Þ	DE	AE	Latin capital lettern thorn (Icelandic)	N/A	
®	AE	AF	Registered sign	N/A	
¬	AC	B0	Not sign	N/A	
£	A3	B1	Pound sign	N/A	
¥	A5	B2	Yen sign	N/A	
·	B7	B3	Middle dot	N/A	
©	A9	B4	Copyright sign	N/A	
§	A7	B5	Section sign	N/A	
¶	B6	B6	Pilcrow sign	N/A	
¼	BC	B7	Vulgar fraction one quarter	N/A	
½	BD	B8	Vulgar fraction one half	N/A	
¾	BE	B9	Vulgar fraction three quarter	N/A	
Ý	DD	BA	Latin capital letter Y with acute	Y	

Extended Character	ASCII Hex	EBCDIC Hex	Description	Mapped to	Note
¨	A8	BB	Diaereses	N/A	
¯	AF	BC	Macron	-	
´	B4	BE	Acute accent	N/A	
×	D7	BF	Multiplication sign	*	
-	AD	CA	Soft hypen	-	
ô	F4	CB	Latin small letter o with circumflex	o	
ö	F6	CC	Latin small letter o with diaereses	o	
ò	F2	CD	Latin small letter o with grave	o	
ó	F3	CE	Latin small letter o with acute	o	
õ	F5	CF	Latin small letter o with tilde	o	
¹	B9	DA	Superscript one	1	
û	FB	DB	Latin small letter u with circumflex	u	
ü	FC	DC	Latin small letter u with diaereses	u	
ù	F9	DD	Latin small letter u with grave	u	
ú	FA	DE	Latin small letter u with acute	u	
ÿ	FF	DF	Latin small letter y with diaeresis	y	
÷	F7	E1	Division sign	/	
²	B2	EA	Superscript two	2	
Ô	D4	EB	Latin capital letter O with circumflex	O	
Ö	D6	EC	Latin capital letter O with diaeresis	O	
Ò	D2	ED	Latin capital letter O with grave	O	
Ó	D3	EE	Latin capital letter O with acute	O	
Õ	D5	EF	Latin small letter O with tilde	O	
³	B3	FA	Superscript three	3	
Û	DB	FB	Latin capital letter U with circumflex	U	
Ü	DC	FC	Latin capital letter U with diaeresis	U	
Ù	D9	FD	Latin capital letter U with grave	U	
Ú	DA	FE	Latin capital letter U with acute	U	

Oct 2005

Length Attributes

Table 4.3—Data Length Attributes

Notation	Description
-digit(s)	Fixed length in number of positions. Example: "n-3" indicates a 3-position numeric field. Example: "an-10" indicates a 10-position alphanumeric field.
...digit(s)	Variable length field, with maximum number of positions specified. Example: "n...11" indicates a variable length numeric field of up to 11 digits. Example: "an...25" indicates a variable length alphanumeric field of up to 25 characters.
LLVAR	Present with a variable-length data element attribute, indicates that the data element contains two fields: "LL" is the length field and represents the number of positions in the variable-length data field that follows. The length field contains a value in the range of 01–99. "VAR" is the variable-length data field. Example: "an...25; LLVAR" represents a variable-length alphanumeric data element with a length of 1–25 positions.
LLLVAR	Present with a variable-length data element attribute, indicates that the data element contains two fields: "LLL" is the length field and represents the number of positions in the variable-length data field that follows. The length field contains a value in the range 001-999. "VAR" is the variable-length data field. Example: "an...500; LLLVAR" indicates a variable-length alphanumeric data element having a length of 1–500 positions.

Field Content Attributes

Table 4.4—Data and Time Attributes

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

Message Data Elements

Table 4.5 lists all data elements implemented within the ISO 8583–1987 message standard in numeric order. Where indicated, some data elements are currently not used. **ISO 8583–1987 messages should not contain these data elements.**

Table 4.5—ISO 8583–1987 Message Standard Data Elements

Data Element ID and Name		Attributes
1	Bit map, Secondary	b-64
2	Primary Account Number	n...19; LLVAR
3	Processing Code	n-6
4	Amount, Transaction	n-12
5	Amount, Settlement	n-12
6	Amount, Cardholder Billing	n-12
7	Transmission Date and Time	n-10; MMDDhhmmss
8	Amount, ICCR	n-8
9	Conversion Rate, Settlement	n-8
10	Conversion Rate, Cardholder Billing	n-8
11	System Trace Audit Number	n-6
12	Time, Local Transaction	n-6; hhmmss
13	Date, Local Transaction	n-4; MMDD
14	Date, Expiration	n-4; YYMM
15	Date, Settlement	n-4; MMDD
16	Date, Conversion	n-4; MMDD
17	Date, Capture (not currently used)	n-4; MMDD
18	Merchant Type (MCC)	n-4
19	Acquiring Institution Country Code (not currently used)	n-3
20	Primary Account Number, Extended, Country Code (not currently used)	n-3
21	Forwarding Institution Country Code (not currently used)	n-3

Data Element ID and Name		Attributes
22	Point of Service Entry Mode	n-3
23	Card Sequence Number	n-3
24	Network International Identifier (not currently used)	n-3
25	Point of Service Condition Code (not currently used)	n-2
26	Point of Service PIN Capture Code	n-2
27	Authorization Identification Response Length (not currently used)	n-1
28	Amount, Transaction Fee	x+n-8
29	Amount, Settlement Fee	x+n-8
30	Amount, Transaction Processing Fee (not currently used)	x+n-8
31	Amount, Settlement Processing Fee	x+n-8
32	Acquiring Institution Identification Code	n...11; LLVAR
33	Forwarding Institution Identification Code	n...11; LLVAR
34	Primary Account Number, Extended (not currently used)	ns...28; LLVAR
35	Track-2 Data	z...37; LLVAR
36	Track-3 Data (not currently used)	z...104; LLLVAR
37	Retrieval Reference Number	an-12
38	Authorization Identification Response	an-6
39	Response Code	an-2
40	Service Restriction Code (not currently used)	an-3
41	Card Acceptor Terminal Identification	ans-8
42	Card Acceptor Identification Code	ans-15
43	Card Acceptor Name/Location	ans-40
44	Additional Response Data	ans...25; LLVAR
45	Track-1 Data	ans...79; LLVAR
46	Additional Data (ISO) (not currently used)	ans...999; LLLVAR
47	Additional Data (National) (not currently used)	ans...999; LLLVAR
48	Additional Data (Private/ISO 8583–1987)	ans...999; LLLVAR
49	Currency Code, Transaction	n-3
50	Currency Code, Settlement	n-3

Data Element ID and Name		Attributes
51	Currency Code, Cardholder Billing	n-3
52	Personal Identification Number (PIN) Data	b-64
53	Security Related Control Information (not currently used)	n-16
54	Additional Amounts	an...120; LLLVAR
55	Integrated Circuit Card (ICC) System Related Data	b...255; LLLVAR
56	Reserved (ISO) (not currently used)	ans...999; LLLVAR
57–59	Reserved (National) (not currently used)	ans...999; LLLVAR
60	Advice Reason Code	ans...060; LLLVAR
61	Point of Service (POS) Data	ans...026; LLLVAR
62	Intermediate Network Facility (INF) Data	ans...050; LLLVAR
63	Network Data	ans...044; LLLVAR
64	Message Authentication Code (MAC) (not currently used)	b-64
65	Bit map, Extended (not currently used)	b-64
66	Settlement Code	n-1
67	Extended Payment Code (not currently used)	n-2
68	Receiving Institution Country Code (not currently used)	n-3
69	Settlement Institution Country Code (not currently used)	n-3
70	Network Management Information Code	n-3
71	Message Number (not currently used)	n-4
72	Message Number Last (not currently used)	n-4
73	Date, Action (not currently used)	n-6; YYMMDD
74	Credits, Number	n-10
75	Credits, Reversal Number	n-10
76	Debits, Number	n-10
77	Debits, Reversal Number	n-10
78	Transfers, Number	n-10
79	Transfers, Reversal Number	n-10
80	Inquiries, Number	n-10

Data Element ID and Name		Attributes
81	Authorizations, Number	n-10
82	Credits, Processing Fee Amount	n-12
83	Credits, Transaction Fee Amount	n-12
84	Debits, Processing Fee Amount	n-12
85	Debits, Transaction Fee Amount	n-12
86	Credits, Amount	n-16
87	Credits, Reversal Amount	n-16
88	Debits, Amount	n-16
89	Debits, Reversal Amount	n-16
90	Original Data Elements	n-42
91	File Update Code	an-1
92	File Security Code (not currently used)	an-2
93	Response Indicator (not currently used)	an-5
94	Service Indicator (not currently used)	an-7
95	Replacement Amount	n-42
96	Message Security Code (not currently used)	b-64
97	Amount, Net Settlement	x+n-16
98	Payee (not currently used)	ans-25
99	Settlement Institution Identification Code	n...11; LLVAR
100	Receiving Institution Identification Code	n...11; LLVAR
101	File Name	ans...17; LLVAR
102	Account Identification-1	ans...28; LLVAR
103	Account Identification-2	ans...28; LLVAR
104	Transaction Description (not currently used)	ans...100; LLLVAR
105–109	Reserved for ISO use (not currently used)	ans...999; LLLVAR
110	Unique Merchant ID	n-6
111	Amount, Currency Conversion Assessment	ans...999; LLVAR
112	Parcelas Data	ans...248; LLLVAR
113–119	Reserved for National use (not currently used)	ans...999; LLLVAR
120	Record Data	ans...999; LLLVAR

Oct 2005

Data Element ID and Name		Attributes
121	Authorizing Agent Identification Code (not currently used)	ans...011; LLLVAR
122	Additional Record Data	ans…100; LLLVAR
123	Reserved for future definition and use by MasterCard (not currently used)	ans...999; LLLVAR
124	Member-defined Data	ans...099; LLLVAR
125	Reserved for future definition and use by MasterCard (not currently used)	ans...999; LLLVAR
126	Reserved (Private/ISO 8583–1987) (not currently used)	ans...999; LLLVAR
127	Private Data	ans...050; LLLVAR
128	Message Authentication Code (not currently used)	b-64

Data Element Definitions

The remainder of this chapter contains detailed definitions of all the ISO 8583–1987 message data elements.

Message Type Identifier (MTI)

The Message Type Identifier is a four-digit numeric field describing the type of interchange message.

Attribute

n-4

Usage

This data element must be present as the first field of each ISO 8583–1987 message.

Values

Table 4.6 lists the valid message types for the MDS.

Table 4.6—ISO 8583–1987 Message Types

Code	Description
Financial Transaction/02xx Messages	
0200	Financial Transaction Request
0210	Financial Transaction Request Response
0220	Financial Transaction Advice
0230	Financial Transaction Advice Response
0290	Financial Transaction Negative Acknowledgment
File Update/(03xx Messages	
0302	File Update Request
0312	File Update Request Response

Code	Description
Reversal Advice/04xx Messages	
0420	Acquirer Reversal Advice
0430	Acquirer Reversal Advice Response
0422	Issuer Reversal Advice
0432	Issuer Reversal Advice Response
Administrative Advice/06xx Messages	
0620	Administrative Advice
0630	Administrative Advice Response
0644	Administrative Advice
Network Management/08xx Messages	
0800	Network Management Request
0810	Network Management Request Response
0820	Network Management Advice

Primary and Secondary Bit Maps

A bit map is a series of 64 bits used to identify the presence or absence (denoted by "1" or "0", respectively) of each data element. The MDS interprets the bit map from left to right. The leftmost bit represents DE 1 in the Primary Bit Map and DE 65 in the Secondary Bit Map. The rightmost bit represents DE 64 in the Primary Bit Map and DE 128 in the Secondary Bit Map.

Attribute

b-64 (for each bit map)

Note **If both bit maps are present, the total length of the bit map field is 128 bits (16 bytes).**

Usage

All bit positions are interpreted from left to right within each bit map; such as within the Primary Bit map the leftmost bit is "DE 1", and the rightmost bit is "DE 64".

- ISO 8583–1987 messages are variable length, with a bit map scheme that indicates the presence or absence of additional fields in the message
- Each bit map is a 64-bit string contained within an 8-byte field.
- The first bit in each bit map is set to "1" indicating the presence or "0" indicating the absence of an additional 64-bit bit map field which immediately follows the preceding bit map field.
- ISO 8583–1987 message format uses a maximum of 2 bit maps: a "Primary" and a "Secondary" bit map.
- Bits set to "1" or "0" in the Primary Bit map indicate the presence or absence of DE 2 through DE 64.
- Bits set to "1" or "0" in the Secondary Bit map indicate the presence or absence of DE 66 through DE 128.

- Bit No. 1 in the Primary Bit Map and DE 65 in the Secondary Bit Map (such as the first bit in each bit map) do not have corresponding data elements. These bits indicate the presence or absence of additional bit map fields in the message.
  - If bit No. 1 is set to "1", it indicates that the Secondary Bit Map is present, and selected data elements in the DE 66 through DE 128 range are also present in the message (as indicated by bit positions in the Secondary Bit Map.)
  - Bit No. 65 **must always be set to "0"**, because there are no additional bit maps defined beyond the Secondary Bit Map in the ISO 8583–1987 message specification.
- All ISO 8583–1987 messages must contain a Primary Bit Map.
  - The Secondary Bit Map is only included in a message when data elements in the range DE 66 through DE 128 are present in the message.
- Although additional bit maps are accommodated in ISO Standard 8583 (such as setting the first bit in any bit map to "1" to indicate the presence of a following extended bit map), the ISO 8583–1987 implementation uses a **maximum of two bit maps** (Primary and Secondary), with a maximum number of message data elements in the range DE 1 through DE 128. Consequently, DE 65 (the first bit in Bit Map, Secondary) **must always be set to zero**.
- Bits corresponding to **mandatory** data elements for a specific message type must be set to "1" to indicate the presence of the data element in the message. Otherwise, the message will be rejected by the MDS through the appropriate response message or through an Administrative Advice (Reject)/0620 message.

DE 1—Bit Map, Secondary

The Bit Map, Secondary (DE 1) is a series of 64 bits used to identify the presence ("1") or absence ("0") of each data element in the second segment of a message (for example, data elements in the range Settlement Code (DE 66) through Message Authentication Code (DE 128).

Attribute

b-64

DE 2—Primary Account Number (PAN)

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

Attribute

n...19; LLVAR

Usage

This data element has two primary uses:

1. It contains the Primary Account Numbers (PAN) in authorization (01xx), financial transaction (02xx) and reversal advice (04xx) messages.

   The MDS uses this data element for all PANs up to 19 digits in length, in authorization (01xx), financial transaction (02xx), and reversal advice (04xx) messages.

   PAN data consists of three primary components:

   – Issuer identification number (IIN)

   – Individual account identification number

   – PAN check digit

   ISO specification 7812 and 7813 details the specific requirements for PAN composition. All PANs used in ISO 8583–1987 messages must conform to the ISO PAN encoding requirements as specified in these documents.

   The (class 0) network management (08xx) messages may use the data element to contain a valid processor ID number or a variable-length issuer card prefix.

   The PAN field may contain only an Issuer Identification Number or card prefix sequence identified by a card-issuing institution. It may also contain a valid processor ID for certain 08xx-series messages. The individual Message Format Specification charts detail the specific usage requirements for each message.

2. The MDS will accommodate variable-length prefix sequences from four to eleven digits, where card prefix information is required. Processor IDs used in this data element must be valid values assigned by MasterCard.

Note **The processor ID is a ten-digit number of the form: "9000000xxx" where "xxx" is the 3-digit MDS–assigned processor ID.**

DE 3—Processing Code

The Processing Code (DE 3) is a series of digits used to describe the effect of a transaction on the customer account and the type of accounts affected.

Attribute

n-6

Usage

Table 4.7 describes the subfields in DE 3.

Table 4.7—Processing Code Subfields

Subfield	Position	Attribute	Value
Transaction Type	1-2	n	Describes the transaction being performed. **00** Purchase (00 code also used for cash back and scrip transactions) **01** Withdrawal **02** Debit Adjustment (*Debit MasterCard Only*) **17** Cash Disbursement (can be sent to 0100 issuers) **20** Refund/Correction **21** Deposit **23** Credit Adjustment *(Debit MasterCard Only)* **28** Payment **30** Balance Inquiry **40** Account Transfer **50** Bill Payment **90** Electronic Commerce (Set Certificate and Cardholder Certificate information)
Account Type (From)	3-4	n	Describes the cardholder account type affected for cardholder account debits and inquiries, and the "from" account type for cardholder account transfer transactions. **00** No account specified (NAS)/Default Account **10** Savings Account **20** Checking Account **30** Credit Card Account

Subfield	Position	Attribute	Value
Account Type (To)	5-6	n	Describes the cardholder account type affected for cardholder account credits and the "to" account type for cardholder account transfer transactions. **00** No account specified (NAS)/Default Account **10** Savings Account **20** Checking Account **30** Credit Card Account

Table 4.8 lists all valid combinations of subfields supported by the MasterCard® Debit Switch (MDS) as Processing Codes.

Table 4.8—MasterCard® Debit Switch Processing Code Values

Code	Description
000000	Purchase; no account specified *Not valid for ATM Gateway transactions (for example, Plus, or Visa).*
001000	Purchase from savings account
002000	Purchase from checking account
010000	Withdrawal; no account specified
011000	Withdrawal from savings account
012000	Withdrawal from checking account
013000	Withdrawal from credit card account. *Acquirer Processing Systems (APS) connected to the MDS must use this processing code for cash advance transactions. The MDS translates this processing code as an Authorization Request/0100 message with a processing code of 173000.* *NOTE: The MDS performs the above processing for any cash withdrawal request.*
020000	Debit adjustment; no account specified *Codes valid for debit MasterCard only. Debit MasterCard adjustments must be 020000.*
021000	Debit adjustment to savings account *(debit MasterCard Only)*
022000	Debit adjustment to checking account *(debit MasterCard Only)*
200000	Online refund; no account specified *Codes valid for debit MasterCard and Maestro transactions only.*
201000	Online refund to savings account
202000	Online refund to checking account

Code	Description
210010	Online deposit to savings account
210020	Online deposit to checking account
230000	Credit adjustment; no account specified *Codes valid for debit MasterCard only. Debit MasterCard adjustments must be 230000.*
231000	Credit adjustment to savings account *(debit MasterCard Only)*
232000	Credit adjustment to checking account *(debit MasterCard Only)*
280000	Payment to NAS
280010	Payment to Savings
280020	Payment to Checking
280030	Payment to Credit Account
300000	Balance inquiry; no account specified *When no account is specified on a balance inquiry transaction, the issuer may return both checking and savings account balances if applicable.*
301000	Balance inquiry on savings account
302000	Balance inquiry on checking
303000	Balance inquiry on credit card (credit line)
401020	Transfer from savings account to checking account
402010	Transfer from checking account to savings account
500000	Bill Payment, no account specified
501000	Bill Payment, savings
502000	Bill Payment, checking
503000	Bill Payment, credit card
900000	Electronic Commerce, no account specified, certificate request
901000	Electronic Commerce, savings, certificate request
902000	Electronic Commerce, checking, certificate request
903000	Electronic Commerce, credit card, certificate request

Note

The MasterCard® Debit Switch (MDS) only supports the specific Processing Code subfield combinations listed in Table 4.8.

When the Account Type value processing code in the Financial Transaction Request/0200 message indicates “no account specified”, the issuer may specify an Account Type in the Financial Transaction Request Response/0210 message. For example, when an acquirer sends processing code 010000 (withdrawal, no account specified), the issuer may send a Financial Transaction Request Response/0210 message containing processing code 012000 (withdrawal, checking account).

DE 4—Amount, Transaction

Amount, Transaction (DE 4) is the amount of funds requested by the cardholder in the local currency of the acquirer or source location of the transaction. The Transaction Fee Amount (DE 28) must be included in DE 4. DE 4 may include ATM Access Charges if DE 28 is present.

Attribute

n-12

Usage

The local currency of the card acceptor (currency used by the cardholder and merchant at the point of service) must always be specified using the Currency Code, Transaction (DE 49). The MDS refers to this currency as the "currency of the acquirer" or the "currency of the transaction at the point of service".

Amounts are expressed without a decimal separator. For currencies that support exponents, users and systems are responsible for placing the decimal separator appropriately. Refer to the *Quick Reference Booklet* for a listing of currencies and their exponents. See Table 4.9 for examples of decimal separator placement.

Table 4.9—Decimal Separator Example (DE 4)

Amount, Transaction DE 4	Currency Code DE 49	Currency Exponent	Currency Name	Actual Monetary Value of DE 4
000000001500	792	0	Turkish Lira	1500 Lira
000000001500	124	2	Canadian Dollar	15.00 Dollars
000000001500	788	3	Tunisian Dinar	1.500 Dinars

Values

For debit MasterCard clearings (Financial Transaction Advice/0220 message), this data element will contain the completed amount.

DE 5—Amount, Settlement

Amount, Settlement (DE 5) is the amount of funds to be transferred between the acquirer and the issuer (exclusive of fees and ICCR) equal to the Amount, Transaction (DE 4) in the currency of settlement. This field may contain Currency Conversion Assessment, if applicable. Oct 2005

Attribute

n-12

Usage

The currency of this data element must always be specified using the Currency Code, Settlement (DE 50). The MDS automatically inserts this data element into all originating Financial Transaction/02xx messages as a currency conversion service under the following conditions:

- The transaction Currency (DE 49) differs from the currency of settlement (DE 50)
- The transaction currency (DE 49) differs from the issuer currency and Currency Conversion Assessment is applied to the transaction. Oct 2005
- The transaction is settled as ISIS

Amounts are expressed without a decimal separator. For currencies that support exponents, users and systems are responsible for placing the decimal separator appropriately. Refer to the *Quick Reference Booklet* for a listing of currencies and their exponents. See Table 4.10 for examples of decimal separator placement.

Table 4.10—Decimal Separator Example (DE 5)

Amount, Settlement DE 5	Currency Code DE 50	Currency Exponent	Currency Name	Actual Monetary Value of DE 5	Comments
000000001500	840	2	United States Dollar	15.00 Dollars	
000000001500	792	0	Turkish Lira	1500 Lira	ISIS only
000000001500	124	2	Canadian Dollar	15.00 Dollars	
000000001500	788	3	Tunisian Dinar	1.500 Dinars	ISIS only

When this field is present in a message, Conversion Rate, Settlement (DE 9), Date, Conversion (DE 16), and Currency Code, Settlement (DE 50) must also be present.

DE 6—Amount, Cardholder Billing

Amount, Cardholder Billing (DE 6) is the transaction amount converted to the cardholder billing amount. This amount is exclusive of Currency Conversion Assessment or ICCR adjustments.

Oct 2005

Note **This data element is provided to all issuers regardless of participation in the optional ICCR service.**

Attribute

n-12

Usage

The currency of this data element must always be specified using the Currency Code, Cardholder Billing (DE 51). The MDS calculates the Amount, Cardholder Billing (DE 6) for all issuers. This data element is not returned to the acquirer in the 0210 message. The ICCR amount is not included in the MDS settlement amounts.

The MDS performs the calculation to adjust the Amount, Settlement (DE 5) to obtain the Amount, Cardholder Billing (DE 6), which appears in the Financial Transaction Request/0200 message sent by the MDS to the issuer.

When this field is present in a message, Conversion Rate, Cardholder Billing (DE 10), Date, Conversion (DE 16), and Currency Code, Cardholder Billing (DE 51) must also be present.

DE 7—Transmission Date and Time

Transmission Date and Time (DE 7) is the date and time a message was transmitted by a processing entity, to be expressed in coordinated universal time (UTC) time units.

The UTC timestamp is the date and time that a processor, including the MDS, transmits any message (as opposed to the initiation of an entire transaction), containing this data element, to another processor.

MasterCard recommends that processors do not include the values of this data element as part of their message key if they expect this data element to contain the original acquirer transmission timestamp.

If processors want to use the original acquirer timestamp as part of their message key, MasterCard recommends that they use Time, Local Transaction (DE 12) and Date, Local Transaction (DE 13).

Attribute

n-10; MMDDhhmmss

Usage

Upon receipt of the Financial Transaction Request/200 message, with limited exceptions, the MDS updates Data Element 7 with its internal time stamp before sending the message to the issuer. The issuer may return this time to the MDS in the Financial Transaction Request Response/0210 message, or the issuer may send its own transmission time in the data element.

When sending the Financial Transaction Request Response/0210 message to the acquirer, the MDS re-inserts the acquirer's time stamp from the request message in this data element.

Values

This field must contain a valid date and time.

- **MM** must be in the range 01–12
- **DD** must be in the range 01–31
- **hh** must be in the range 00–23
- **mm** must be in the range 00–59
- **ss** must be in the range 00–59

DE 8—Amount, ICCR

Amount, ICCR (DE 8) is the amount calculated by MDS that is the result of the Issuer's Currency Conversion Rate being applied to transactions where the transaction qualifies for the MasterCard Currency Conversion Assessment service and the issuer participates in the MasterCard Issuer Currency Conversion Rate (ICCR) service.

Oct 2005

The MDS automatically inserts this data element in originating 0200 (request), 0220 (force post), and 0420 (reversal), online messages, only when ICCR has been applied to the transaction.

Attribute

n-8; right justified

Usage

Amounts are expressed without a decimal separator. For currencies that support exponents, users and systems are responsible for placing the decimal separator appropriately. Refer to the *Quick Reference Booklet* for a listing of currencies and their exponents.

DE 9—Conversion Rate, Settlement

Conversion Rate, Settlement (DE 9) is the factor used in the conversion from transaction to settlement amount. The MDS multiplies the Amount, Transaction (DE 4) by DE 9 to determine the Amount, Settlement (DE 5).

Attribute

n-8

Usage

The MDS provides automatic currency conversion as a service for customers that participate in international interchange and will supply the conversion rate in this field.

When this data element is present in a message, Amount, Settlement (DE 5), Date, Conversion (DE 16), and Currency Code, Settlement (DE 50) must also be present.

Values

The format is left justified with trailing zeroes. The left-most digit denotes the number of positions that the MDS moves the decimal separator **from the right**. The leftmost digit must be in the range 0 to 7. For example, a field value of 76887050 is interpreted as a conversion rate of 0.6887050.

DE 10—Conversion Rate, Cardholder Billing

Conversion Rate, Cardholder Billing (DE 10) is the factor used in the conversion from transaction to cardholder billing amount. The Amount, Transaction (DE 4) is multiplied by DE 10 to determine Amount, Cardholder Billing (DE 6).

Attribute

n-8

Usage

When this data element is present in a message, Amount, Cardholder Billing (DE 6), Date, Conversion (DE 16), and Currency Code, Cardholder Billing (DE 51) must also be present.

Values

The format is left justified with trailing zeroes. The left-most digit denotes the number of positions that the MDS moves the decimal separator **from the right**. The leftmost digit must be in the range zero to seven. For example, a field value of 69972522 is interpreted as a conversion rate of 9.972522.

DE 11—System Trace Audit Number

The System Trace Audit Number (STAN) is the unique identifier assigned to each transaction by the originator of the message.

Attribute

n-6

Usage

The message originator assigns DE 11. This identifier must be unique for each transaction that occurs within an originator's day. Each originator's day must be based on coordinated universal time (UTC).

DE 11 must remain constant throughout the life of the transaction including responses and acknowledgments that relate to the original request or advice message. One exception to this rule is that the MDS will supply a new trace number in the 0820 message that it sends to **debit** processors. The trace number supplied in the 0820 message to **credit** customers will remain the same value as sent in the original 0800 message.

Note **In the Acquirer Reversal Advice/0420 message, an acquirer may submit a new trace number in DE 11; however, that is not recommended practice. The MDS will always send the trace number from the original Financial Transaction Request/0200 message to the issuer. The Acquirer Reversal Advice Response/0430 message to the acquirer will contain the same trace number as the Acquirer Reversal Advice/0420.**

DE 11 from the original transaction request is located in DE 90, subfield 2 of a reversal message.

Enhanced Delivery Option

In debit MasterCard Financial Advice/0220 clearing messages, the MDS distinguishes messages depending on whether they originate from the store-and-forward (SAF) file through the SAF process or directly from the main processing module, through the Enhanced Delivery option. The values for the STAN in these cases are:

- 999999 Store and Forward
- 999998 Enhanced Delivery

In the Financial Advice Response/0230 message, issuers must return the value received in DE 11 of the Financial Advice/0220 message.

DE 12—Time, Local Transaction

Time, Local Transaction (DE 12) is the local time at which the transaction takes place at the point of service.

Attribute

n-6; hhmmss

Usage

DE 12 is the local time that a cardholder transaction takes place, and should be the same value that is printed on the cardholder receipt, if possible. This time must be specified in local time zone units, and **not** in coordinated universal time (UTC) units.

For debit MasterCard clearings (Financial Transaction Advice/0220 messages), this will contain the MDS time that the store and forward message is sent, **not** the value set in the original pre-authorization.

Values

The value in this field must be a valid time.

DE 13—Date, Local Transaction

Date, Local Transaction (DE 13) is the local month and day on which the transaction takes place at the point of service.

Attribute

n-4; MMDD

Usage

DE 13 is the local date that a cardholder transaction takes place, and should be the same value printed on the cardholder receipt, if possible. This time must be specified in local time zone units, and **not** in coordinated universal time (UTC) units.

Values

The value in this field must be a valid date.

DE 14—Date, Expiration

The Date, Expiration (DE 14) specifies the year and month that a cardholder's bank card expires.

Attribute

n-4; YYMM

Usage

This data element may be present in manually-keyed debit MasterCard transactions, where allowed.

Values

The value in this field must be a valid date.

Note **For debit MasterCard, the MDS uses a default date of 4912 if not present in track data.**

DE 15—Date, Settlement

Date, Settlement (DE 15) is the date (month and day) that funds will be transferred between an acquirer and an issuer by the MDS.

Attribute

n-4; MMDD

Usage

This data element is present in Financial Transaction (02xx) and Reversal (04xx) messages that convey a settlement value. The exception is a Timeout-induced Reversal/0420 message; which does not contain DE 15. It contains the calendar date on which funds for a transaction will be settled.

A Timeout induced Reversal/0420 message does not contain DE 15, since the acquirer never received the Financial Transaction Request Response/0210 message providing the settlement date.

Values

This data element must contain a valid date.

DE 16—Date, Conversion

The Date, Conversion (DE 16) is the month and day that the conversion rate is effective to convert the transaction amount from the original currency into the currency of settlement, or to convert the transaction amount from the original currency into the cardholder billing currency.

Oct 2005

Attribute

n-4; MMDD

Usage

DE 16 indicates the effective date (month and day) of the Conversion Rate, Settlement (DE 9) and the Conversion Rate, Cardholder Billing (DE 10). DE 16 must be present whenever either of these data elements is present within a message.

Oct 2005

Values

The value in this field must be a valid date.

DE 17—Date, Capture

Date, Capture (DE 17) is the month and day the acquirer processed the transaction data.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-4; MMDD

Usage

The MasterCard® Debit Switch does not currently use this data element.

Values

The value in this field must be a valid date.

DE 18—Merchant Type

The Merchant Type (DE 18) code is the classification of the merchant's type of business or service.

Attribute

n-4

Usage

DE 18 code is a four-digit indicator used to classify a merchant's product or service, selected from a standard list of classification codes referred to as merchant category codes (MCCs). The MCC is included in Financial Transaction Request/0200 messages and Financial Transaction Advice/0220 completion messages.

The issuer has the option of whether or not to receive DE 18 in ATM cash transactions.

Values

Refer to the *Quick Reference Booklet* for a list of MCCs and transaction category codes (TCCs).

Processors should use the following codes for cash transactions:

- 6010—Bank teller over-the-counter (OTC) cash transaction
- 6011—ATM cash transaction - Processing Code (DE3) = 01, 30, or 40
- 6012—ATM purchase transaction

For Cirrus Purchase transactions (DE 3 = "00xx00"), the Merchant Type Code data element must contain a value of 6012. The value 6012 is not valid for Maestro POS transactions.

For ATM cash disbursements, this data element must contain a value of 6011. In these instances, the MDS, unless otherwise directed by the issuer's configuration file, removes DE 18 from the message before sending the message to the issuer.

MasterCard reserves the right to reject online financial request messages when the merchant category code (MCC) value in the Merchant Type field (DE 18) equals 0000. Acquirers should anticipate receiving a format error when an 0200/0210, 0220/0230 message contains a value of 0000 in DE 18.

For debit MasterCard and Maestro POS transactions, the *Quick Reference Booklet* provides a list of permissible values that members must use in the Merchant Type Code data element.

Note **The Merchant Type Code of 6012 is not valid for Maestro point of sale transactions.**

DE 19—Acquiring Institution Country Code

Acquiring Institution Country Code (DE 19) is the code of the country where the acquirer is located. Refer to the ISO 3166 specification for more information.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-3

Usage

The MasterCard® Debit Switch does not currently use this data element.

DE 20—Primary Account Number (PAN) Country Code

The PAN Country Code (DE 20) is a code identifying the country where the card issuer is located.

Attribute

n-3

Usage

The MDS retrieves this data from configured data of the issuer and provides it back to the acquirer in the Financial Transaction Request Response/0210 by the MDS when the acquirer uses the MDS enhanced issuer identification (EII) service.

DE 20 is required to be included within any message whenever the associated PAN (in Primary Account Number [DE 2] or Primary Account Number Extended [DE 34]) is present and begins with a "59" prefix. PANs beginning with a "59" prefix are **not** guaranteed to be unique without the use of this associated Country Code.

Values

Country codes must be selected from the numeric ISO Standard Country Codes listed in ISO 8583–1987 Appendix 2, ISO Country and Currency Codes.

DE 21—Forwarding Institution Country Code

Forwarding Institution Country Code (DE 21) is the code of the country where the forwarding institution is located.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-3

DE 22—Point of Service Entry Mode

The Point of Service Entry Mode (DE 22) consists of numeric codes that indicate the method used to enter the PAN into the terminal device and the PIN entry capability of that device.

Attribute

n-3

Usage

Note **On Behalf Service 02 or 03 will only be performed when the first two positions of DE 22 (PAN Entry Mode) are 05 or 07. PAN Entry mode of 81x is not supported for On Behalf Service 02 or 03.**

Table 4.11 describes the subfields in DE 22.

Table 4.11—Point of Service Entry Mode Subfields

Subfield	Position	Attribute	Value
POS Terminal PAN Entry Mode	1-2	n	Describes the method used for PAN entry to initiate a transaction. **00** PAN entry mode unknown **01** PAN manual entry **02** PAN auto-entry via magnetic stripe **03** PAN auto-entry via bar code reader **04** PAN auto-entry via optical character reader (OCR) **05** PAN auto-entry via integrated circuit card **06** PAN key entry **07** PAN auto-entry via contact less M/Chip **79** Chip card or chip-capable terminal was unable to process the transaction using the data on the chip or magnetic stripe, the PAN was entered manually *Or,* Acquirer is not certified to process the value 80 **80** PAN auto entry with magnetic stripe – the full track data has been read and transmitted in Track 1 data (DE 45) or Track 2 Data (DE 35) without alteration or truncation. To use this value, the acquirer must be qualified to use a value of 90. This mode is used as fallback to PAN auto-entry when **all** the conditions apply: • The physical Track 1 or Track 2 contains a Service Code of 2xx or 6xx • The terminal is an EMV type approved terminal enabled to accept MasterCard branded smart cards • The transaction cannot proceed as a smart card transaction and therefore proceeds as a magnetic stripe-read transaction. • Only chip certified acquirers can use the fallback indicator. • All fallback transactions must be authorized online **81** PAN manual entry via electronic commerce. **90** PAN auto-entry via magnetic stripe **91** PAN auto-entry with contactless Magnetic Stripe - The full track data has been read from the data on the card and transmitted within the authorization request in Track 2 Data (DE 35) or Track 1 (DE 45) without alteration or truncation.

Oct 2005

Oct 2005

Subfield	Position	Attribute	Value
POS Terminal PIN Entry Mode	3	n	Describes the capability of the terminal device to support/accept PIN entry **0** Unspecified or unknown **1** Terminal has PIN entry capability. **2** Terminal **does not** have PIN entry capability. **8** Terminal has PIN entry capability, but PIN pad is out of service. **9** PIN verified by terminal device.

[a] If the MDS creates any track 2 Data using track 1 Data, the processors must be prepared to accept any character that would have been present in the track-1.

For ATM transactions, the POS Terminal Entry Mode (position 1-2) should contain either 02 or 90. The MDS may overwrite any other value received from an acquirer with 02. Issuers should therefore receive only values 02x or 90x in this data element. Oct 2005

If acquirers submit Integrated Circuit Card (ICC) System-Related Data (DE 55) in the message, then DE 22, Subfield 1 must be "05" PAN Auto-Entry, "07" PAN Auto-Entry Via contactless M/Chip, or "81" E-Commerce. If DE 55 is present in the message, the MDS will decline the transaction if acquirers do not include 05, 07, or 81 in Subfield 1 of DE 22.

Special Mapping for Point-of-Sale transactions

Oct 2005

DE 22, subfield 1	Track 2 data present in inbound request message from the acquirer	MDS Action taken
01	Yes	• DE 22 and DE 35 will be sent as received.
01	No	• If track 1 data is not present, track 2 data will be built using the PAN (DE 2) and the expiration date (DE 14). If the expiration date is not available, the MDS builds track 2 using 4912 as the default expiration date: • If track 1 data is present, track 2 data will be built using track 1 data. • Message will be forwarded with DE 22, subfield 1, value of 01.

DE 22, subfield 1	Track 2 data present in inbound request message from the acquirer	MDS Action taken
02	Yes	• DE 22 and DE 35 will be sent as received.
02	No	• If track 1 data is not present, track 2 data will be built using the PAN (DE 2) and the expiration date (DE 14). If the expiration date is not available, the MDS builds track 2 using 4912 as the default expiration date. Message will be forwarded with DE 22, subfield 1, value of 01. • If track 1 data is present, track 2 data will be built using track 1 data. Message will be forwarded with DE 22, subfield 1, value of 02.
90	Yes	• DE 22 and DE 35 will be sent as received
90	No	• If track 1 data is not present, track 2 data will be built using the PAN (DE 2) and the expiration date (DE 14). If the expiration date is not available, the MDS builds track 2 using 4912 as the default expiration date. Message will be forwarded with DE 22, subfield 1, value of 01. • If track 1 data is present, track 2 data will be built using track 1 data. Message will be forwarded with DE 22, subfield 1, value or 02.

Oct 2005

If issuers are validating the CVC data in the discretionary data within track 2, these values should be used to determine when the CVC data is available.

DE 23—Card Sequence Number

The Card Sequence Number (DE 23) is used to distinguish among individual cards having the same Primary Account Number (DE 2) or Primary Account Number, Extended (DE 34).

Attribute

n-3

Usage

DE 23 must be present in all ICC transactions (where DE 22= '05x' or '07x') which include EMV-compliant ICC system related data (DE 55) and where the Application PAN Sequence Number (tag 5F34) is provided by the IC card to the terminal.

Valid values for Card Sequence Number are in the range 000-999.

Note **On Behalf Service 02 or 03 will only be performed when the first two positions of DE 22 (PAN Entry Mode) are 05 or 07. PAN Entry mode of 81x is not supported for On Behalf Service 02 or 03.**

DE 24—Network International Identifier

Network International Identifier identifies a single international network of card issuers.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-3

DE 25—Point of Service Condition Code (ISO)

Point of Service Condition Code (ISO) (DE 25) is an identification of the condition under which the transaction takes place at the point of service.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-2

Usage

All programs and services that the MasterCard® Debit Switch supports use Point of Service (POS) Data (DE 61) as MasterCard defined and implemented for use by all customers in all countries to specify the applicable conditions at the point of service.

DE 26—Point of Service (POS) PIN Capture Code

The POS PIN Capture Code (DE 26) is a code indicating the technique, maximum number of PIN characters, or both, that can be accepted by the point of service device used to construct the personal identification number (PIN) data.

Attribute

n-2

Usage

The point of service PIN capture code must be used to indicate the maximum number of PIN characters that the acquiring terminal device (ATM, POS terminal, etc.) is **capable** of accepting.

Note

If this field is not present in debit MasterCard transactions the MDS defaults to a value of 12.

The MDS does not use this data element to specify the number of PIN characters actually accepted by a point of service terminal device.

The MDS requires that this data element be included in 0200 Financial Transaction messages **only** when PIN Data (DE 52) is present **and** the maximum PIN character acceptance capability of the terminal is known to be **other than 12 digits**.

Values

Table 4.12 describes the subfields in DE 26.

Table 4.12—Point of Service (POS) PIN Capture Code Values

Code	Description
00–03	Invalid.
04–12	Indicates the maximum number of PIN characters that the terminal can accept.
13–99	Reserved.

DE 27—Authorization Identification Response Length

The Authorization Identification Response Length (DE 27) is the maximum length of the authorization response that the acquirer can accommodate. MasterCard expects the issuer, or its agent, to limit response to this length.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-1

DE 28—Amount, Transaction Fee

Amount, Transaction Fee (DE 28) is the fee charged (for example, by the acquirer) for transaction activity in the currency of the Amount, Transaction (DE 4).

Attribute

x+n-8

Usage

This data element may be present in a message whenever an online transaction fee is permitted by the operating rules of a bank card product.

The credit or debit indicator (the first position of the data element) applies to the message recipient. Within acquirer-generated message types, a D (debit) fee amount indicates that the fee is to be applied as a debit to the message recipient, the issuer (and therefore as a credit to the message originator, the acquirer).

Edits

This data element must contain valid numeric data with an appropriate indicator (C or D) in the first character position.

Note **For acquirers that are approved to levy ATM Access Charges, this data element must contain the access fee amount and this amount must also be added to the requested amount contained in Transaction Amount (DE 4).**

Acquirers must test with the MDS before implementation of this data element.

DE 29—Amount, Settlement Fee

Amount, Settlement Fee (DE 29) is the transferred fee between the acquirer and the issuer in the currency of Amount, Settlement (DE 5).

Attribute

x+n-8

Usage

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

DE 30—Amount, Transaction Processing Fee

In some transaction processing systems, Amount, Transaction Processing Fee (DE 30) can represent the switch fee for the handling and routing of messages in the currency of Amount, Transaction (DE 4).

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

x+n-8

DE 31—Amount, Settlement Processing Fee

Amount, Settlement Processing Fee (DE 31) is the fee charged by the MDS for handling and routing messages in U.S. dollars.

Attribute

x+n-8

Usage

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

DE 32—Acquiring Institution Identification Code

The Acquiring Institution Identification Code (DE 32) identifies the acquirer (for example, merchant bank) or its agent.

Attribute

n...11, LLVAR

Usage

The length of DE 32 is 9 positions. For processor systems connected to the MDS this data element contains either:

- The 9-digit Federal Reserve Routing and Transit (R & T) number of the institution that owns the terminal device.

  Or,

- The 9-digit ID pseudo-number assigned by MasterCard in accordance with applicable product rules.

For debit MasterCard, this code will contain 70xxxxxxC where:

- **70** Literal text
- **xxxxxx** Six digits of the acquiring/forwarding institution code
- **C** Check digit

For MasterCard Europe requests, this code will contain 99xxxxxxC, where:

- **99** Literal text
- **xxxxxx** Six digits of the acquiring/forwarding institution code
- **C** Check digit

For the MasterCard PIN for Credit request, this code will contain:

- **786** Literal text
- **xxxxx** Five digits for the group signin ID (GSI)
- **C** Check digit

DE 33—Forwarding Institution Identification Code

The Forwarding Institution Identification Code (DE 33) identifies the institution forwarding a Request or Advice message in an interchange system if not the same institution as specified in the Acquiring Institution Identification Code (DE 32).

Attribute

n...11; LLVAR

Usage

This data element **must** be present in all authorization (01xx), financial transaction (02xx), and reversal (04xx) messages. Routing of all these messages throughout the MDS is based upon the Acquirer ID Code (DE 32), the DE 33, and PAN (DE 2) information. It is important that all of these data elements are properly encoded to ensure accurate routing for both the original transaction and any subsequent reversals, chargebacks, adjustments, or representments.

Values

When present in a message, this data element must contain the processor ID.

Note

The processor ID is a ten-digit number of the form:

"9000000xxx"

where "xxx" is the 3-digit MDS Processor ID assigned by MasterCard.

This data element must always contain a length value of "10" followed by ten characters of numeric data in the associated variable-length data field.

DE 34—Primary Account Number, Extended

The Primary Account Number, Extended (DE 34) identifies a customer account or relationship. It is used only when a PAN is longer than 19 digits in length or contains special characters, and therefore cannot be placed into Primary Account Number (DE 2).

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

ns...28; LLVAR

DE 35—Track 2 Data

Track 2 Data (DE 35) is the information encoded on track 2 of the card magnetic stripe as defined in ISO 7813, **including field separators**, but excluding beginning and ending sentinels and Longitudinal Redundancy Check (LRC) characters as defined therein.

If any track 2 data must be created by the MDS using track 1 data, the processors must be prepared to accept any character that would have been present in the track 1.

For chip transactions, this data element carries data read from the chip as "Track 2 Equivalent Data" (EMV tag 57), which is then treated in the same way as magnetic stripe data. All ICCs issued by MasterCard members must support the EMV data object "Track 2 equivalent date" (EMV tag 57.) The issuer may vary the discretionary data between the magnetic stripe and the chip (for example; by not writing the CVC on the chip.)

Note **Since all ATMs must send full and unaltered track two data from the ATM to the issuer, MasterCard recommends that issuers validate the CVC1 data.**

Attribute

z...37; LLVAR

Usage

Whenever track 2 data is captured automatically at the point of service, this field must contain whatever is encoded on the magnetic stripe (track 2) of the card (regardless of whether or not the card has been properly encoded with information in accordance with ISO specifications).

The member's system must encode the following minimum data on track 2 as shown in Table 4.13.

Oct 2005

Table 4.13—Track 2 Minimum Data Subfields

Subfield	Attribute	Value
Start Sentinel	n-1	binary "1011" *(not transmitted)*
PAN	n…19	
Field Separator	ans-1	binary "1101" (see note)
Expiration Date	n-4	"YYMM" format
Service Code	ans-3	
Discretionary Data	ans…17	optional by issuer
End Sentinel	n-1	binary "1111" *(not transmitted)*
LRC	n-1	*(not transmitted)*

Oct 2005

Total maximum characters transmitted = 37

For manually keyed Maestro and debit MasterCard transactions, the MDS builds track 2 using the PAN (DE 2) and the Expiration Date (DE 14). If the Expiration Date is not available, the MDS uses 4912 as the default.

For debit MasterCard transactions where the acquirer sends (DE 45) Track 1 without (DE 35) Track 2, the MDS builds track 2 from the PAN, field separator, expiration date, service code, and first thirteen positions of the discretionary data.

Oct 2005

For electronic commerce (e-commerce) requests that do not contain track 2 data, the MDS builds track 2 using the PAN (DE 2), expiration date (DE 14) if available, and a Service Code subelement value of "101". E-commerce requests contain a POS entry mode (DE 22) value of "81x" or a value of "05x" with DE 48 subelements 40, 42, and 43 present.

For chip transactions, this data element carries data read from the chip as "Track 2 Equivalent Data" (EMV tag 57), which is then treated in the same way as magnetic stripe data. All ICCs issued by MasterCard members must support the EMV data object "Track 2 equivalent data" (EMV tag 57), although the issuer may vary the discretionary data between the magnetic stripe and the chip (for example, by not writing the CVC on the chip).

Note **The maximum length of the discretionary data is dependent upon the length of the PAN. For example, if the PAN has a length of 12 digits, the discretionary data may have a maximum length of 17. The overall length of DE 35 cannot be greater than 37.**

Values

This data element must contain the hexadecimal digits "0" through "9" and "D" or "=" (the "equal sign").

Note **The field separator character (binary "1101") is represented as the EBCDIC character "D." However, because many ATM and POS devices perform non-standard character translation while reading binary coded decimal (BCD)-encoded magnetic stripe data, the EBCDIC character "=" may also be used to represent the field separator character in magnetic stripe data forwarded to the MDS.**

If the MDS must create track 2 data from track 1 information, the issuer must be prepared to accept ANY character sent from the acquirer in track 1 data.

Track 2 data is not present in the 0220 messages for Maestro non-preauth or Cirrus transactions. It is present in the issuer bound 0220 message for:

Maestro "MS" preauthorization completion 0220 messages

Debit MasterCard "MD" completion 0220 messages, if the MDS receives DE 35 in the IPM 1240 record from GCMS

"Chip Clearing" 0220 messages, if present in the 0220 message from the acquirer.

DE 36—Track 3 Data

Track 3 Data (DE 36), as represented in the ISO 8583 specification, is the information encoded on track 3 of the card magnetic stripe as defined in ISO 4909-1986. This includes field separators, but excludes beginning and ending sentinels and LRC characters as defined therein.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

z...104; LLLVAR

DE 37—Retrieval Reference Number

The Retrieval Reference Number (DE 37) is a document reference number supplied by the system retaining the original source document of the transaction. It is used to assist in locating that source document or a copy thereof.

Attribute

an-12

Usage

This data element is reserved for use by the acquiring institution (or an affiliated merchant organization) for the purpose of recording a document retrieval reference number. The number can be used to locate original cardholder transaction information in subsequent retrieval request or any subsequent chargeback action.

The issuer in all corresponding response messages and in any subsequent chargeback action must return DE 37. The retrieval reference number should be printed on a customer's ATM or POS receipt.

Chip Data

This data element is mandatory for chip transactions (DE 22 = "05x" or "07x") and chip fallback transactions (DE 22 = "80x") as well as contactless magnetic stripe transactions (DE 22 = "91x").

MasterCard recommends the following format for DE 37 for chip transactions (contents are discretionary).

Table 4.14—Retrieval Reference Number Data Subfields

Subfield	Position	Attribute	Value
Transaction Date and Initiator Discretionary Data	1-7	an-7	The date (MMDD) the transaction is captured at the point-of-service terminal. If no discretionary data is included, the remaining 3 positions of this subfield should be zero-filled. This subfield is left-justified with trailing zeros.
Terminal Transaction Number	8-12	n-5	The Terminal Transaction Number – a sequential number, per terminal. Only numeric data may be present in this subfield. This subfield must contain a unique number that identifies the transaction with a specific POS terminal within a specific 24-hour time period. MasterCard recommends that this subfield contains the value of the Transaction Sequence Counter (EMV tag 9F41), if available. This subfield is right-justified with leading zeros.

DE 38—Authorization Identification Response

The Authorization Identification Response (DE 38) is a transaction response identification code assigned by the authorizing institution.

Attribute

an-6

Usage

The issuer processing system may use this data element for authorization tracking information. It is not mandatory for use in the MDS; however, MasterCard credit card issuers participating in the program via the Banknet network will provide this data element in approved MasterCard ATM transactions that are forwarded to the APS via the MDS.

This data element is required in "approved" debit MasterCard Financial Transaction Request Response/0210 messages.

Note **The Authorization Code may also be present in any "denied" Financial Transaction Request Response/0210 message.**

Values

Any valid alphanumeric character sequence may be used.

Debit MasterCard clearing 0220 messages will contain all six positions from the original authorization response.

The MDS Stand-In service will set this data element to a six-digit switch serial number.

Note **The debit MasterCard program does not support the MDS Stand-In service. Banknet performs MasterCard authorization Stand-In support to the debit MasterCard program. For more information regarding Stand-In Processing refer to the *MDS Programs and Services* manual.**

DE 39—Response Code

The Response Code (DE 39) is a code that defines the disposition of a message.

Attribute

an-2

Usage

Response codes indicate the disposition of a previous message or indicate approval or denial of a transaction. When an authorization is declined, the response code will indicate the reason for rejection and may indicate an action to be taken by the card acceptor or POS terminal device (for example, to capture the card).

This data element must be present in all response messages. In addition, it will also be present in Financial Transaction Advice (Stand-In)/0220 messages to indicate that DE 39 was utilized in the Financial Transaction Request Response (Stand-In)/0210 message response to the original Financial Transaction Request/0200 message.

For File Update Request Response/0312 messages, the response code will indicate whether the account record was successfully updated or the messages resulted in an error.

Note **The MDS will invoke Stand-In processing if a participating issuer (Stand-In) responds to a Financial Transaction Request/0200 message with response code 91 or response code 80. If the transaction meets established Stand-In parameters, the MDS will approve the transaction.**

Values

Table 4.15 provides a list of valid values for DE 39.

Table 4.15—Response Code Values

Code	Response	Description
Valid Response Codes for 0210 and 0220 messages		
00	Approve	Approved or completed successfully
01	Decline	Refer to card issuer *Valid for AVS and e-commerce only*
04	Capture	Capture Card
05	Decline	Do not honor
12	Decline	Invalid transaction *For MDS use only*
13	Decline	Invalid amount
14	Decline	Invalid PAN
15	Decline	Invalid issuer *For MDS use only*
30	Decline	Message format error *Debit MasterCard issuers may only use this code if the MDS sends a message indicating a format error*
41	Capture	Lost Card
43	Capture	Stolen Card
51	Decline	Non-sufficient funds
54	Decline	Expired card
55	Decline	Invalid PIN
57	Decline	Transaction not permitted to issuer or cardholder MasterCard recommends that chip issuers use response code 57 to indicate a chip cryptographic error.
58	Decline	Transaction not permitted to acquirer or terminal
61	Decline	Exceeds withdrawal limit
62	Decline	Restricted Card
63	Decline	Error in decryption of PIN block
65	Decline	Exceeds withdrawal count limits
75	Decline	Allowable number of PIN tries exceeded
76	Decline	Invalid “To” account specified
77	Decline	Invalid “From” account specified

Code	Response	Description
78	Decline	Invalid account specified *For MDS use only*
80	Decline	System not available
85	NA	Not declined *Valid only for "AVS Only" or e-commerce certificate requests*
91	Decline	Destination processor (CPS or INF) not available 1 MDS Generated: **Timeout**—Authorization Request sent to issuer processor and no response is received by MDS within required timers. **Issuer Processor Inoperative**—Issuer processor does not logically have an online status with the MDS. **Format Error**—Issuer processor returns invalid data in the authorization response message (0110/0210). 2 Issuer Generated: **Issuer Processor Inoperative**—An MDS direct connect customers' 'downstream issuer processor' is not responding.
92	Decline	Unable to route transaction
94	Decline	Duplicate transmission detected
96	Decline	System error
Valid Response Codes for 0290 messages		
30	—	Format error
68	—	Response received late The MDS forwards a response code "68" in the Financial Transaction Negative Acknowledge/0290 message in reply to a late 0210 message or other unsolicited response message.
80	—	System not available *Response codes from the acquirer Financial Transaction Advice/0220 and Acquirer reversal Advice/0420 messages are stored temporarily in a queue. When the MDS formulates the Financial Transaction Advice Response/0230 or Acquirer Reversal Advice Response/0430 message, the MDS returns the response code from the queue in the online message. If the acquirer sends a response code 80, 96, the MDS echoes it back to the acquirer.*

Oct 2005

Code	Response	Description
96	—	System error or system timer expired on expected CPS Message *Response codes from the acquirer's 0220 and 0420 messages are stored temporarily in a queue.* *The MDS forwards a response code "96" in the Financial Transaction Negative Acknowledgment/0290 message to the issuer when the transaction timer expires before a valid Financial Transaction Request Response/0210 transaction response is received.* *When the MDS formulates the 0230 or 0430 response message, the MDS returns the response code from the queue in the online message.* *If the acquirer sends a response code 80, 96, the MDS echoes it back to the acquirer.*
Valid Response Codes for 0230 messages		
00	—	Approved or completed successfully
30	—	Format error
80	—	System not available *Response codes from the acquirer's 0220 and 0420 messages are stored temporarily in a queue.* *When the MDS formulates the 0230 or 0430 response message, the MDS returns the response code from the queue in the online message* *If the acquirer sends a response code 80, 96, the MDS echoes it back to the acquirer.*
96	—	System error or system timer expired on expected CPS Message *Response codes from the acquirer's 0220 and 0420 messages are stored temporarily in a queue.* *When the MDS formulates the 0230 or 0430 response message, the MDS returns the response code from the queue in the online message.* *If the acquirer sends a response code 80, 96, the MDS echoes it back to the acquirer.*
Valid Response Codes for 0312 messages		
00	—	File update action completed successfully.
25	—	Unable to locate record on file (no action taken). *Valid for debit MasterCard only.*
27	—	File update field edit error. *Valid for debit MasterCard only.*
30	—	Format error
40	—	Requested function not supported. *Valid for debit MasterCard only.*
63	—	Security violation. *Valid for debit MasterCard only.*
80	—	Duplicate add; action not performed. *Valid for debit MasterCard only.*

Code	Response	Description
96	—	System error
Valid Response Codes for Timeout-Induced Reversal/0420 messages		
00	—	Required value
Valid Response Codes for 0430, 432 messages		
00	—	Approved or completed successfully
30	—	Format error
80	—	System not available *Response codes from the acquirer's 0220 and 0420 messages are stored temporarily in a queue.* *When the MDS formulates the 0230 or 0430 response message, the MDS returns the response code from the queue in the online message.* *If the acquirer sends a response code 80, 96 the MDS echoes it back to the acquirer.*
96	—	System error or system timer expired on expected CPS Message *Response codes from the acquirer's 0220 and 0420 messages are stored temporarily in a queue.* *When the MDS formulates the 0230 or 0430 response message, the MDS returns the response code from the queue in the online message.* *Therefore, if the acquirer sends a response code 80, 96, the MDS echoes it back to the acquirer.*
Valid Response Codes for 0630 messages (for reference only)		
00	—	Approved or completed successfully
30	—	Format error
80	—	System not available
96	—	System error or system timer expired on expected CPS Message
Valid Response Codes for 0810 messages		
00	—	Approved or completed successfully
96	—	System error or system timer expired on expected CPS Message

DE 40—Service Restriction Code

Service Restriction Code (DE 40) identifies geographic or service availability.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

an-3

DE 41—Card Acceptor Terminal Identification

The Card Acceptor Terminal Identification (DE 41) is a unique code identifying the terminal at the Card Acceptor Location. It is mandatory for initial requests, and must be returned, unchanged, in subsequent response message.

Attribute

ans-8

Usage

The MDS uses this data element to identify specific terminal devices of acquiring institutions or merchant point of service (POS) systems. The terminal owner assigns each terminal ID. It must be unique within the terminal-owning organization.

When this data element is included within an originating financial transaction (02xx) or reversal (04xx) message, it must be returned in the corresponding response message.

Values

The MDS does not perform edits on this data element.

DE 42—Card Acceptor Identification Code

The Card Acceptor Identification Code (DE 42) identifies the card acceptor, which defines the point of the transaction in both local and interchange environments.

Attribute

ans-15

Usage

The MDS uses DE 42 as a "merchant ID" to uniquely identify the merchant in a POS transaction. For a Maestro or debit MasterCard transaction, this data element must contain an alphanumeric merchant identifier.

Note **This data element is required in Maestro (U.S.) and debit MasterCard transactions and is forwarded to the issuer in Financial Transaction Request (Pre-Authorization)/0200 and Financial Transaction Advice/0220 messages. The MDS does not require Maestro International acquirers to use this data element.**

Values

The MDS does not perform edits on this data element.

DE 43—Card Acceptor Name and Location

The Card Acceptor Name and Location (DE 43) field contains the name and location of the card acceptor, which defines the point of service in both local and interchange environments.

Attribute

ans-40

Usage

The MDS uses this data element to satisfy national regulatory requirements concerning merchant identification within financial transaction (02xx) messages. It is a required data element within all financial transaction (02xx) request and advice messages.

Table 4.16 describes the subfields in DE 43.

Table 4.16—Card Acceptor Name and Location Subfields

Subfield	Position	Attribute	Value
1	1–22	ans-22	ATM owning institution and/or Terminal/Merchant address. This subfield cannot be blank.
2	23	ans-1	Delimiter (space)
3	24–36	ans-13	ATM or Merchant location city
4	37	ans-1	Delimiter (space)
5	38–40	a-3	For U.S.A and U.S. territories: ATM or Merchant location state code. This data must be right-justified, blank-filled, and in upper case. Or, For Canada and Canadian territories: ATM or Merchant location province code. This data must be right-justified, blank-filled, and in upper case. Or, For all other countries: ATM or Merchant location country code. This data must be right-justified, blank-filled, and in upper case.

Oct 2005

Members must select all State, Province, and Country Codes from the *Quick Reference Booklet*. If a country code is used, it must be the ISO 3-character alphabetic (not numeric) Country Code. If used, a State or Province Code should be right justified in this subfield with one leading blank space.

Delimiter fields must be the **blank** character. This is required because most cardholder statement rendering systems in operation today are not designed to perform printer output editing or formatting of the acquirer-supplied data contained within DE 43. The acquirer must pre-format DE 43 exactly as they want it printed on the cardholder's statement.

Members must not use all zeros, all low values (binary zeros), or all high values (binary F's) when formatting DE 43.

Oct 2005

DE 44—Additional Response Data

The MDS uses the Additional Response Data (DE 44) field to provide other supplemental data (for example, a telephone number) that may be required in response to an authorization or other type of transaction request.

Attribute

ans...25; LLVAR

Usage

This data element may be present in any response message when the Response Code (DE 39) is set to "30", indicating that a Format Error condition was detected in the preceding message. The first three bytes of DE 44, if present, will contain a 3-digit numeric value indicating the ISO data element number where the MDS encountered the format error.

Table 4.17—DE 44 Format for 0210 Responses when the Response Code (DE 39) is set to "30"

Subelement	Position	Attribute	Description
Data Element Length	1–2	n-2	Length of DE 44
Data Element in Error	3–5	n-3	Data element that failed the MDS edit
Subelement in Error	6–7	n-2	Subelement that failed the MDS edit
Error Description	8–25	an-18	Description of the error

When DE 44 exists in a File Update Request Response/0312, it contains the data element (in the File Update Request/0302 message) in which the error exists. If the error is in DE 120 of the 0302 message, the next three digits provide more specific information to identify the error condition. See

Table 4.18 for examples of an error in DE 120 for a file update message.

Table 4.18—DE 44 Sample Values in 0312 File Update Response

Value	Description
120001	The code has one of the following meanings: • PAN is not numeric • BIN in PAN is not numeric • BIN does not belong to message initiator • Check digit of PAN is incorrect • PAN is not on the Account file
120002	Entry reason is not one of the following: P, L, S, X, O, F, V, G, C, U
120005	PIN length not numeric or spaces
120006	Entry reason V and VIP limit is not numeric

For electronic commerce cardholder certificate requests, the issuer must send a telephone number in DE 44 of the 0210 message when the response code is equal to "01". If the response code is equal to "85," then the issuer must send delay date and time in DE 44 of the 0210 message. Table 4.19 describes these values in DE 44.

Table 4.19—DE 44 Values for 0210 Responses to Electronic Commerce Certificate Requests

Response Code DE 39	Attribute	Value
01	ans…25	DE 44 contains the telephone number for "call issuer" response codes.
85	ans…10	DE 44 contains the date and time after which a cardholder may reapply for a certificate.

Note **When DE 39 = "30", DE 44 is optional; DE 44 will not always be present to indicate the source location of a format error. If response code "30" is not generated by the MDS, DE 44 will not be present in the Financial Transaction Request Response/0210 message to the acquirer.**

DE 45—Track 1 Data

Track 1 Data (DE 45) is the information encoded on track 1 of a bankcard magnetic stripe as defined in ISO 7813, including field separators. However, this excludes beginning and ending sentinels and LRC characters, as defined therein.

Attribute

ans...79; LLVAR

Usage

DE 45 is used in point of service (POS) applications where the POS terminal equipment reads and transmits track 1 data in lieu of or in addition to the track 2 information encoded on the card magnetic stripe.

When it is received, as a part of a financial authorization request (debit MasterCard **only**), the MDS will build track 2 data (DE 35) from this data element to forward to the issuer. DE 45 will also be sent, when present.

If any track 2 data must be created by the MDS using track 1 data, the processors must be prepared to accept any character that would have been present in the track 1.

The acquirer must encode the following minimum data on DE 45 (Table 4.20):

Table 4.20—Track 1 Data Subfields

Subfield	Attribute	Value
Start Sentinel	n-1	*(not transmitted)*
Format Code	an-1	Literal character "B"
PAN	n…19	
Field Separator	ans-1	Binary 1101
Cardholder Name	ans…26	
Field Separator	ans-1	Binary 1101
Expiration Date	ans-4	"YYMM" format
Service Code	ans-3	

Subfield	Attribute	Value
Discretionary Data	ans…24	optional by issuer
End Sentinel	n-1	*(not transmitted)*
LRC	n-1	*(not transmitted)*

Note

The field separator character (binary "1101") is represented as the EBCDIC character "D." However, because many ATM and POS devices perform non-standard character translation while reading binary coded decimal (BCD)-encoded magnetic stripe data, the EBCDIC character "=" may also be used to represent the field separator character in magnetic stripe data forwarded to the MDS.

If the MDS must create track 2 data from track 1 information, the issuer must be prepared to accept ANY character sent from the acquirer in track 1 data.

DE 46—Additional Data (ISO)

Additional Data (ISO) (DE 46) provides data supplemental to that already conveyed in the specific data elements in the message.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

ans...999; LLLVAR

Usage

ISO reserves this data element for future definition and use.

DE 47—Additional Data (National)

Additional Data (National) (DE 47) is reserved for national organizations to define data unique to country applications

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

ans...999; LLLVAR

Usage

This data element is reserved for future definition and use by appropriate national standards organizations.

DE 48—Additional Data

Additional Data (DE 48) is reserved for use based on product type.

Attribute

ans...100; LLLVAR

Usage

Table 4.22 provides formats and descriptions for the subelements (SE) in DE 48. The subelement sequence does not have to be in the order of tag value. For example, subelement 11 does not have to precede subelement 40, which does not have to precede subelement 41, and so on.

DE 48 provides other supplemental data in a message when a specific ISO-designated data element is not available. It is a free-format, variable-length alphanumeric data element that may be used for multiple purposes. This data element's content may vary by program and service.

Note **The length of this data element has been limited to 100 bytes for practical operational and system constraints.**

Transaction Category Code (TCC)

If the first character in DE 48 is an **alphabetic** character, the MDS reads that character as the transaction category code (TCC). Refer to the *Quick Reference Booklet* for TCC values.

If the first character in DE 48 is a **blank** character, the MDS reads that character as no Transaction Category Code being present from the Acquirer. Therefore, following the rules below, the MDS forwards the message to the issuer with a space in the first character of DE 48 when required.

Inclusion of the TCC received from the acquirer in DE 48 of the 0200 request, into the outbound 0200 message sent by the MDS to the issuer, adheres to the following rules:

- For Cirrus ATM and Maestro ATM requests, any acquirer-supplied TCC is never passed to the issuer in the outbound message.
- For Maestro POS requests, if the TCC is **not** the only subelement in DE 48, the MDS **will** send the TCC to the issuer.

- For Maestro POS and Cirrus purchase requests, if the TCC is the **only** subelement contained in DE 48 from the acquirer, the MDS **will not** send the TCC to the issuer. If the TCC is accompanied by only Implied Decimal (SE 70), the MDS **will not** send the TCC to the issuer. If the TCC is accompanied by only Implied Decimal (SE 70) and Nation's ID (SE 41, code 11), the MDS **will** send the TCC to the issuer.
- For debit MasterCard transactions, regardless of whether the TCC is alone or with other subelements, the MDS **will** send the TCC to the issuer.

Table 4.21 illustrates the TCC message inclusion rules.

Table 4.21—TCC Message Inclusion Rules

Transaction Type	TCC	Nation's ID (SE 41)	Implied Dec (SE 70)	Other SEs	To Issuer
MS ATM	•	NA	NA	Any	No
MS ATM	•	NA	NA	None	No
CI ATM	•	NA	NA	Any	No
CI ATM	•	NA	NA	None	No
MS POS	•	NA	NA	Any	Yes
MS POS	•	NA	NA	None	No
CI Purchase	•	No	No	NA	No
CI Purchase	•	No	•	NA	No
CI Purchase	•	•	•	NA	Yes
CI Purchase	•	•	No	NA	Yes
MD	•	NA	NA	Any	Yes
MD	•	NA	NA	None	Yes

Subelement Encoding Scheme

Note **This is the encoding scheme if subelements exist in transactions.**

DE 48 consists of encoded subelements. Except for the TCC, each subelement begins with a two-byte tag **and** an associated two-byte length indicator. The subelements do not need to be in any particular order or sequence within DE 48. Members should be able to send and receive all subelements available within DE 48.

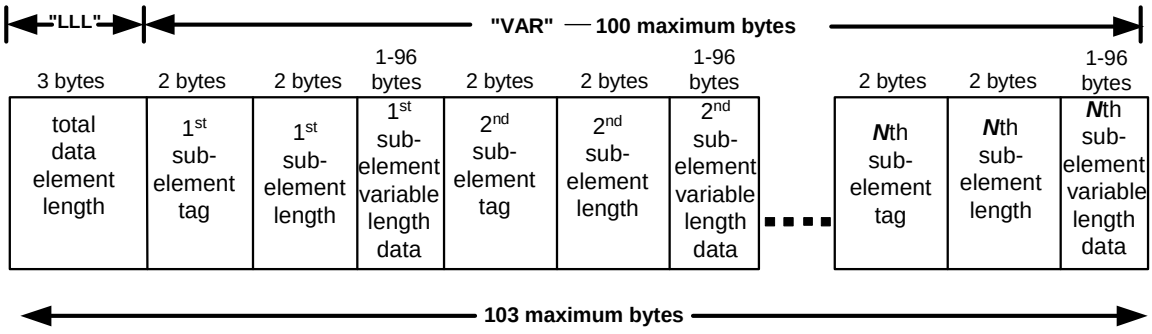
The first two bytes of each subelement must contain a tag in the range 00–99 to specify the type of DE 48 subelement. MDS universally defines values 00–69 for use by all programs and services. Values 70–99 are defined for use within individual programs and services only; individual program and service requirements dictate the use and content of the DE 48 subelement.

The second two bytes of each subelement must contain a length indicator in the range 00–99.

The overall length of the DE 48 is specified in its first three bytes (the "LLL" portion of the data element). The overall length of DE 48 is restricted to 100 bytes to accommodate practical operational limitations.

Figure 4.1 illustrates the construction of the entire DE 48 as well as subelements that may exist within it:

Figure 4.1—Subelements of DE 48



Subelement Descriptions

Table 4.22 provides formats and descriptions for DE 48 subelements.

Table 4.22—Additional Data Subelements

Subelement	Value
11	Processors must use the following subfield formatting for Network Management/0800 and 0810 messages used in Key Exchange Data Block sequences. During a key exchange, the key length being exchanged will be verified against the set-up for that particular encryption zone. The database will have an indicator for each zone (based on processor number, group sign-in (GSI)) to represent the key length required for that zone. For example, if the link is set-up of double-length keys and DE 48 subelement 11 contains single- or a triple-length key, the key exchange will be denied.

Subfield	Attribute	Value
Single DES Prefix	an-4	1138 (Constant value for MDS; indicates that this is a key exchange data block)
Triple DES Double Length Prefix	an-4	1154 (Constant value for MDS; indicates that this is a key exchange data block)
Triple DES Triple Length Prefix	an-4	1170
Key Class Identifier	an-2	PK (Pin Key Change)
Key Index Number	n-2	00 (Constant value for MDS)
Key Cycle Number	n-2	00 ... 99
Encrypted Key – Single DES	an-16	Hex characters 0 ... 9 and A ... F. Contains the hexadecimal representation of the 64 bits of the new encryption key, encrypted under the current communications key.
Encrypted Key – Triple DES Double Length	an-32	Hex characters 0 ... 9 and A ... F. Contains the hexadecimal representation of the 64 bits of the new encryption key, encrypted under the current communications key.
Encrypted Key – Triple DES Triple Length	an-48	Hex characters 0 ... 9 and A ... F. Contains the hexadecimal representation of the 64 bits of the new encryption key, encrypted under the current communications key.
Key Check Value	an-16	The key check value consists of the first four hexadecimal characters (0-9, A-F) of the calculated check value followed by spaces.

Subelement	Value
11	Processors must expect the following subfield formatting for Network Management/0820 message used in Key Exchange Data Block sequences. During a key exchange, the key length being exchanged will be verified against the set-up for that particular encryption zone. The database will have an indicator for each zone (based on processor number, group sign-in (GSI)) to represent the key length required for that zone. For example, if the link is set-up of double-length keys and DE 48 subelement 11 contains single- or a triple-length key, the key exchange will be denied.

Subfield	Attribute	Value
Single DES Prefix	an-4	1138 (Constant value for MDS; indicates that this is a key exchange data block)
Key Class Identifier	an-2	PK (Pin Key Change)
Key Index Number	n-2	00 (Constant value for MDS)
Key Cycle Number	n-2	00 ... 99
Encrypted DES Key	an-16	Blank-filled
Key Check Value	an-16	Blank-filled

Subelement	Value
40	For electronic commerce transactions, the acquirer can send the merchant certificate serial number and/or cardholder certificate serial number in subelement 40 of DE 48 of the 0100 and 0200 messages. The subelement designation has the format 40xx, where xx is the length of the data in the subelement. Should only be used for purchases and cardholder certificate information.

Subfield	Attribute	Value
Merchant/Cardholder Certificate Serial Number	2	40 contains UCAF (Universal Card Authentication Field) compliant information.
Subelement length	2	05…40
Contains one or both of the following subfields:		
01-Merchant Certificate Serial Number	2	01
Subfield 01 length	2	Length of Merchant Certificate Serial Number
Merchant Certificate Serial Number, if present	1-16	Must be binary data
02- Cardholder Certificate Serial Number	2	02
Subfield 02 length	2	Length of Cardholder Certificate Serial Number
Cardholder Certificate Serial Number, if present	1-16	Must be binary data

Oct 2005

Subelement	Value
41	At least one of the subfields must be present, to a maximum of ten subfields. The prefix of this subelement is 41xx, where xx is the length of the sublelement. These subfields contain authentication data used in the 0100 and 0200 electronic commerce cardholder certificate message. A few examples of the data stored in these subfields are password, date of birth, mother's maiden name, social security number, etc. NOTE: not all of the data shown can be sent at once because it would exceed the maximum length of DE 48.

Citizens ID for Maestro POS

For Maestro POS transactions, the MDS accepts a Financial Transaction Request/0200 message with data present in DE 48 subelement 41 subfield 11 (National ID) from participating acquirers. The MDS will not log the actual data; only the presence of the data will be recognized. Issuers have the option of echoing back the data. Citizen's ID has no effect on settlement, or financial value. This means no changes to adjustment/chargeback processing, no special fees/no ISIS impact. Citizen's ID does not apply to ATM transactions.

Subfield	Attribute
01 Password	1-26
02 Date of Birth (YYMMDD)	6
03 Card Validation Code 2	3
04 Cardholder's Name (as it appears on the card)	1-22
05 Street Address	1-20
06 Cardholder's City of Residence	1-13
07 Cardholder's State/ Country Code	3
08 Cardholder's Postal Code	1-10
09 Mother's Maiden Name	1-22
10 Social Security No.	9
11 National ID	1-20
12 Home Phone Number	1-20
13 Work Phone Number	1-20
14 Passport Number	1-20
15 Birth Date (YYYY/MM/DD)	10
16 Member Since (YY)	2
17 Photo Card Indicator(Y/N)	1
18 Country	1-20
19 Miscellaneous Authorization 1	1-30
20 Miscellaneous Authorization 2	1-30
21 Miscellaneous Authorization 3	1-30

Subelement	Value
42	For electronic commerce purchases, the acquirer can send a level of security in subelement 42 of DE 48 of the 0200 message. The prefix is 42xx, where xx has a value of "07". Subelement 42 must be present in all Authorization Request/0200 messages for electronic commerce transactions.

Subfield	Length	Value
Subelement identifier	2	42
Subelement data length	2	07
Subfield number (currently only one value = 01)	2	01
Subfield data length	2	03
Security level code	2	**11** UCAF encryption; cardholder certificate not used **12** UCAF encryption; cardholder certificate used **13** UCAF encryption; chip cryptogram used, cardholder certificate not used **14** UCAF encryption; chip cryptogram used, cardholder certificate used **21** channel encryption; cardholder certificate not used **23** channel encryption; chip cryptogram used, cardholder certificate not used **91** no security protocol; cardholder certificate not used
Universal Cardholder Authentication Field (UCAF) data status	1	**0** UCAF data collection is not supported at the merchant's Web site. **1** UCAF data collection is supported by the merchant but the UCAF data is not populated. (DE 48, SE 43 is not present) **2** UCAF data collection is supported by the merchant and the UCAF data is populated. (DE 48, SE 43 must be present)

Oct 2005

<table>
<tr><th>Subelement</th><th>Value</th></tr>
<tr><td>43</td><td>For electronic commerce purchases, this subelement can carry Universal Cardholder Authentication Field (UCAF) data. This subelement is only present when a UCAF-enabled merchant has collected authentication data from the cardholder and passed it to the acquirer for inclusion in the 0200 financial request or 0200 preauthorization request.
The format of the tag and length is 43xx, where xx is the length of the data that follows. The structure of these subfields is as follows:
<table>
<tr><th>Subfield</th><th>Length</th><th>Value</th></tr>
<tr><td>Subelement identifier</td><td>2</td><td>43</td></tr>
<tr><td>Subelement data length</td><td>2</td><td>Variable up to 40 bytes</td></tr>
<tr><td>UCAF data</td><td>32</td><td>Accountholder Authentication Value (AAV)</td></tr>
</table></td></tr>
<tr><td>70</td><td>The MDS supports subelement 70 (implied decimal) for participating processors. The MDS supports implied decimal exponent values for all currencies maintained by the MDS.
<table>
<tr><th>Subfield</th><th>Length</th><th>Value</th></tr>
<tr><td>Subelement Tag</td><td>2</td><td>70</td></tr>
<tr><td>Subelement Length</td><td>n-2</td><td>01</td></tr>
<tr><td>Subelement Value</td><td>n-1</td><td>0 through 3</td></tr>
</table></td></tr>
<tr><td>71</td><td>The On-Behalf (OB) Service Indicator identifies the type of on-behalf service performed on the transaction. The On Behalf Result 1 Indicator identifies the results of the Authorization Request Cryptogram (ARQC) validation and Authorization Response Cryptogram (ARPC) generation. The issuer can use these results in the authorization decision process. The issuer must echo this sub-element in the 0210 message. Sub-element 71 is not sent to the acquirer in any message.
The Account Holder Authentication Value (AAV) is part of the MasterCard SecureCode program that uses the Universal Cardholder Authentication Field (UCAF) data to validate cardholder identity. AAV uses sub-element 71 within the On Behalf services program infrastructure to accomplish account holder validation.
<table>
<tr><th>Subfield</th><th>Attribute</th><th>Value</th></tr>
<tr><td>Subelement Tag</td><td>n-2</td><td>71</td></tr>
<tr><td>Subelement Length</td><td>n-2</td><td>04</td></tr>
<tr><td>On Behalf Service Indicator</td><td>an-2</td><td>Contents of positions 1–2
01 Chip to Magnetic Stripe Conversion Service
02 M/Chip Cryptogram Pre-validation Service
03 M/Chip Cryptogram Validation in Stand-In Processing
05 MasterCard® SecureCode™ AAV Verification Service
06 MasterCard® SecureCode™ Dynamic AAV Validation Service</td></tr>
</table></td></tr>
</table>

Subelement	Value		
71	**Subfield**	**Attribute**	**Value**
	On Behalf Result 1	an-1	Contents of position 3 **C** Conversion of the M/Chip transaction to a magnetic stripe transaction was completed or AAV process completed **G** Application Cryptogram is valid but not an ARQC, status of TVR/CVR unknown **I** Invalid—Application Cryptogram (AC) is incorrect, status of TVR/CVR unknown or invalid; possible result from AAV **T** Valid ARQC, TVR/CVR invalid **U** Unable to process—No check on Cryptogram, status of TVR/CVR unknown or unable to process; possible result from AAV **V** Valid ARQC, valid TVR/CVR or valid; possible result from AAV
	On Behalf Result 2	an-1	Contents of position 4 **C** Created: Authorization Reply Cryptogram (ARPC) and Authorization Response Code (ARC) were created. The ARPC and ARC are sent to the issuer in DE48 SE 72 of the 0200 message. This value will be "C" when DE 48 SE71 position 3 (the On Behalf Result 1) contains the value "T" or "V" **U** Unable to create: Authorization Response Cryptogram (ARPC) was not created. DE 48 SE 72 will not be sent to the issuer. DE 55 will not be sent to the acquirer in the 0210 message. This value will be "U" when DE 48 SE 71 position 3 (the On Behalf Result 1) contains the value "G", "I", or "U".

<table>
<tr><th>Subelement</th><th>Value</th></tr>
<tr><td>72</td><td>Issuer Chip Authentication Data contains the Authorization Response Cryptogram (ARPC) followed by the Authorization Response Code (ARC), which is normally found in the chip field identifier Tag 91. The Enhanced Service Provider (ESP) generates these values. Subelement 72 is not sent to the acquirer in any message.
<table>
<tr><th>Subfield</th><th>Attribute</th><th>Value</th></tr>
<tr><td>Subelement Tag</td><td>2</td><td>72</td></tr>
<tr><td>Subelement Length</td><td>n-2</td><td>LLVAR from 08 bytes up to 16 bytes</td></tr>
<tr><td>Subelement Value</td><td>b…16</td><td>If the issuer approves the transaction, the MDS moves the value from DE48 SE72 of the issuer originated 0210 message and passes it to the acquirer in DE 55 of the acquirer destined 0210 message.

If the issuer approves the transaction, but fails to send SE 72 in the 0210 message, the acquirer destined 0210 message will not contain DE 55.

If the issuer declines the transaction, but fails to send SE 72 in the 0210 message, the MDS sends the ARPC followed by the ARC (chip field identifier Tag 91) in DE 55 of the acquirer 0210 message.

If the transaction is approved in MDS stand-in, the MDS sends the ARPC followed by the ARC (chip field identifier Tag 91) in DE 55 of the acquirer 0210 message. The MDS stores the mandatory subfields of the acquirer's original DE 55, and sends the issuer a 0220 stand-in advice message with the mandatory subfields in DE 55 (see DE 55 for details). The MDS sends the ARPC followed by the ARC in DE 48 SE 72 to the issuer. The 0220 message will also contain DE 48 SE 71.

If the transaction is declined in MDS stand-in, the MDS sends the ARPC followed by the ARC (chip field identifier Tag 91) in DE 55 of the acquirer 0210 message. If the issuer has chosen to receive MDS stand-in advice 0220 messages for denied transactions, the MDS stores the mandatory subfields of the acquirer's original DE 55, and sends the issuer a 0220 stand-in advice message with the mandatory subfields in DE 55 (see DE 55 for details). The MDS sends the ARPC followed by the ARC (chip field identifier Tag 91) in DE 48 SE 72 to the issuer. The 0220 message will also contain DE 48 SE 71.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Subelement</th><th>Value</th></tr>
<tr><td>76</td><td>Identifies that the transaction is a MasterCard electronic transaction. Indicates that the acquirer participates or does not participate in MasterCard Electronic.
<table>
<tr><th>Subfield</th><th>Attribute</th><th>Value</th></tr>
<tr><td>Transaction Subelement Identifier</td><td>n-2</td><td>76</td></tr>
<tr><td>Subelement Length</td><td>n-2</td><td>01</td></tr>
<tr><td>Identifies the participation level in the MasterCard Electronic program</td><td>a-1</td><td>C MasterCard only participant (not considered a MasterCard Electronic transaction).
E Acquirer and its merchant both participate in MasterCard Electronic (considered a MasterCard Electronic transaction).
U Unidentified acquirer. It is unknown if the acquirer is a MasterCard Electronic participant.</td></tr>
</table></td></tr>
<tr><td>82</td><td>Contains the AVS address verification request option code.
<table>
<tr><th>Subfield</th><th>Attribute</th><th>Value</th></tr>
<tr><td>Transaction Subelement Identifier</td><td>n-2</td><td>82</td></tr>
<tr><td>Subelement Length</td><td>n-2</td><td>02</td></tr>
<tr><td>AVS Option Code</td><td>n-2</td><td>51 AVS only
52 AVS and Authorization Request/0100</td></tr>
</table></td></tr>
</table>

Subelement	Value
83	Contains the AVS address verification response.

Subfield	Attribute	Value
Transaction Subelement Identifier	n-2	83
Subelement Length	n-2	01
AVS Result Code	an-1	**X** for U.S. addresses, all digits match, nine-digit ZIP code; for addresses outside the U.S., the postal code matches **Y** yes, all digits match, five-digit ZIP code **A** address matches, postal/ZIP code does not **W** for U.S. addresses, nine-digit ZIP code matches, address does not; for address outside the U.S., the postal code matches, address does not **Z** five-digit ZIP code matches, address does not **N** nothing matches **U** no data from issuer/Authorization System **R** retry, system unable to process **S** AVS currently not supported

84 Contains a merchant advice code to enable issuers to advise merchants of debit MasterCard account status, or to advise of system status. Used in conjunction with Authorization Request Response (Recurring Payment, Data Element 61, Subelement 4 = 4) 0210 decline messages.

Subfield	Attribute	Value
Transaction Subelement Tag	n-2	84
Subelement Length	n-2	02
Merchant Advice Code	an-2	**01** New account information available **02** Can not approve at this time, try again later **03** Do not try again

Subelement	Value
87	Contains the magnetic stripe/CVC error tag, provided by the issuer when applicable. Cirrus and Maestro products do not support the use of this subelement.

Subfield	Attribute	Value
Magnetic stripe/CVC error tag	n-2	Issuer provides this subelement when applicable. Value = 87.
Subelement Length	n-2	Value is 01; the subelement designation will be 87xx, where xx = 01
Code value	an-1	**M** CVC2 match (in issuer response) **N** CVC2 non-match (in issuer response) **P** CVC2 not processed (may be in acquirer request) **U** CVC2 issuer not registered (may be in acquirer request) **X** Invalid Magneprint **Y** CVC1 is invalid (in issuer response) **Z** CVC1 and Magneprint are invalid (in issuer response)

Subelement	Value
88	Contains the magnetic stripe/CVC error tag, provided by the issuer when applicable. Cirrus and Maestro products do not support the use of this subelement.

Subfield	Attribute	Value
Magnetic stripe/CVC error tag	n-2	Authorization System provides this subelement when applicable. Value = 88.
Subelement Length	n-2	Value is 01
Monitoring Status	an-1	Y Indicates that the Authorization System replaced DE 22, subfield 1, value 90 or 91 with the value 02, meaning that the acquirer submitting the transaction is monitoring status for CVC processing.

<table>
<tr><th>Subelement</th><th>Value</th></tr>
<tr><td>89</td><td>Contains the magnetic stripe/CVC error tag provided by the issuer when applicable. Cirrus and Maestro products do not support the use of this subelement.
<table>
<tr><th>Subfield</th><th>Attribute</th><th>Value</th></tr>
<tr><td>Magnetic stripe/CVC error tag</td><td>n-2</td><td>Authorization System provides this subelement when applicable. Value = 89.</td></tr>
<tr><td>Subelement Length</td><td>n-2</td><td>Value is 01</td></tr>
<tr><td>Data/Code Indicators</td><td>an-1</td><td>The following codes indicate track data, POS data, or TCC errors:
A track 1 or track 2 not present in the message
B track 1 and track 2 present in the message
C PAN (DE 2) not equal in track data
D Expiration Date (DE 14) not equal in track data
E service code invalid in track data
F field separator(s) invalid in track data
G a field within the track data exceeds maximum length
H TCC (in DE 48) is T
I POS customer presence indicator (DE 61, position 4) is 1, 2, 3, 4, or 5
J POS card presence indicator (DE 61, position 5) is 1</td></tr>
</table></td></tr>
<tr><td>90</td><td>Contains an indication of cardholder participation in the MasterCard Travel Industries Premier Service (TIPS).
<table>
<tr><th>Subfield</th><th>Attribute</th><th>Value</th></tr>
<tr><td>TIPS Tag</td><td>n-2</td><td>90</td></tr>
<tr><td>Subelement Length</td><td>n-2</td><td>Value is 01</td></tr>
<tr><td>Enrolled Program</td><td>An-1</td><td>P Indicates the request is from a cardholder enrolled in a merchant preferred customer program, and magnetic stripe data may be absent.</td></tr>
</table></td></tr>
<tr><td>92</td><td>Contains the CVC 2 value from the signature panel of the card when applicable.
<table>
<tr><th>Subfield</th><th>Attribute</th><th>Value</th></tr>
<tr><td>CVC2 Tag</td><td>n-2</td><td>Value = 92</td></tr>
<tr><td>Subelement Length</td><td>n-2</td><td>Value = 03</td></tr>
<tr><td>CVC1 value</td><td>n-3</td><td>The value for CVC2 sent in the request.</td></tr>
</table></td></tr>
</table>

Subelement	Value		
93	Contains the airline ticket number information.		
	Subfield	**Attribute**	**Value**
	T&E Tag	n-2	Value = 93
	Subelement Length	n-2	Value is variable up to 15. Current value is fixed at 15.
	Ticket no.	ans-15	Ticket number.
95	This subelement indicates participation in a particular program or service established between issuers and merchants.		
	Subfield	**Attribute**	**Value**
	Promotion Tag	n-2	95
	Subelement Length	n-2	Value = 06
	Surcharge Free Alliance	an-6	**Y** Prefix participates in Surcharge Free Alliance. This field must be left justified and blank filled.
98	MasterCard Corporate Fleet Card® ID/Driver Number, used to enable the corporate customer to verify the user of the card, and to provide more detailed reporting.		
	Subfield	**Attribute**	**Value**
	Tag	n-2	Value = 98
	ID/Driver Number	n-6	MasterCard Corporate Fleet Card® ID/driver number
99	MasterCard Corporate Fleet Card® Vehicle Number, used to enable the corporate customer to verify the user of the card, and to provide more detailed reporting.		
	Subfield	**Attribute**	**Value**
	Tag	n-2	Value = 99
	Vehicle Number	ans-15	MasterCard Corporate Fleet Card® vehicle number

Note

Registered issuers should note that if an acquirer transmits both CVC1 and CVC2 data, CVC1 processing takes precedence over CVC2 processing.

If the CVC1 value is incorrect, registered issuers should respond with a value of Y (incorrect CVC1) in subelement 87 without validating the CVC2 value. However, if the CVC1 value is correct, then registered issuers must validate the CVC2 and send the appropriate response to the acquirer.

DE 49—Currency Code, Transaction

The Currency Code, Transaction (DE 49) is the local currency of the acquirer or source location of the transaction. The MDS uses it to specify the currency used in Amount, Transaction (DE 4).

Attribute

n-3

Usage

This data element is mandatory whenever DE 4 is present in a message.

Values

Acquirers must select all currency codes from the numeric ISO Standard Currency Codes provided in the *Quick Reference Booklet*. Members must not use alpha currency codes.

DE 50—Currency Code, Settlement

The Currency Code, Settlement (DE 50) is the code defining the currency of Amount, Settlement (DE 5).

Attribute

n-3

Usage

This data element is mandatory whenever DE 5 is present in a message. For transactions where the MDS performs automatic currency conversion, the MDS automatically inserts this data element into the message.

When this field is present in a message, Conversion Rate, Settlement (DE 9) and Date, Conversion (DE 16) must also be present.

Values

The data element value of 840 is populated by the MDS except for an ISIS transaction where the value will equal the ISIS intra-country currency code.

DE 51—Currency Code, Cardholder Billing

The Currency Code, Cardholder Billing (DE 51) is the code defining the currency of Amount, Cardholder Billing (DE 6), Amount, ICCR (DE 8), and Amount, Currency Conversion Assessment (DE 111).

Oct 2005

Attribute

n-3

Usage

This data element is mandatory whenever Amount, Cardholder Billing (DE 6) is present in a message. The MDS automatically inserts this data element into the message.

When this field is present in a message, Conversion Rate, Cardholder Billing (DE 10) and Date, Conversion (DE 6) must also be present.

DE 52—Personal Identification Number (PIN) Data

The Personal Identification Number (PIN) Data (DE 52) contains a number assigned to a cardholder intended to uniquely identify that cardholder at the point of interaction (POI).

Attribute

b-64

Usage

The MDS uses this data element to transmit a cardholder's PIN, in **encrypted form** for issuer verification or validation. It is required in all ATM Financial Transaction Request/0200 messages and in some POS Financial Transaction Request/0200 messages.

For chip transactions DE 52 must be supplied at online capable terminals when online PIN is the appropriate Cardholder Verification Method. Product rules define when this option is allowed. International ATM and international cash advance EMV transactions must always use online PIN. For chip transactions, DE 52 is formatted and encrypted for non-chip transactions.

Acquirers must encrypt all PINs using the procedures identified in Chapter 6 of this manual.

The MasterCard® Debit Switch (MDS) permits PINs from 4 to 12 characters in length. Regardless of the original PIN length, the encrypted PIN block is always 64 bits (8 bytes) in length.

Strict security requirements implemented within data communications with the MDS, mandate that PINs are never transmitted in the clear as character data. PINs must always be encrypted into a 64-bit Encrypted PIN block. PIN Data is never included in online 0220 store-and-forward or other bank card transaction messages.

If the MDS performs PIN validation or verification on behalf of an issuer, this data element will be turned off, unless the transaction is a balance inquiry, in which case the MDS will transmit the following binary value:

0000 0001 0000 0001 0000 0001 0000 0001 0000 0001 0000 0001 0000 0001 0000 0001

Note

A Banknet® telecommunications-connected 0100 member may elect not to receive this data element in balance inquiry messages. Contact your Implementation Representative for additional information.

DE 53—Security Related Control Information

As of the publication date of this document, the ISO 8583 organization has not determined the specific definition and usage requirements for Security Related Control Information (DE 53).

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-16

DE 54—Additional Amounts

Additional Amounts (DE 54) provides information for a maximum of six amounts and related account data for which specific data elements have not been defined.

Attribute

an...120; LLLVAR

Usage

DE 54 can return account balance information in a balance inquiry (0210) requests. It can also provide cash back information on a purchase with a cash back transaction. Table 4.23 describes the subelements of DE 54.

Account Balance Information

Use of DE 54 subfields is optional within other Authorization Response/0110 and Financial Transaction Response/0210 messages. When present, they can contain account balance information that the acquirer may print on transaction receipts for the benefit of the cardholder.

The terminal screen displays the account balance information on the receipt in the currency of the acquirer.

The MDS provides the account balance information in the Financial Transaction Response/0210 message in the issuer's currency. The MDS performs a currency conversion from the issuer's currency to the acquirer's currency. The MDS returns this in the Financial Transaction Response/0210 message to the acquirer.

Cash Back Processing

A "purchase with cash back" Financial Transaction Request/0200 requires the following:

- DE 3 Processing Code, positions 1 and 2 (Transaction Type) must be "00"
- DE 54 positions 1 and 2 (Account Type) must match what is present in DE 3 Processing Code, positions 3 and 4 (Account Type)
- DE 54 must contain the value 40 in positions 3 and 4 (Amount Type)

Table 4.23 illustrates the format for DE 54. The MDS will not return DE 54 to the acquirer if the content is cash back information.

Table 4.23—Additional Amounts Subfields

Subfield	Position	Attribute	Value
Account Type	1–2	n-2	**00** no account specified **10** savings account **20** checking account **30** credit card account
Amount Type	3–4	n-2	**01** Ledger Balance **02** Available Balance **40** Cash Back **90** Available Credit **91** Credit Limit
Currency Code	5–7	n-3	Valid numeric Currency Code selected from the *Quick Reference Booklet*.
Debit or Credit Indicator	8	a-1	**C** credit amount or positive balance **D** debit amount or negative balance
Amount	9–20	n-12	12 digits, right-justified with leading zeroes

Note

The MasterCard® Debit Switch (MDS) only uses two Additional Amount data subfields.

Acquirers not capable of printing/displaying negative balances should print/display a zero balance value.

DE 55—Integrated Circuit Card (ICC) System-Related Data

Integrated Circuit Card (ICC) System-Related Data (DE 55) contains chip data formatted in accordance with the MasterCard Europe-MasterCard-Visa (EMV) 2000 specifications. EMV uses Basic Encoding Rules (BER). (Reference the EMV 2000 specifications for further details regarding the coding of BER-TLV (Tag, Length, Value) data objects.)

Note **This data element is used only when the financial transaction card is equipped with an integrated circuit and when that mode is activated and selected by the cardholder for the transaction.**

Attribute

b…255; LLLVAR

Usage

The issuer and the payment application (on the chip) use Integrated Circuit Card (ICC) System related data (DE 55) in the Financial Transaction Request/0200 and Financial Transaction Request Response/0210 messages to communicate with each other.

DE 55 includes cryptogram information that only the issuer or issuer agent and the ICC card are able to use.

Note **If acquirers submit Integrated Circuit Card (ICC) System-Related Data (DE 55) in the message, then DE 22, Subfield 1 must be '05' PAN Auto-Entry or '07' PAN Auto-Entry Via contactless M/Chip, or 81 E-Commerce. If not, decline.**

Note **The MDS performs no edits on the data in DE 55; it passes the data from the acquirer to the issuer and from the issuer to the acquirer. The description of this data is intended to show relevant information from the EMV 2000 specification.**

The provided functionality is known as Online Mutual Authentication (OMA). The chip is able to authenticate itself to the issuer in the Financial Transaction Request/0200 and the issuer is able to authenticate itself to the chip in the Financial Transaction Response/0210 message.

After initial designation of the overall data-element length (LLL), the remaining binary data consists of a series of subelement tag-length-value (TLV) segments up to a total of 255 bytes. The subelement tags can be from one to two bytes long, which are followed by a one-byte designation of the length, and the subelement data, respectively.

OMA-Card Application Data is Financial Transaction Request/0200 messages inbound to an issuer and Financial Transaction Response/0210 messages outbound to an acquirer. DE 55 contains binary data that only the issuer or the issuer agent can process. The chip in a smart card uses it locally at a chip-capable terminal. The MDS does not edit the contents of this data element.

If DE 55 is present in a Financial Transaction Request/0200 message, the POS Entry Mode Code (DE 22) must equal 05x, 07x, or 81x. Otherwise, the MDS rejects the message with a format error.

DE 55 is mandatory in Financial Transaction Request/0200 messages that are related to a chip full grade transaction (transactions carrying chip data to the issuer).

Depending on issuer profile (chip grade or magnetic stripe grade) and ICC personalization, the issuer or issuer agent may send DE 55 in the Financial Transaction Request Response/0210 message. Refer to the M/Chip Functional Architecture for a definition and further details about chip full grade, chip grade and magnetic stripe grade issuers.

Table 4.24, Table 4.25, and Table 4.26 indicate the differences between the contents of DE 55 in the Financial Transaction Request/0200 message and the contents of DE 55 in the Financial Transaction Request Response/0210 message.

For debit MasterCard issuers, if the contents of DE 55 in the Financial Transaction Request Response/0210 message are the same as the contents of DE 55 in the Financial Transaction Request/0200 message, then the MDS will not pass DE 55 back to the acquirer in the Financial Transaction Request Response/0210 message. Also for debit MasterCard transactions, if the MDS sends DE 55 in the Financial Transaction Response/0210 message, DE 55 must have been present in the corresponding Financial Transaction Request/0200 message.

Note **On Behalf Service 02 or 03 will only be performed when the first two positions of DE 22 (PAN Entry Mode) are 05 or 07. PAN Entry mode of 81x is not supported for On Behalf Service 02 or 03.**

Required Subelements for DE 55 in a Financial Transaction Request/0200

Table 4.24 conveys current chip specification requirements for subelements in DE 55 for a Financial Transaction Request/0200. These subelements are considered mandatory.

Table 4.24—Required DE 55 Subelements in 0200 Message

Subelement Name	Tag Value [a]	Length [b]
Application Cryptogram (AC)	9F26	8
Cryptogram Information Data	9F27	1
Issuer Application Data (IAD) [c]	9F10	1–32
Unpredictable Number	9F37	4
Application Transaction Counter	9F36	2
Terminal Verification Result (TVR)	95	5
Transaction Date	9A	3
Transaction Type	9C	1
Transaction Amount or Amount Authorized	9F02	6
Transaction Currency Code	5F2A	2
Application Interchange Profile	82	2
Terminal Country Code	9F1A	2
Amount Other [d]	9F03	6

a Hexadecimal representation: two characters = one byte binary.

b This column shows the actual character length of the data for the subelement. The actual length designator in the TLV is the one-byte binary designation of the data that follows.

c The acquirer must provide this value if the corresponding data object (EMV tag 9F10) is provided by the card to the terminal

d When the product rules do not allow cashback, then 9F03 must be absent, or zero filled.

When the product rules allow cashback:

Cashback Amount - 9F03 will carry the cashback amount and this data element is mandatory

No Cashback Amount - The value of 9F03 will be zero, in which case 9F03 may be absent or present with a zero value

Optional Subelements for DE 55 in a Financial Transaction Request/0200

Table 4.25 conveys current smart specification requirements for subelements in DE 55 for a Financial Transaction Request/0200. These subelements are considered optional.

Table 4.25—Optional DE 55 Subelements in 0200 Message

Subelement Name	Tag Value	Length
Cardholder Verification Method (CVM) Results	9F34	3
Terminal Capabilities	9F33	3
Terminal Type	9F35	1
Interface Device (IFD) Serial Number	9F1E	8
Transaction Category Code	9F53	1
Dedicated File Name	84	5–16
Terminal Application Version Number	9F09	2
Transaction Sequence Counter	9F41	2–4

Oct 2005

Optional Subelements for DE 55 in a Financial Transaction Request Response/0210

Table 4.26 conveys current chip specification requirements for subelements in DE 55 for a Financial Transaction Request Response/0210. These subelements are optional.

Table 4.26—Optional DE 55 Subelement in 0210 Message

Subelement Description	Tag Value	Length
Issuer Script Template 1 and 2 (Allows the issuer to provide a command for transmission to the card; present if issuer sends commands to ICC; acquirer network must support a subfield length up to 127 bytes.) MasterCard allows one occurrence of the EMV tag 71 and/or EMV tag 72 in the Financial Transaction Request Response/0210 message.	71 and/or 72	1–127
Issuer Authentication Data (Provides data to be transmitted to the card for issuer authentication.)	91	8–16

Required Subelements for DE 55 in a Debit MasterCard Financial Transaction Advice/0220

For debit MasterCard completion messages (stemming from chip-based authorizations) acquired from the batch system and sent to the issuer in the form of Financial Transaction Advice/0220 messages, the MDS uses DE 55 for supplying transaction certificate chip data to the issuer.

Note

It is assumed that track 2 equivalent data (PAN, PAN Sequence Number, and Expiration Date) are already present in the clearing message.

Transaction certificate data is defined in the EMV 2000 specification, and consists of the mandatory subelements defined for the Financial Transaction Request/0200 in chapter 2.

DE 56—Reserved for ISO Use

Reserved for ISO Use (DE 56) is reserved for future definition and use.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

ans...999; LLLVAR

DE 57—Reserved for National Use

ISO reserved this data element for future definition and use.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

ans…999; LLLVAR

DE 58—Authorizing Agent Institution ID

This data element is the institution identifier of the card issuer.

Attribute

n...11; LLLVAR

Usage

For members using the enhanced issuer identification (EII) service, this data element contains the issuing processor's financial institution routing and transit number. The MDS retrieves this data from configured data of the issuer and supplies it to the IPS in the outbound Financial Transaction Request/0200 message and in any subsequent acquirer reversal advice sent to the issuer.

DE 59—Reserved for National Use

ISO reserved this data element for future definition and use.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

ans...999; LLLVAR

DE 60—Advice Reason Code

The MDS uses the Advice Reason Code (DE 60) to indicate the specific purpose of an advice message.

Attribute

ans...060; LLLVAR

Usage

DE 60 is present in all advice messages, with the exception of network management advices (08xx message types). The data element has one or more of the following subelements:

Table 4.27—Data Element 60 Advice Reason Structure

Subelement	Position	Description	Value
1	1–3	Advice Reason Code	This subfield is mandatory for all advice messages and indicates the general purpose of the advice message.
2	4–7	Advice Reason Detail Code	This subfield usage may be conditionally required; it provides additional, specific information as to the exact nature of the advice message.
3	8–60	Advice Reason Detail Text	This optional subfield contains textual information supplementary to the Advice Detail Code.

The value and meaning of the contents of the Advice Reason data element vary according to the advice message type (for example, 02xx, 04xx, or 06xx), card product type, and whether the advice message is inbound to or outbound from the MDS.

Table 4.28 displays the general values for subelements 1 and 2 based on message type for all products, though each code does not pertain to all products. To determine whether the processor or the MDS will populate DE 60, refer to the message flow descriptions and diagrams for advice messages in chapter 2.

Table 4.28—Data Element 60 Advice Reason Subelements 1 and 2

Message Type	Advice Reason Code	Advice Detail Code	Description
0220	200	–	Network Stand-In: issuer selected option
	201	–	Network Stand-In: IPS signed out
	202	–	Network Stand-In: IPS timed out
	203	–	Network Stand-In: IPS unavailable
	201	0000	Network Stand-In: IPS signed out; Valid ARQC, valid TVR/CVR
	202	0000	Network Stand-In: IPS timed out; Valid ARQC, valid TVR/CVR
	203	0000	Network Stand-In: IPS unavailable; Valid ARQC, valid TVR/CVR
	201	0032	Network Stand-In: IPS signed out; Invalid input data to ESP/Result Code '50' from ESP or ESP device timeout
	202	0032	Network Stand-In: IPS timed out; Invalid input data to ESP/Result Code '50' from ESP or ESP device timeout
	203	0032	Network Stand-In: IPS unavailable; Invalid input data to ESP/Result Code '50' from ESP or ESP device timeout
	201	0034	Network Stand-In: IPS signed out; Chip validation failed
	202	0034	Network Stand-In: IPS timed out; Chip validation failed
	203	0034	Network Stand-In: IPS unavailable; Chip validation failed
	201	0035	Network Stand-In: IPS signed out; TVR/CVR validation failed
	202	0035	Network Stand-In: IPS timed out; TVR/ VR validation failed
	203	0035	Network Stand-In: IPS unavailable; TVR/CVR validation failed
	201	0039	Network Stand-In: IPS signed out; Cryptogram not ARQC
	202	0039	Network Stand-In: IPS timed out; Cryptogram not ARQC
	203	0039	Network Stand-In: IPS unavailable; Cryptogram not ARQC
	201	0018	Network Stand-In: IPS signed out; preauthorization completion, zero completion/completion for an amount greater than amount originally requested
	202	0018	Network Stand-In: IPS timed out; preauthorization completion, zero completion/completion for an amount greater than amount originally requested
	203	0018	Network Stand-In: IPS unavailable; preauthorization completion, zero completion/completion for an amount greater than amount originally requested

Message Type	Advice Reason Code	Advice Detail Code	Description
0220	201	0010	Network Stand-In: IPS signed out; partial preauthorization completion
	202	0010	Network Stand-In: IPS timed out; partial preauthorization completion
	203	0010	Network Stand-In: IPS unavailable; partial preauthorization completion
	251	0010	APS approved transaction; card returned; partial dispense
	251	1010	APS approved transaction; card retained; partial dispense
	260	0091	Clear Chip
	280	–	APS approved transaction
	280	0000	Outbound from MDS, APS approved transaction
	290	–	APS approved transaction; pre-authorized by issuer
	291	–	APS approved transaction; network timeout
	293	–	APS approved transaction; APS system error
	Any of the advice reason codes for a 0220 message.	x2yy	Network Advice: Possible Duplicate As indicated by the 2 in the second position of the detail code, this 0220 message has been determined by the MDS to be a possible duplicate of a previous 0220 message. The reason code and the other positions of the detail code are from the original advice message: **x** card disposition of previous message, 1 = retain, 0 =return **yy** detail code (position 3, 4) of previous message If the Advice Detail Code of the original advice message is not present or contains zeroes, the Advice Detail Code of this possible duplicate message is “0200”.
	454	0000	Network advice, invalid data (generated by MDS only)
0420	400	–	Network advice: APS error; unable to deliver response
	400	0000	Late response from issuer
	401	0080	Network advice: APS error
	402	0090	Network advice: IPS timeout error not acceptable from acquirer
	450	0011	Zero dispense: card returned; no receipt issued
	450	1011	Zero dispense: card retained; no receipt issued
	450	0018	Zero dispense/Over dispense card returned; POI failure. For the Timeout-Induced Reversal/0420 message, this code indicates an 0210 timeout at the acquirer.
	450	1018	Zero dispense: card retained; POI failure

Message Type	Advice Reason Code	Advice Detail Code	Description
	450	0019	Zero dispense: card returned, POI timeout
0420	450	1019	Zero dispense: card retained; POI timeout
	450	0040	Zero dispense: card returned; cardholder timeout
	450	1040	Zero dispense: card retained; cardholder timeout
	451	0010	Partial dispense: card returned
	451	1010	Partial dispense: card retained
	453	0041	Financial transaction cancellation: card returned
	453	1041	Financial transaction cancellation: card retained
	454	–	APS unable to deliver response
	454	0000	Network advice, invalid data
	455	0090	APS timeout; card returned
	455	1090	APS timeout; card retained
	487	0005	Retrieval request: cardholder does not agree
	487	0021	Retrieval request: transaction not recognized
	487	0023	Retrieval request: need for personal records
	487	0041	Retrieval request: fraud investigation
	487	0042	Retrieval request: potential chargeback
	488	–	Fulfillment
	489	0001	Chargeback – Requested transaction information not received (debit MasterCard Only)
	489	0002	Chargeback – Requested/required item illegible or missing (debit MasterCard Only)
	489	0007	Chargeback – Warning bulletin file (debit MasterCard only)
	489	0008	Chargeback – Requested/required authorization not obtained (debit MasterCard only)
	489	0012	Chargeback – Account number not on file (debit MasterCard Only)
	489	0017	Chargeback – Cardholder dispute (ATM only)
	489	0030	Chargeback – Cardholder disputed amount (deposits only)
	489	0031	Chargeback – Transaction amount differs (debit MasterCard only)
	489	0034	Chargeback – Duplicate processing (debit MasterCard only)
	489	0035	Chargeback – Card not valid or expired (debit MasterCard only)

Message Type	Advice Reason Code	Advice Detail Code	Description
	489	0037	Chargeback – No cardholder authorization (debit MasterCard only)
0420	489	0040	Chargeback – Fraudulent processing of transactions (debit MasterCard only)
	489	0041	Chargeback – Canceled Recurring Transaction (debit MasterCard only)
	489	0042	Chargeback – Late presentment (debit MasterCard only)
	489	0046	Chargeback – Correct transaction currency code not provided (debit MasterCard only)
	489	0047	Chargeback – Exceeds floor limit—not authorized and fraudulent transaction (debit MasterCard only)
	489	0049	Chargeback – Questionable merchant activity (debit MasterCard only)
	489	0050	Chargeback – Credit posted as a purchase (debit MasterCard only)
	489	0053	Chargeback – Not as described (debit MasterCard only)
	489	0054	Chargeback – Cardholder dispute—not elsewhere classified (U.S. Region Only) (debit MasterCard only)
	489	0055	Chargeback – Nonreceipt of merchandise (debit MasterCard only)
	489	0057	Chargeback – Card-activated telephone transaction (debit MasterCard only)
	489	0059	Chargeback – Services not rendered (RS3 = ATM dispute) (debit MasterCard only)
	489	0060	Chargeback – Credit not processed (debit MasterCard only)
	489	0062	Chargeback – Counterfeit transaction magnetic stripe POS fraud (debit MasterCard only)
	489	0063	Chargeback – Cardholder does not recognize - potential fraud (debit MasterCard only)
	489	0071	Chargeback – Disputed Amount (POS only)
	489	0072	Chargeback – Credit Posted as Debit (POS only)
	489	0073	Chargeback – Duplicate Transaction (POS and ATM)
	489	0074	Chargeback – Missing or Illegible Signature (POS only)
	489	0075	Chargeback – Credit not Received (POS only)
	489	0076	Chargeback – Documentation not received on retrieval request (POS only)

Message Type	Advice Reason Code	Advice Detail Code	Description	
	489	0077	Chargeback – Cardholder Denies Transaction Finalized (POS only)	
	489	0078	Chargeback – Documentation not legible on retrieval request (POS only)	
	489	0079	Chargeback – Goods or services not delivered (e-commerce only)	
0420	490	0001	Arbitration chargeback – Requested transaction information not received (debit MasterCard only)	Oct 2005
	490	0002	Arbitration chargeback – Requested/required item illegible or missing (debit MasterCard only)	
	490	0003	Correction processed by the MDS to reverse a chargeback with fees	
	490	0004	Duplicate Transaction – Indicates two copies of a transaction were posted and this adjustment is backing out one of the transactions.	
	490	0006	Correction processed by the MDS to reverse an Arbitration chargeback with fees	Oct 2005
	490	0007	Correction processed by the MDS to reverse adjustment, chargeback or Arbitration chargeback	
	490	0010	Adjustment	
	490	0012	Arbitration chargeback – Account number not on file (debit MasterCard only)	Oct 2005
	490	0019	Reversal of a representment–no documentation fulfillment	
	490	0020	Adjustment–Returned Item (deposits only)	
	490	0024	Adjustment–Empty deposit envelope (deposits only)	
	490	0025	Adjustment–Error in addition (deposits only)	
	490	0026	Adjustment–Error in settlement (deposits only)	
	490	0027	Adjustment–Customer keyed wrong amount (deposits only)	
	490	0028	Adjustment–Non-cash item deposited (deposits only)	
	490	0029	Adjustment–Foreign/Counterfeit currency deposited (deposits only)	
	490	0031	Arbitration chargeback–Transaction amount differs (debit MasterCard only)	Oct 2005
	490	0034	Arbitration chargeback – Duplicate processing (debit MasterCard only)	
	490	0035	Arbitration chargeback – Card not valid or expired (debit MasterCard only)	

Oct 2005

Message Type	Advice Reason Code	Advice Detail Code	Description
	490	0037	Arbitration chargeback – No cardholder authorization (debit MasterCard only)
	490	0040	Arbitration chargeback – Fraudulent processing of transactions (debit MasterCard only)
	490	0041	Arbitration chargeback - Canceled Recurring Transaction (debit MasterCard only)
0420	490	0042	Arbitration chargeback – Late Arbitration chargeback (debit MasterCard only)
	490	0046	Arbitration chargeback – Correct transaction currency code not provided (debit MasterCard only)
	490	0047	Arbitration chargeback – Exceeds floor limit—not authorized and fraudulent transaction (debit MasterCard only)
	490	0049	Arbitration chargeback – Questionable merchant activity (debit MasterCard only)
	490	0050	Arbitration chargeback – Credit posted as a purchase (debit MasterCard only)
	490	0053	Arbitration chargeback – Not as described (debit MasterCard only)
	490	0054	Arbitration chargeback – Cardholder dispute—not elsewhere classified (U.S. Region only—debit MasterCard only)
	490	0055	Arbitration only – Non-receipt of merchandise (debit MasterCard only)
	490	0057	Arbitration only – Card-activated telephone transaction (debit MasterCard only)
	490	0059	Arbitration only – Services not rendered (RS3 = ATM dispute) (debit MasterCard only)
	490	0060	Arbitration only – Credit not processed (debit MasterCard only)
	490	0062	Arbitration only – Counterfeit transaction magnetic stripe POS fraud (debit MasterCard only)
	490	0063	Arbitration only – Cardholder does not recognize - potential fraud (debit MasterCard only)
	491	0001	Presentment - Requested transaction information not received (debit MasterCard only)
	491	0002	Presentment - Requested/required item illegible or missing (debit MasterCard only)
	491	0007	Presentment - Warning bulletin file (debit MasterCard only)

Message Type	Advice Reason Code	Advice Detail Code	Description
	491	0008	Presentment - Requested/required authorization not obtained (debit MasterCard only)
	491	0012	Presentment - Account number not on file (debit MasterCard only)
	491	0013	Representment
	491	0031	Presentment - Transaction amount differs (debit MasterCard only)
	491	0034	Presentment - Duplicate processing (debit MasterCard only)
0420	491	0035	Presentment - Card not valid or expired (debit MasterCard only)
	491	0037	Presentment - No cardholder authorization (debit MasterCard only)
	491	0040	Presentment - Fraudulent processing of transactions (debit MasterCard only)
	491	0041	Presentment - Canceled Recurring Transaction (debit MasterCard only)
	491	0042	Presentment - Late presentment (debit MasterCard only)
	491	0046	Presentment - Correct transaction currency code not provided (debit MasterCard only)
	491	0047	Presentment - Exceeds floor limit—not authorized and fraudulent transaction (debit MasterCard only)
	491	0049	Presentment - Questionable merchant activity (debit MasterCard only)
	491	0050	Presentment - Credit posted as a purchase (debit MasterCard only)
	491	0053	Presentment - Not as described (debit MasterCard only)
	491	0054	Presentment - Cardholder dispute—not elsewhere classified (U.S. Region Only) (debit MasterCard only)
	491	0055	Presentment - Nonreceipt of merchandise (debit MasterCard only)
	491	0057	Presentment - Card-activated telephone transaction (debit MasterCard only)
	491	0059	Presentment - Services not rendered (RS3 = ATM dispute) (debit MasterCard only)
	491	0060	Presentment - Credit not processed (debit MasterCard only)
	491	0062	Presentment - Counterfeit transaction magnetic stripe POS fraud (debit MasterCard only)
	491	0063	Presentment - Cardholder does not recognize - potential fraud (debit MasterCard only)
	491	0086	Invalid chargeback for IPM, dollar amount does not match original transaction

Message Type	Advice Reason Code	Advice Detail Code	Description
	491	0088	Invalid chargeback for IPM, rejection of adjustment due to a duplicate request
	491	0089	Invalid chargeback for IPM, adjustment over 180 days
	491	0099	Invalid chargeback for IPM, unable to locate transaction in Cirrus file
0420	Any of the advice reason codes for a 0420 message.	x2yy	Network Advice: Possible Duplicate As indicated by the 2 in the second position of the detail code, this 0420 message has been determined by the MDS to be a possible duplicate of a previous 0420 message. The reason code and the other positions of the detail code are from the original advice message: **x** card disposition of previous message, 1 = retain, 0 =return **yy** detail code (position 3, 4) of previous message If the Advice Detail Code of the original advice message is not present or contains zeroes, the Advice Detail Code of this possible duplicate message is "0200".
0422	487	0005	Retrieval request: cardholder does not agree
	487	0021	Retrieval request: transaction not recognized
	487	0023	Retrieval request: need for personal records
	487	0041	Retrieval request: fraud investigation
	487	0042	Retrieval request: potential chargeback
	488	–	Fulfillment
	489	0001	Chargeback - Requested transaction information not received (debit MasterCard only)
	489	0002	Chargeback - Requested/required item illegible or missing (debit MasterCard only)
	489	0007	Chargeback - Warning bulletin file (debit MasterCard only)
	489	0008	Chargeback - Requested/required authorization not obtained (debit MasterCard only)
	489	0012	Chargeback - Account number not on file (debit MasterCard only)
	489	0017	Chargeback - Cardholder dispute (ATM only)
	489	0030	Chargeback – Cardholder disputed amount (deposits only)
	489	0031	Chargeback - Transaction amount differs (debit MasterCard only)
	489	0034	Chargeback -Duplicate processing (debit MasterCard only)
	489	0035	Chargeback - Card not valid or expired (debit MasterCard only)

Message Type	Advice Reason Code	Advice Detail Code	Description
	489	0037	Chargeback - No cardholder authorization (debit MasterCard only)
	489	0040	Chargeback - Fraudulent processing of transactions (debit MasterCard only)
	489	0041	Chargeback - Canceled Recurring Transaction (debit MasterCard only)
0422	489	0042	Chargeback - Late presentment (debit MasterCard only)
	489	0046	Chargeback - Correct transaction currency code not provided (debit MasterCard only)
	489	0047	Chargeback - Exceeds floor limit—not authorized and fraudulent transaction (debit MasterCard only)
	489	0049	Chargeback - Questionable merchant activity (debit MasterCard only)
	489	0050	Chargeback - Credit posted as a purchase (debit MasterCard only)
	489	0053	Chargeback - Not as described (debit MasterCard only)
	489	0054	Chargeback - Cardholder dispute—not elsewhere classified (U.S. Region Only) (debit MasterCard only)
	489	0055	Chargeback - Nonreceipt of merchandise (debit MasterCard only)
	489	0057	Chargeback - Card-activated telephone transaction (debit MasterCard only)
	489	0059	Chargeback - Services not rendered (RS3 = ATM dispute) (debit MasterCard only)
	489	0060	Chargeback - Credit not processed (debit MasterCard only)
	489	0062	Chargeback - Counterfeit transaction magnetic stripe POS fraud (debit MasterCard only)
	489	0063	Chargeback - Cardholder does not recognize - potential fraud (debit MasterCard only)
	489	0070	Chargeback -- Chip Liability Shift (POS and ATM)
	489	0071	Chargeback - Disputed Amount (POS only)
	489	0072	Chargeback - Credit Posted as Debit (POS only)
	489	0073	Chargeback - Duplicate Transaction (POS and ATM)
	489	0074	Chargeback - Missing or Illegible Signature (POS only)
	489	0075	Chargeback - Credit not Received (POS only)
	489	0076	Chargeback – Documentation not received on retrieval request (POS only) Chargeback

Oct 2005

Message Type	Advice Reason Code	Advice Detail Code	Description
	489	0077	Chargeback – Goods or services not delivered (e-commerce only)
	489	0078	Chargeback – Documentation not legible on retrieval request (POS only)
	489	0079	Chargeback – Goods or services not delivered (e-commerce only)
	490	0004	Duplicate Transaction
0422	490	0007	Correction processed by the MDS to reverse adjustment, chargeback or representment
	490	0010	Adjustment
	490	0019	Reversal of a representment - no documentation fulfillment
	491	0002	Presentment - Requested/required item illegible or missing (debit MasterCard only)
	491	0007	Presentment - Warning bulletin file (debit MasterCard only)
	491	0008	Presentment - Requested/required authorization not obtained (debit MasterCard only)
	491	0012	Presentment - Account number not on file (debit MasterCard only)
	491	0013	Representment
	491	0031	Presentment - Transaction amount differs (debit MasterCard only)
	491	0034	Presentment -Duplicate processing (debit MasterCard only)
	491	0035	Presentment - Card not valid or expired (debit MasterCard only)
	491	0037	Presentment - No cardholder authorization (debit MasterCard only)
	491	0040	Presentment - Fraudulent processing of transactions (debit MasterCard only)
	491	0041	Presentment - Canceled Recurring Transaction (debit MasterCard only)
	491	0042	Presentment - Late presentment (debit MasterCard only)
	491	0046	Presentment - Correct transaction currency code not provided (debit MasterCard only)
	491	0047	Presentment - Exceeds floor limit—not authorized and fraudulent transaction (debit MasterCard only)
	491	0049	Presentment - Questionable merchant activity (debit MasterCard only)
	491	0050	Presentment - Credit posted as a purchase (debit MasterCard only)
	491	0053	Presentment - Not as described (debit MasterCard only)

Message Type	Advice Reason Code	Advice Detail Code	Description
	491	0054	Presentment - Cardholder dispute—not elsewhere classified (U.S. Region Only) (debit MasterCard only)
	491	0055	Presentment - Nonreceipt of merchandise (debit MasterCard only)
	491	0057	Presentment - Card-activated telephone transaction (debit MasterCard only)
0422	491	0059	Presentment - Services not rendered (RS3 = ATM dispute) (debit MasterCard only)
	491	0060	Presentment - Credit not processed (debit MasterCard only)
	491	0062	Presentment - Counterfeit transaction magnetic stripe POS fraud (debit MasterCard only)
	491	0063	Presentment - Cardholder does not recognize - potential fraud (debit MasterCard only)
	491	0086	Invalid chargeback for IPM, dollar amount does not match original transaction
	491	0088	Invalid chargeback for IPM, rejection of adjustment due to a duplicate request
	491	0089	Invalid chargeback for IPM, adjustment over 180 days
	491	0099	Invalid chargeback for IPM, unable to locate transaction in Cirrus file
	Any of the advice reason codes for a 0422 message.	x2yy	Network Advice: Possible Duplicate As indicated by the 2 in the second position of the detail code, this 0422 message has been determined by the MDS to be a possible duplicate of a previous 0422 message. The reason code and the other positions of the detail code are from the original advice message: **x** disposition of previous message, 1 = retain, 0 =return **yy** detail code (position 3, 4) of previous message If the Advice Detail Code of the original advice message is not present or contains zeroes, the Advice Detail Code of this possible duplicate message is “0200”.
0620	600	–	Message unreadable/indecipherable/contains invalid data; (Advice Detail Code field MAY contain bit map number of data element where message scanning was aborted)
	601	–	Retrieval Request (Not used by MDS)
	602	–	Fulfillment notification (Not used by MDS)
	603	–	Message unreadable/indecipherable/contains invalid data
	603	0091	Duplicate Transaction

Message Type	Advice Reason Code	Advice Detail Code	Description
0644	650	6904	Message not dispatched from remote MIP
	650	6905	Message not dispatched to remote MIP
	650	6906	Message not delivered to remote MIP
	650	6907	Message not delivered from remote MIP
0644	650	6908	No confirmation 0210 message was delivered to the remote MIP

Note

For debit MasterCard transactions, 04xx message types, a number of additional advice detail codes are valid. Please refer to the *Chargeback Guide* for a listing of valid values.

Subelement 2 Usage Notes

The advice detail code (SE 2) description above has certain special meanings and the code has some special applications as indicated below:

In the column for Advice Detail Code, a hyphen indicates no data will be present in subelement 2.

The first two digits of subelement 2 Advice Detail Code are normally "00"; common practice for acquirers designating "card retained" in an inbound 0420 reversal is to use "10" in these positions.

The MDS has a facility for determining whether an inbound exception advice is a possible duplicate. When positions 4 and 5 of DE 60 (positions 1 and 2 of SE 2) in an exception message outbound from the MDS have the value "20", this indicates the advice is a possible duplicate.

Note

For deposit transactions, issuers can only process a chargeback if the acquirer first processed an adjustment. Issuers cannot process a chargeback against the original transaction. The interchange fees will not be returned to the issuer.

Subelement 3 Usage Notes

A debit MasterCard issuer must provide subelement 3, as defined in Table 4.29, when sending an online exception (chargeback) Issuer Reversal Advice/0422 message to the MDS through the issuer's online facility.

Table 4.29—DE 60, SE 3 for Debit MasterCard 0422 from Issuer

DE 60 Position	Subfield Name and Values
8	Usage Code **1** Issuer disputing initial presentment **2** Acquirer sending a second presentment **3** Arbitration chargeback
9	Documentation Indicator **Blank** No documentation **1** Documentation will follow **2** Invalid ARN in prior chargeback, no documentation required or received **3** Invalid ARN in prior chargeback, documentation received **4** Non-receipt of required documentation
10-11	Condition Code, reference only, generated by the MDS to batch
12-49	Message Block, optional message text
50-51	Chargeback Flag, reference only, generated by the MDS to batch
52-53	Future use – space fill
54	Reject Code – space fill
55-60	Future use – space fill

Maestro and Cirrus processors can provide the contact information (Table 4.30) to the MDS in the online exception 042x advice DE 60 SE 3. Similar information may be sent from the processor's terminal entry on a NICS exception advice.

Table 4.30—DE 60 SE 3, Advice Reason Text (Maestro and Cirrus)

Subelement	Position	Description
3	8-28	Contact name
	29-44	Contact phone
	45-60	Contact fax

DE 61—Point of Service (POS) Data

The MDS uses the Point of Service (POS) Data (DE 61) to indicate the specific conditions present at the point of service (POS) at the time that a transaction takes place.

Attribute

ans...026; LLLVAR

Usage

Issuers of debit MasterCard require the 26 characters of DE 61 in the request message, and acquirers must supply this information in the request message in accordance with Table 4.30. Maestro and Cirrus issuers must be prepared to accept the full 26 characters of DE 61 in the request message. Acquirers should supply at least the first 11 bytes of this information in the request message in accordance with Table 4.30.

Note

The MDS does not perform edits on the contents of this data element in the Financial Transaction Request/0200 message it receives from the acquirer. The MDS passes the data element contents to the issuer in the outbound request message to the issuer.

The Financial Transaction Request/0200 message must contain a value of "4" in position 7 of DE 61 for Debit MasterCard and Maestro preauthorization transactions. The Financial Transaction Advice/0220 message will contain a value of '0' in position 7 of DE 61 for a Debit MasterCard preauthorization completion.

Debit MasterCard force post messages may only contain the first ten positions described below. The MDS populates the first nine positions with 010001000. The 10th position (CAT level) value is a one-digit translation of the three-character code obtained from the POS Data Terminal Type field of the batch GCMS integrated product message (IPM) record.

Table 4.31 describes the subfields in DE 61.

Table 4.31—Point of Service (POS) Data Subfields

Subfield	Position	Attribute	Value	
POS Terminal Attendance Indicator	1	n-1	0	Attended terminal
			1	Unattended terminal
			2	No terminal used (voice/audio response unit [ARU] authorization)
			9	Unknown data not available (MDS Use Only)
POS Terminal Operator Indicator	2	n-1	No longer used—zero filled	
POS Terminal Location Indicator	3	n-1	0	On premises of card acceptor facility
			1	Off premises of card acceptor facility (remote location)
			2	On premises of cardholder (home PC)
			3	No terminal used
			6	Off cardholder premised, unattended (MDS Use Only)
			9	Unknown data not available (MDS Use Only)
POS Customer Presence Indicator	4	n-1	0	Customer present
			1	Cardholder not present, unspecified
			2	Cardholder not present, mail/facsimile order
			3	Cardholder not present, phone/ARU order
			4	Cardholder not present, recurring transaction
			5	Electronic order (home PC, Internet)
			9	Unknown data not available (MDS Use Only)
POS Card Presence Indicator	5	n-1	0	Card present
			1	Card not present
			9	Unknown data not available (MDS Use Only)
POS Card Retention Indicator	6	n-1	0	Terminal/operator does not have card capture capability
			1	Terminal/operator has card capture capability
			9	Unknown data not available (MDS Use Only)
POS Transaction Status Indicator	7	n-1	0	Normal request (original presentment)
			1	Merchant authorized
			3	Time Based Payment Authorization Request or CDC inquiry request
			4	Pre-authorization request
			5	Debit MasterCard Stand-In
			7	Purchase with Cash back

Oct 2005

Subfield	Position	Attribute	Value
POS Transaction Security Indicator	8	n-1	0 No security concern 1 Suspected fraud 2 Identification verified
POS Transaction Routing Indicator	9	n-1	0 Zero fill; field no longer used
Cardholder-Activated Terminal Level Indicator	10	n-1	0 Not a CAT transaction 1 Authorized Level 1 CAT: automated dispensing machine with PIN or ATM 2 Authorized Level 2 CAT: self service terminal 3 Authorized Level 3 CAT: limited amount terminal 4 Authorized Level 4 CAT: In-flight Commerce 5 Scrip device 6 Electronic Commerce Transactions 7 Authorized Level 7 CAT: transponder
POS Card Data Terminal Input Capability Indicator	11	n-1	0 Unknown 1 No terminal used 2 Magnetic stripe reader 3 Contact less M/Chip (Proximity Chip) 4 Contact less Magnetic Stripe (Proximity Chip) 5 Magnetic stripe reader and EMV specification compatible integrated circuit card (ICC) reader 6 Key entry only 7 Magnetic stripe reader and key entry 8 Magnetic stripe reader and key entry and EMV-compatible ICC reader 9 EMV compatible ICC reader
POS Authorization Life Cycle Indicator	12-13	n-2	Indicates the number of days pre-authorization stays in effect (ATM and Maestro POS transactions should use 01.)
POS Country Code Indicator	14-16	n-3	Indicates the country of the terminal location (use valid three digit ISO numeric country code)
POS Postal Code Indicator	17-26	ans-10	Indicates the geographic code of the terminal location (if data is unknown or unavailable, zero fill.)

DE 62—Intermediate Network Facility (INF) Data

Intermediate Network Facility (INF) Data (DE 62) is provided for use by acquiring network processors (CPS or INF) to contain acquiring network trace information that is useful for routing chargeback or adjustment transactions to the original acquiring institution.

Attribute

ans...50; LLLVAR

Usage

INF data is an optional data element within any originating Financial Transaction Request/0200 or Financial Transaction Advice/0220 message originated by an acquiring CPS or INF. Subsequently, this data element (if present within an original transaction) is returned without alteration in any chargeback or adjustment related to the original transaction.

This data element is provided to assist acquiring processor facilities directly-connected to the MDS. It allows these processors to maintain sufficient data within a message to facilitate online routing of chargebacks and adjustment messages without maintaining an online database of original transaction routing data.

Values

INF data is a free-format, variable length alphanumeric field that may be used to store unique acquiring processor ID codes, acquiring network linking data, or other information useful to processors in routing online chargeback and adjustment messages. The MDS does not edit or modify the field.

DE 63—Network Data

Network Data (DE 63) is a mandatory switch-generated data element composed of subelements that contain various descriptive and identifying attributes of the transaction.

Attribute

ans...044; LLLVAR

Usage

The MDS generates this data element for each originating message routed to the MDS. The receiver must retain and use this data element in any response or acknowledgment message associated with the originating request or advice message. The exception is a Timeout-Induced Reversal/0420 message; which does not contain DE 63.

Note **The MDS will supply a new Network Reference Number in DE 63 of the 0820 message it sends to debit processors. The Network Reference Number supplied in the 0820 message to credit customer will remain the same value as sent in the original 0800 message.**

The MDS determines the appropriate financial network code for all transactions routed through the MDS, based upon customer-established product configuration tables, customer parameter tables, and MDS routing priority tables.

Table 4.32 describes the subfields in DE 63.

Table 4.32—Network Data Subfields

Subfield	Position	Attribute	Value
Financial network code	1-2	a-2	Identifies the financial bank card product associated with the transaction. **MC** MasterCard **CI** Cirrus® **MS** Maestro® **MD** MasterCard® debit card **PL** Plus® **VI** VISA
Interchange rate indicator	3	n-1	Identifies the transaction as domestic (within the U.S.A. and Canada), International (Asia Pacific, Europe, Latin America and the Caribbean and Middle East/Africa), or Intra-country (within a country where an ISIS agreement is in effect). **0** U.S. and Canada Regions **1** Asia Pacific, Europe, Latin America and the Caribbean, and Middle East/Africa Regions **2** Intracountry (ISIS)
Network reference number	4-12	n-9	A unique transaction identification number (switch serial number) generated (or assigned) by the MDS.
Banknet reference number	13-21	an-9	A unique identifier assigned to debit MasterCard authorizations and is present in both Financial Transaction Request/0200 Authorization and Financial Transaction Advice/0220 Clearing messages. Only present in debit MasterCard transactions.
Acquirer's reference number	22-44	n-23	A unique identifier assigned by the acquirer of debit MasterCard transactions. Only present in debit MasterCard 0220 clearing messages.
GCMS Processing Date and Cycle Number	45-49	n-5	Contains the Global Clearing Management System's business processing date and cycle number (pds0158 subfield 5 and subfield 6 of the GCMS 1240 message). Only present in debit MasterCard 0220 advice messages (Valid value; mmdd# where # = cycle number)

Note **The issuer processor must use the switch serial number contained in this data element to match an online same day Acquirer Reversal Advice/0420 message and a Financial Transaction Acknowledgment/0290 message for issuer late response to the original Financial Transaction Request/0200 message.**

Online same day reversals contain the original switch serial number of the 0200 message. MDS generated (such as NICS™) exception items will be assigned a unique switch serial number.

The batch record will contain both switch serial numbers (the original switch serial number of the 0200 and the switch serial number of the NICS™ processed exception item).

The online reversal/04xx message will only contain the new switch serial number.

For debit MasterCard file updates, the Financial Request Response/0312 messages returning to the MDS from the Banknet Account Management Service (AMS) contain a unique Banknet identifier in DE 63.

For 0312 messages returned to the issuer by the MDS, the data conforms to Table 4.32.

In those 0312 messages, the following values are used:

- Financial network code = CI, MS, or MD
- Interchange rate indicator = 0 (U.S. and Canadian regions)
- Network reference identifier = Nine digits, generated by the internal MDS file update process for Cirrus or Maestro
- Banknet reference number = Nine alphanumeric characters, received from AMS by the MDS for debit MasterCard updates
- The acquirer reference number is not applicable to 0312 messages.

For MDS generated Network Management/08xx messages, the first three positions of DE 63 will contain the value CI0. For Acquirer or Issuer initiated Network Management/08xx messages, the MDS will overwrite the first three positions of DE 63 with the value CI0.

DE 64—Message Authentication Code (MAC)

Message Authentication Code (MAC) (DE 64) validates the source and the text of the message between the sender and the receiver.

The MDS reserves the last bit position within any bit map for DE 64. If the member uses authentication on a message, the final bit of the final bit map of that message indicates the MAC information. The final bit of all preceding bit maps shall contain 0; for example, there shall be only one DE 64 per message and that DE 64 must be the last data element of the message.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

b-64

DE 65—Bit Map, Extended

Bit map, Extended (DE 65) is a series of 64 bits used to identify the presence ("1") or absence ("0") of each data element in an extended [third] message segment.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

b-64

Usage

The MasterCard® Debit Switch defines only two message segments, the presence or absence of which is indicated by Primary and Secondary bit maps. DE 65 would indicate the presence of a "third" message segment, and must never be present in an MasterCard® Debit Switch message. The corresponding bit (number 65) must always be "0" in the Secondary Bit Map.

Refer to the Primary and Secondary Bit Maps subsection.

DE 66—Settlement Code

The Settlement Code (DE 66) is a code indicating the result of a reconciliation request.

Note **The MDS does not support this data element.**

Attribute

n-1

Usage

The MDS does not use this data element.

Values

Table 4.33 lists design values for the Settlement Code data element.

Table 4.33—Settlement Code Values

Code	Description
1	Reconciliation message totals balance.
2	Reconciliation message totals do not balance.
9	Reconciliation message received; no balancing performed.

DE 67—Extended Payment Code

Extended Payment Code (DE 67) indicates the number of months that the cardholder prefers to pay for an item (the item purchased during the course of this transaction), if permitted by the card issuer.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-2

DE 68—Receiving Institution Country Code

Receiving Institution Country Code (DE 68) is the code of the country where the receiving institution is located.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-3

DE 69—Settlement Institution Country Code

The Settlement Institution Country Code (DE 69) is the code of the country where the settlement institution is located.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-3

DE 70—Network Management Information Code

The MDS uses the Network Management Information Code (DE 70) to identify network status. The Customer Processing System may use Additional Data (DE 48) in conjunction with DE 70 to provide network status or control information.

Attribute

n-3

Usage

This data element indicates the specific classification and purpose of network management (08xx) messages. It must be present in all network management (08xx) messages.

Values

Table 4.34 lists all Network Management Information Codes valid on the MDS.

Table 4.34—Network Management Information Codes

Code	Description
060	Processor-initiated Store-and-Forward (SAF) session request
061	General sign-on by the processor to the MDS
062	General sign-off by the processor from the MDS
065	Issuer sign-off, directing the MDS to begin Stand-In processing for the issuer
066	Issuer sign-on, directing the MDS to cease Stand-In processing for the issuer
161	Encryption key change
162	Initiate Encryption Key Change (by processor)
270	Echo test
363	End-of-file (EOF) encountered for SAF traffic. SAF complete.

DE 71—Message Number

Message Number (DE 71) is a sequential, cyclic number the message initiator assigns to a message. The Message Number monitors the integrity of interchange.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-4

DE 72—Message Number Last

Message Number Last (DE 72) is a sequential, cyclic number the message initiator assigns to a message. The Message Number monitors the integrity of interchange.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-4

DE 73—Date, Action

Date, Action (DE 73) specifies the date (year, month, and day) of a future action. In addition, the member may use it as a static time such as a birth date.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-6; YYMMDD.

DE 74—Credits, Number

Credits, Number (DE 74) is the number of transactions the MDS processes as credits (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-10

DE 75—Credits, Reversal Number

Credits, Reversal Number (DE 75) is the number of transactions the MDS processes as credit reversals (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-10

DE 76—Debits, Number

Debits, Number (DE 76) is the number of transactions the MDS processes as debits (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-10

DE 77—Debits, Reversal Number

Debits, Reversal Number (DE 77) is the number of transactions the MDS processes as reversal debits (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-10

DE 78—Transfers, Number

Transfers, Number (DE 78) is the number of transactions the MDS processes as transfer transactions (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-10

DE 79—Transfers, Reversal Number

Transfers, Reversal Number (DE 79) is the number of transactions the MDS processes as transfer reversals (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-10

DE 80—Inquiries, Number

Inquiries, Number (DE 80) is the number of transactions the MDS processes as inquiries (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-10

DE 81—Authorizations, Number

Authorizations, Number (DE 81) is the number of transactions the MDS processes as Authorization Request/100 and Authorization Advice/0120 messages (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-10

DE 82—Credits, Processing Fee Amount

Credits, Processing Fee Amount (DE 82) is the amount the MDS processes as processing fees (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-12

DE 83—Credits, Transaction Fee Amount

Credits, Transaction Fee Amount (DE 83) is the amount the MDS processes as interchange transactions (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-12

DE 84—Debits, Processing Fee Amount

Debits, Processing Fee Amount (DE 84) is the amount the MDS processes as processing fees dealing with handling and routing (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-12

DE 85—Debits, Transaction Fee Amount

Debits, Transaction Fee Amount (DE 85) is the amount the MDS processes as processing fees of interchange transactions (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-12

DE 86—Credits, Amount

Credits, Amount (DE 86) is the amount the MDS processes as cardholder credits (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-16

DE 87—Credits, Reversal Amount

The Credits, Reversal Amount (DE 87) is the amount the MDS processes as reversal credits (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-16

DE 88—Debits, Amount

Debits, Amount (DE 88) is the amount the MDS processes as debits (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-16

DE 89—Debits, Reversal Amount

Debits, Reversal Amount (DE 89) is the amount the MDS processes as reversal debits (to the CPS) during the daily settlement reporting period.

Note **The MDS does not support this data element.**

Attribute

n-16

DE 90—Original Data Elements

Original Data Elements (DE 90) are data elements contained in an original message that may identify a transaction for correction or reversal.

Attribute

n-42

Usage

DE 90 **must** be present in the following messages as a reference to an original transaction being affected by a new message or transaction:

- Acquirer Reversal Advices/0420
- Issuer Reversal Advices/0422
- Financial Transaction Advices/0220

Note

For transactions processed by the MDS, please refer to data element (DE 63) subfield 3—switch serial number, as the key data element to match online same day acquirer and issuer reversal advices.

Please note that this data element is not present in the Financial Transaction Negative Acknowledgment/0290 messages.

Values

This data element is composed of 5 fixed-length subfields. Table 4.35 describes how each subfield is encoded as alphanumeric, or right-justified with leading zeroes.

Table 4.35—Original Data Elements Subfields

Subfield	Attribute	Value
1	n-4	Original MTI, Message Type Identifier
2	n-6	Original DE 11, System Trace Audit Number
3	n-10	Original DE 7, Transmission Date and Time
4	n-11	Original DE 32, Acquiring Institution ID Code
5	n-11	Original DE 33, Forwarding Institution ID Code

DE 91—File Update Code

The File Update Code (DE 91) is used in File Update Request/0302 messages. It indicates, to the MDS or to the MasterCard Account Management System (AMS), the action to perform to the file named in File Name (DE 101).

Note **The MasterCard® Debit Switch (MDS) does not use this data element for the Financial Transaction/02xx messages.**

Attribute

an-1

Usage

For File Update Request/0302 messages, the value of this data element indicates the execution of a specific file update action. The File Update Request Response/0312 message must return the same value as was sent in the 0302 message.

Values

Table 4.36 describes the File Update Code values for DE 91.

Table 4.36—File Update Code Values

Code	Description
1	Add record
2	Change record
3	Delete record
5	Inquiry

Table 4.37 lists valid update codes for each of the files identified in DE 101.

Table 4.37—Valid Updates by File Type

Filename (DE 101)	Add (DE 91 = 1)	Change (DE 91 = 2)	Delete (DE 91 = 3)	Inquiry (DE 91 = 5)
MCC102	•	•	•	•
MCC103	•		•	
MCCNEG	•	•	•	•

DE 92—File Security Code

File Security Code (DE 92) is a file update security code that indicates a message originator is authorized to update a file.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n-2

DE 93—Response Indicator

Response Indicator (DE 93) indicates the update action a POS system takes.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

an-5

DE 94—Service Indicator

Service Indicator (DE 94), in some systems, is an indication of the type of support service required by the recipient of a File Update Request/0302 message.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

an-7

DE 95—Replacement Amounts

Replacement Amounts (DE 95) are the new actual amount data elements necessary to perform a partial or full reversal of a financial transaction or a partial completion amount. This data element can also be used for the completed amount in a Maestro Financial Transaction Advice/0220 completion message for automated fuel transactions.

Attribute

n-42

Usage

The Customer Processing System must use DE 95 in the following messages when the original transaction amounts are being modified:

- Financial Transaction Advice/0220 (Acquirer-generated only) except debit MasterCard
- Acquirer Reversal Advice/0420 message
- Issuer Reversal Advice/0422 message

This data element will not be present in debit MasterCard transaction clearing messages.

Values

This data element is composed of 4 fixed-length subfields. Each subfield is encoded as alphanumeric, right justified with leading zeroes, as described below.

Subfield No. 1 must contain valid numeric data. The message initiator must zero-fill all other subfields. Currency conversion of actual Amount, Transaction (DE 4) into actual Amount, Settlement (DE 5) will be performed by the MDS, when required.

Table 4.38 describes the subfields in DE 95.

Table 4.38—Replacement Amounts Subfields

Subfield	Position	Attribute	Value
1		n-12	Actual Amount, Transaction. For the acquirer Timeout-Induced Reversal Advice/0420 message, this field contains all zeros.
2		n-12	Actual Amount, Settlement (provided by the MDS). For the acquirer Timeout-Induced Reversal Advice/0420 message, this field contains all zeros.
3		n-12	Actual Amount, Cardholder Billing (provided by the MDS). For the acquirer Timeout-Induced Reversal Advice/0420 message, this field contains all zeros.
4		n-6	zero fill

DE 96—Message Security Code

Message Security Code (DE 96) contains an MDS "password" security code to verify that the originator of the sign-on request is allowed access to the requested functions.

Attribute

b-64

Usage

This data element is used in Network Management/0800 messages.

DE 97—Amount, Net Settlement

Amount Net Settlement (DE 97) is the net value of all gross settlement amounts including fees.

Note **The MDS does not support this data element.**

Attribute

x+n-16

DE 98—Payee

Payee (DE 98) is the third party beneficiary in a payment transaction.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

ans-25

DE 99—Settlement Institution Identification Code

The Settlement Institution Identification Code (DE 99) is a code identifying a settlement institution or its agent.

Note **The MDS does not support this data element.**

Attribute

n...11; LLVAR

DE 100—Receiving Institution Identification Code

The Receiving Institution Identification Code (DE 100) identifies the receiver of the message.

Attribute

n...11; LLVAR

Usage

For processors using enhanced issuer identification (EII), the MDS retrieves the issuer processor ID from configured data and sends it in the Financial Transaction Request/0200 to the issuer. The issuer must return the issuer processor ID in the 0210 response, which the MDS will include in the Financial Transaction Request Response/0210 message to the acquirer.

The MDS uses the Receiving Institution Identification Code (DE 100) to determine the destination routing of administrative (06xx) messages. For these messages, the Forwarding Institution ID (DE 33) identifies the sender of the message; the receiver of the message is identified by the Receiving Institution ID (DE 100).

Values

The processor ID is a ten-digit number of the form "9000000xxx" where xxx is a three-digit number assigned by MasterCard

Note **Processing systems must not exchange the contents of the Forwarding and Receiving Institution ID Code data elements in response messages; the contents must remain the same for accurate response message routing.**

DE 101—File Name

File Name (DE 101) is the actual or abbreviated name of a referenced file that is updated in accordance with the File Update Code (DE 91) of a File Update Request/0302 message.

Note **The MasterCard® Debit Switch (MDS) does not use this data element in the Financial Transaction/02xx messages.**

Attribute

ans...17; LLVAR

Usage

This data element is used to identify the specific name of a Network data file, product parameter table, or Stand-In processing database that is being updated via a File Update Request/0302 message. The File Update Request Response/0312 message contains the same value in DE 101 that was sent in the 0302 message.

Values

Table 4.39 shows the valid values and the allowable file update actions for the file name.

Table 4.39—Valid Filenames and Allowable Updates

File Name (DE 101)	Description	Add (DE 91 = 1)	Change (DE 91 = 2)	Delete (DE 91 = 3)	Inquiry (DE 91 = 5)
MCC102	Account File	•	•	•	•
MCC103	Account Management File	•		•	
MCCNEG	MDS Stand-In Negative File	•	•	•	•
MCCVIP	MDS Stand-In VIP File	•	•	•	•

DE 102—Account Identification-1

Account Identification-1 (DE 102) is a series of digits used to identify a customer account or relationship. It is primarily used to identify the "**from account**" in a transaction.

Attribute

n...28; LLVAR

Usage

Issuers may use DE 102 in an Authorization Response/0110 or a Financial Transaction Response/0210 messages to identify the specific cardholder "from" account number affected by a transaction. Acquirers may use DE 102 for printing on cardholder transaction receipts.

The "from" account is the account specified by the third and fourth digits of the Processing Code (DE 3).

Values

The MDS restricts the values of this data element to be numeric only.

DE 103—Account Identification-2

Account Identification-2 (DE 103) is a series of digits used to identify a customer account or relationship. It is primarily used to identify the "**to" account** in a transaction.

Attribute

n...28; LLVAR

Usage

Issuers may use DE 103 in an Authorization Response/0110 or a Financial Transaction Response/0210 messages to identify the specific cardholder to account number affected by a transaction. Acquirers may use DE 103 for printing on cardholder transaction receipts. The "to" account is the account specified by the fifth and sixth digits of the Processing Code (DE 3).

Values

The MDS restricts the values of this data element to be numeric only.

DE 104—Transaction Description

Transaction Description (DE 104) can be used to describe additional characteristics of the transaction for billing purposes.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

ans...100; LLLVAR

DE 105–DE 109—Reserved for ISO Use

ISO reserves these data elements for future definition and use.

Note **The MasterCard® Debit Switch (MDS) does not use these data elements.**

Attribute

ans...999; LLLVAR

DE 110—Additional Data - 2

Additional Data - 2 (DE 110) is reserved for use based on product type.

Attribute

ans….100; LLLVAR

Usage

DE 110 provides supplemental data in a message when a specific ISO-designated data element is not available. It is free-format, variable-length alphanumeric data element that may be used for multiple purposes. This data element's content may vary by program and service.

Table 4.40 provides formats and descriptions for the subelements (SE) in DE 110. Currently, there are only two subelements, but as subelements are added, the subelement sequence will not have to be in the order of tag value.

Note **The length of this data element has been limited to 100 bytes for practical operational and system constraints.**

Table 4.40—Subfields in DE 110

Subelement	Value		
01	Acquirers send this subelement to identify a specific merchant for tiered interchange calculations. The specific value is assigned by MasterCard.		
	Subfield	**Attribute**	**Value**
	Merchant ID Tag	n-2	Value = 01
	Subelement Length	n-2	Value = 06
	Tiered Merchant ID	n-6	Contains the Merchant ID
02	The Program Registration ID monitors and tracks a participant's activity in special promotion programs, such as Quick Payment Services (QPS), Supermarket, Service Industries, Payment Transactions, and Warehouse Club programs. This subelement is optionally received in Debit MasterCard Force Post.		
	Subfield	**Attribute**	**Value**
	Subelement number	n-2	Value = 02
	Subelement Length	n-2	Value = 03
	Promotional ID indicator	an-3	**PAA** Prestigious Hotel (PH) transaction **Qxx** QPS transaction **Rxx** Service Industries transactions **Sxx** Supermarket transaction **Wxx** Warehouse Club transaction **PAY** Payment Transaction The **xx** is a MasterCard-assigned alphanumeric ID unique to each participant.

DE 111—Amount, Currency Conversion Assessment

Oct 2005

Amount, Currency Conversion Assessment (DE 111) is the amount calculated by MDS that is the result of the currency conversion assessment being applied to qualifying transactions. The MDS automatically inserts this data element into all originating 0200 (request), 0220 (force post), 0420 (reversal) online messages, only when Currency Conversion Assessment has been applied to the transaction. The currency code for data element 111 must be expressed in the cardholder billing currency (DE 51).

Attribute

n…012; LLLVAR

Usage

Amounts are expressed without a decimal separator. For currencies that support exponents, users and systems are responsible for placing the decimal separator appropriately. Refer to the *Quick Reference Booklet* for a listing of currencies and their exponents.

DE 112—Additional Data (National Use)

Additional Data (National Use) (DE 112) is reserved for national organizations to define data unique to specific networks or specific programs and services.

Attribute

ans...248; LLLVAR

Usage

The MDS uses this data element to support the Parcelas, CDC, Post Dated, and Installment Transaction products. Parcelas provides acquirers and issuers with the ability to support a recurring payment option at the point of service.

Note **Parcelas, CDC, Post Dated, and Installment support are presently limited to Maestro® ISIS transactions in Brazil.**

The MDS supports Parcelas, CDC, Post Dated, and Installment Transaction products.

- **CDC**—Consumers at the point of interaction can make an "inquiry" requesting time pay options for a major purchase. The issuer can respond, providing up to four financing plans for the consumer to choose. The consumer can then select one of the options and the merchant submits the "purchase" request in another transaction. The consumer is then billed monthly for the installment payment.
- **Parcelas with interest**—Under this option, the length of repayment installments ranges from 2 to 12 months. The transaction is billed monthly to the cardholder. The authorization returned to the acquirer includes the amount of interest over the total installment value and taxes on interest.
- **Post Dated**—A transaction is authorized in real time with the associated payment due to the issuer up to 30 days hence. No settlement occurs at transaction time. A merchant may pay a 'warranty fee' to guarantee funds availability once the issuer authorizes the transaction. Warranty fees are collected at the time of settlement.
- **Installment**—A transaction is authorized in real time with payments to the merchant spread over a pre-determined number of months with monthly installments on the balance. A merchant may pay a 'warranty fee' to guarantee funds availability for each installment.

Note **CDC Inquiry transactions must include Point of Service (POS) Data (DE 61) where position 7 equals 3.**

Note **If the acquirer sends a transaction type other than '50' in subelement 1 and the issuer returns a transaction type 50, the MDS will create a 0420 reversal message to the issuer with a DE 60 value of 4540000 to indicate a format error in the 0210 message. The MDS will return the 0210 to the acquirer with a DE 39 value of 91.**

Oct 2005

Values

The first three bytes (the "LLL" length field of LLLVAR) specify the overall length of DE 112. The overall length of DE 112 is restricted to 251 bytes.

The MDS organizes DE 112 into a group of encoded subelements. A three-byte ID and an associated three-byte length indicator identify each subelement.

The first three bytes of each subelement must contain an ID in the range 000–999 to specify the type of DE 112 subelement. Individual requirements define the use and content of the DE 112 subelement.

The second three bytes of each subelement must contain a length indicator in the range 000–999.

Figure 4.2 reflects the construction of DE 112 as well as the subelements it may contain.

Figure 4.2—DE 112 Subelement Contents

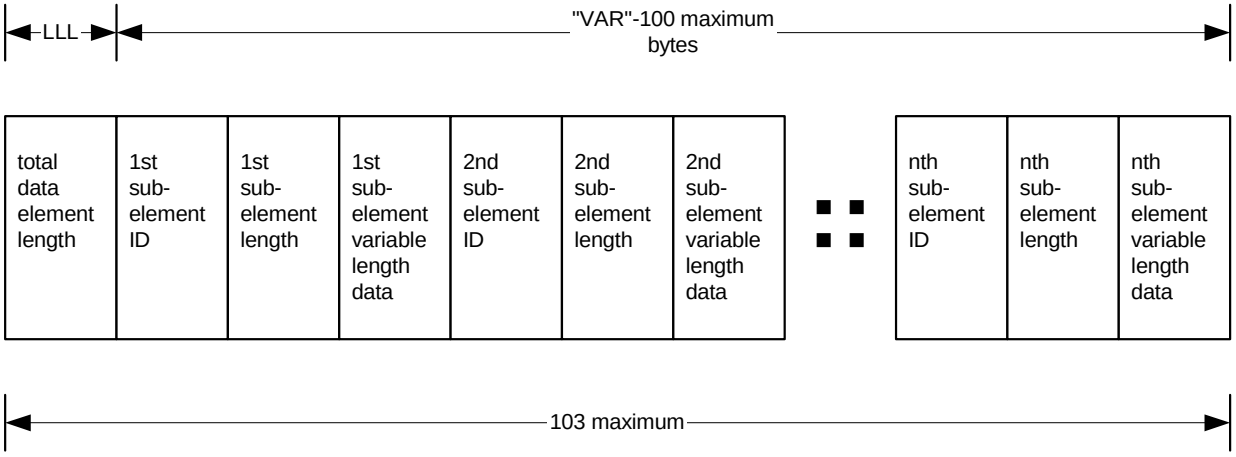


Table 4.41—Parcelas and CDC Transactions Subelement Requirements

Message Type	Subelements												
	1	2	11	12	13	14	15	16	18	19	22	23	24
Parcelas 0200	M	•	•	•	•	•	•	•	•	•	•	•	•
Parcelas 0210	M	M	•	•	•	•	•	•	•	•	•	•	•
CDC Inquiry 0200	M	•	•	•	•	•	•	•	•	•	•	•	•
CDC Inquiry 0210	M	•	M	O	O	O	O	O	•	•	•	•	•
CDC Purchase 0200	M	•	•	•	•	•	•	•	•	•	•	•	•
CDC Purchase 0210	M	•	M	O	•	•	•	•	•	•	•	•	•
Post Dated 0200	M	•	•	•	•	•	•	•	M	•	•	•	•
Post Dated 0210	M	•	•	•	•	•	•	•	•	•	•	•	•
Completion – Post Dated 0200	M	•	•	•	•	•	•	•	M	•	•	•	•
Completion – Post Dated 0220	M	•	•	•	•	•	•	•	M	•	•	•	•
Completion – Post Dated 0230	M	•	•	•	•	•	•	•	•	•	•	•	•
Installment 0200	M	•	•	•	•	•	•	•	•	M	•	•	•
Installment 0210	M	•	•	•	•	•	•	•	•	•	•	•	•
Completion – Installment 0200	M	•	•	•	•	•	•	•	•	M	•	•	•
Completion – Installment 0220	M	•	•	•	•	•	•	•	•	M	•	•	•
Completion – Installment 0230	M	•	•	•	•	•	•	•	•	•	•	•	•
Positive ID 0200	M	•	•	•	•	•	•	•	•	•	M	•	•

Message Type	Subelements												
	1	2	11	12	13	14	15	16	18	19	22	23	24
Positive ID 0210	M	•	•	•	•	•	•	•	•	•	•	C	•
Construcard 0200	O	•	•	•	•	•	•	•	•	•	•	•	•
Construcard 0210	M	•	•	•	•	•	•	•	•	•	•	•	•
Trishop 0200	M	•	•	•	•	•	•	•	•	•	•	•	•
Trishop 0210	M	•	•	•	•	•	•	•	•	•	•	•	•
Time Based 0620	M	•	•	•	•	•	•	•	•	•	•	•	M

Oct 2005

Table 4.42—Additional Data (National Use) Subelements

Subelement	Position	Attribute	Value		
1			For Financial Transaction Request/0200 messages and Financial Transaction Request Response/0210 messages		
			Subfield	**Attribute**	**Value**
	1–3		Subfield tag	n-3	001 1st subfield
	4–6		Subfield length	n-3	008 Length of the subfield
	7–8		Subfield data	an-2	Transaction type: **21** Parcelas Purchase **10** CDC Purchase **11** CDC Inquiry **30** Post Dated with Guarantee **31** Post Dated without Guarantee **40** Installment with Guarantee **41** Installment without Guarantee **50** Construcard **60** Trishop
	9–10			n-2	Number of installments
	11–14		Subfield data	n-4	Date (DDMM)
2			For Financial Transaction Request Response/0210 messages.		
			Subfield	**Attribute**	**Value**
	1–3		Subfield tag	n-3	**002** 2nd subfield
	4–6		Subfield length	n-3	**032** Length of the subfield
	7–8		Subfield data	an-2	Transaction type: **21** Parcelas transaction
	9–10			n-2	Number of installments
	11–22			n-12	Installment Interest
	23–34			n-12	Purchase plus interest amount
	35–38			n-4	Annual interest rate
11			For CDC Inquiry and Purchase Financial Transaction Request Response/0210 messages		
			Subfield	**Attribute**	**Value**
	1-3		Subfield tag	n-3	**011**

Oct 2005

Subelement	Position	Attribute	Value		
	4-6		Subfield length	n-3	**041** Length of the subfield
	7-17		Subfield data	n-11	Estimated installment amount for YY installment
	18-28		Subfield data	n-11	Total amount of transaction with interest
	29-33		Subfield data	n-5	Monthly interest rate xxx.xx
	34-41		Subfield data	n-8	TAC; 2 decimal positions
	42-47		Subfield data	n-6	Annual rate
12			For CDC **Inquiry** Financial Transaction Request Response/0210 messages. Items below are optional at the issuer's discretion.		
			Subfield	**Attribute**	**Value**
	1-3		Subfield tag	n-3	**012**
	4-6		Subfield length	n-3	**002** Length of the subfield
	7-8		Subfield data	n-2	Value = nn nn = number of additional installment options the issuer is offering (detailed in subtags 13 through 16, if applicable)
			For CDC **Purchase** Financial Transaction Request Response/0210 messages.		
			Subfield	**Attribute**	**Value**
	1-3		Subfield tag	n-3	**012** This subtag is optional
	4-6		Subfield length	n-3	**181** Length of the subfield
	7-11		Subfield data	n-5 2 decimal positions	Fee for CDC transaction
	12-15		Subfield data	n-4 2 decimal positions	Percentage penalty if not paid on specific date
	16-19		Subfield data	n-4 2 decimal positions	Percentage of interest on deferred payment
	20-187		Subfield data	an-168	Free text available to issuer to print marketing or agreement data messages to appear on terminal receipt

Subelement	Position	Attribute	Value		
13-16			For CDC **Inquiry** Financial Transaction Request Response/0210 messages.		
			Subfield	**Attribute**	**Value**
	1-3		Subfield tag	n-3	**013**
	4-6		Subfield length	n-3	**037** Length of the subfield
	7-10		Subfield data	an-4	Value = XXYY XX = 20 installment with interest YY = option 2 number of installments
	11-21		Subfield data	n-11	Estimated installment amount for YY installment; two decimal positions
	22-32		Subfield data	n-11	Total amount of transaction with interest; two decimal positions.
	33-37		Subfield data	n-5	Monthly interest rate xxx.xx; two decimal positions.
	38-43		Subfield data	n-6	Annual rate; two decimal positions.
18			For Post Dated Transactions (pre-authorization and completion) Values Supplied by Acquirer		
			Subfield	**Attribute**	**Value**
	1-3		Subfield tag	n-3	018
	4-6		Subfield length	n-3	045
	7		Guarantee	a-1	'Y'es or 'N'o
	8-15		Guarantee amount	n-8	Amount of guarantee to be settled with completion message; zero if no guarantee; assumed to be a credit to the issuer
	16-21		Post Settlement Date	n-6	MMDDYY of proposed settlement date (expected date for completion message arrival)
	22-27		Original MDS Settlement Date	n-6	MMDDYY; MDS settlement date of original pre-authorization; contains zeroes on preauthorization message
	28-36		Original MDS Switch Serial Number	n-9	Original switch serial number assigned by MDS to original pre-authorization request; contains zeroes on preauthorization message

Subelement	Position	Attribute	Value		
	37-37		DR/CR Indicator	a-1	Denotes if the interchange value is a credit "C" or debit "D" to the receiver
	38-45		Interchange	n-8	Interchange amount associated with completion message; contains zeroes on preauthorization message
	46-51		Auth Code	n-6	Contains the online authorization code provided by the issuer on the original preauthorization response
19			For Installment Transactions (pre-authorization and completion) Values Supplied by Acquirer		
			Subfield	**Attribute**	**Value**
	1-3		Subfield tag	n-3	019
	4-6		Subfield length	n-3	049
	7		Guarantee	a-1	**Y** Yes, **N** No
	8-15		Guarantee amount	n-8	Amount of guarantee to be settled with each completion message; zero if no guarantee; assumed to be a credit to the issuer
	16-17		# of Installments	n-2	Typically value between 2 and 6; not edited
	18-19		# of this Installment	n-2	Zero for pre-authorization request
	20-25		Date of First Installment	n-6	MMDDYY; zeroes for completion messages
	26-31		Original MDS Settlement Date	n-6	MMDDYY; MDS settlement date of original pre-authorization; contains zeroes on pre-authorization message
	32-40		Original MDS Switch Serial Number	n-9	Original switch serial number assigned by MDS to original pre-authorization request; contains zeroes on preauthorization message
	41 - 41		DR/CR Indicator	a-1	Denotes whether interchange value is a credit "C" or debit "D" to the receiver
	42-49		Interchange	n-8	Interchange amount associated with completion message; contains zeroes on preauthorization message

Subelement	Position	Attribute	Value		
	50-55		Auth Code	n-6	Contains the online authorization code provided by the issuer on the original preauthorization response
22			For Positive ID transactions. Subelement carries Positive ID data		
			Subfield	**Attribute**	**Value**
	1-3		Subfield tag	n-3	'022'
	4-6		Subfield length	n-3	'016'
	7		Terminal PID Capable	a-1	**Y** Yes, **N** No
	8		PID Requested	a-1	**Y** Yes, **N** No
	9		Information ID Code-1	1 byte hex	01 to 0C
	10		Information Length-1	1 byte hex	01 to 0C
	11		Information ID Code-2	1 byte hex	01 to 0C
	12		Information Length-2	1 byte hex	01 to 0C
	13		Information ID Code-3	1 byte hex	01 to 0C
	14		Information Length-3	1 byte hex	01 to 0C
	15-22		Positive ID	64 bit = 8 bytes	concatenated response in ANSI PIN block format
23			Positive ID Translation/Validation error code		
			Subfield	**Attribute**	**Value**
	1-3		Subfield tag	n-3	023
	4-6		Subfield length	n-3	001

Subelement	Position	Attribute	Value		
	7		Positive ID Error Code	a-1	**1** if the MDS translation error occurred on the PIN block. 0210 msg DE 39 response code '63' **2** if the MDS translation error occurred on Positive ID. 0210 msg DE 39 response code '63' **3** if the issuer validation error occurred on the PIN block. 0210 msg DE 39 response code '55' **4** if the issuer validation error occurred on Positive ID. 0210 msg DE 39 response code '55'
24			For Timed Based Transactions (pre-authorization and completion) Values supplied by originator		
			Subfield	**Attribute**	**Value**
	1-3		Subfield tag	n-3	024
	4-6		Subfield length	n-3	031 Length of the subfield
	7-31		Admin. Message Text	ans-25	Free Form Text supplied by the originator

DE 113–DE 119—Reserved for National Use

The National Standards Organization uses and defines these data elements.

Note **The MasterCard® Debit Switch (MDS) does not use these data elements.**

Attribute

ans...999; LLLVAR

DE 120—Record Data

Record Data (DE 120) is a free-format variable-length data field used for transmitting file record data or textual character string data in various message types.

Attribute

ans...999; LLLVAR

Usage

When used in Administrative Advice/0620 messages having an Advice Reason Code set to "600" (Invalid message; rejected by Network), this data element contains the original (rejected) message.

When used in the File Update Request/0302 message, DE 120 contains the new, actual file record data used in "add" or "change" file-update actions. Table 4.43 illustrates the subelement structure of DE 120 in the 0302 message for each file that the 0302 message updates.

Table 4.43—Message Type 0302 Data Element 120 Structure

Subelement	Position	Attribute	Description
Account File MCC102 DE 120 [a]			
PAN	1-19	n-19	Primary account number to be updated by this request.
Issuer ICA	20-25	n-6	MasterCard assigned member ID.
Entry Reason	26	an-1	Must be one of the following codes: P Capture card S Stolen card O Other V VIP C Credit L Lost X Counterfeit F Fraud G Gold (only for a BIN with a product code of MCC) U Unauthorized use

Subelement	Position	Attribute	Description
Date Last Update	27-32	mmddyy	Returned in inquiry, ignored on add, update, and delete.
Time Last Update	33-36	hhmm	Retained in inquiry, ignored on add, update, and delete.
PIN Length	37, 38	n-2	Always has a value of "00".
VIP Limit	39-50	n-12	Amount, whole dollars. Zero except for Entry Reason = V.
VIP Currency Code	51-53	n-3	Currency code for VIP, only valid for Entry Reason = V.
Account Management File MCC103 DE 120 b			
PAN	1-19	n-19	Primary account number to be updated by this request.
Issuer ICA	20-25	n-6	MasterCard assigned member ID.
Card Program	26-28	an-3	Must be one of the following codes: **MCB** MasterCard Corporate card® **MCC** Mixed BIN **MCD** Debit MasterCard **MCF** MasterCard Corporate Fleet card® **MCG** Gold MasterCard® Corporate Purchasing card **MCP** MasterCard Corporate Purchasing card® **MCS** MasterCard Standard card **MCW** World MasterCard® card **MNS** Non-standard **MPL** Platinum MasterCard® card **OTH** Other
Response Code	29, 30	n-2	Value is "04", capture card.
Entry Reason	31	an-1	Must be one of the following codes: **C** Credit **X** Counterfeit **O** Other **F** Fraud
Filler	32-56	an-25	Reserved for future AMS enhancements.
Regional Information			Nonpositional, may occur up to six times in ascending order.

Subelement	Position	Attribute	Description
Indicator	57	an-1	Valid regions are: **1** United States **A** Canada **B** Caribbean, Central America, Mexico and South America **C** Asia/Pacific **D** Europe **E** South Asia/Middle East/Africa
Purge Date	58-63	yymmdd	The member-requested purge date
MDS Stand-In Negative File MCCNEG DE 120 a			
PAN	1-19	n-19	Primary account number to be updated by this request.
Issuer ICA	20-25	n-6	MasterCard assigned member ID.
Capture Code	26	an-1	Y(es) or N(o), indicates whether to capture the card.
Entry Reason	27	an-1	Must be one of the following codes: **P** Capture card **S** Stolen card **L** Lost **X** Counterfeit **F** Fraud **U** Unauthorized use
Purge Date	28-33	yymmdd	The member-requested purge date. If not included, the MDS calculates a purge date 180 days from the date of the account listing.
MDS Stand-In VIP File MCCVIP DE 120			
PAN	4-22	n-19	Primary account number to be updated via this request.
Issuer ICA	23-28	n-6	MasterCard assigned member ID
Entry Reason	29	an-1	Must be one of the following codes: **P** Capture card **S** Stolen card **O** Other **L** Lost **X** Counterfeit **F** Fraud **U** Unauthorized use NOTE: For MCCVIP add requests, the only valid entry reason code is O (Other)

Subelement	Position	Attribute	Description
			For MCCVIP update requests, all the above entry reason codes are valid
Purge Date	30-35	yymmdd	The member requested purge date
Total Usage Count	36-39	n-4	The total number of ATM and POS debits
Total Usage Amount	40-47	n-8	The total amount of ATM and POS debits
ATM Usage Total Count	48-51	n-4	The total number of ATM debits from all related accounts
ATM Usage Total Amount	52-59	n-8	The total amount of ATM debits from all related accounts
ATM Usage Savings Count	60-63	n-4	The total number of ATM debits from savings
ATM Usage Savings Amount	64-71	n-8	The total amount of ATM debits from savings
ATM Usage DDA Count	72-75	n-4	The total number of ATM debits from checking
ATM Usage DDA Amount	76-83	n-8	The total amount of ATM debits from checking
ATM Usage Credit Card Count	84-87	n-4	The total number of ATM debits from credit card
ATM Usage Credit Card Amount	88-95	n-8	The total amount of ATM debits from credit card
ATM Usage NAS Count	96-99	n-4	The total number of ATM debits from no account specified
ATM Usage NAS Amount	100-107	n-8	The total amount of ATM debits from no account specified
POS Usage Total Count	108-111	n-4	The total number of POS debits
POS Usage Total Amount	112-119	n-8	The total amount of POS debits

[a] Only PAN and Issuer ICA are required for delete or inquiry requests.

[b] Only PAN and Issuer ICA are required for delete requests.

For MCC102 adds, changes, and deletes, the File Update Request Response/0312 echoes back in Record Data (DE 120) the same information that was received in DE 120 of the File Update Request/0302. For MCC102 inquiries, the 0312 response contains in DE 120 the full record of the database that was requested.

For MCC103 adds, changes, and deletes, the File Update Request Response/0312 echoes back in Record Data (DE 120) the same information that was received in DE 120 of the File Update Request/0302. Corresponding to the contents of DE 120 in the MCC103 add/change 0312 message responses, DE 122 will contain the effective dates and purge dates for each region on file for the account.

For MCCNEG adds, changes, and deletes, the File Update Request Response/0312 echoes back in Record Data (DE 120) the same information that was received in DE 120 of the File Update Request/0302.

Note

If a BIN is flagged as debit MasterCard and is eligible for the MDS Stand-In processing, then the issuer will only need to send one File Update Request/0302 to update MCC102 (Account File) on the Account Management System (AMS). This message will update the MCCNEG file on the MDS Stand-In system and the MCC102 (Account File) on the AMS.

Alternatively, this data element is used in 0100 requests to contain billing address data for the MasterCard Address Verification Service (AVS). When the MDS receives an 0100 message with this data present, the MDS submits the data within DE 120 within an 0200 message to the issuing processor and the issuer must respond with the same data in DE 120 that it received from the MDS. The MDS then returns the DE 120 to the acquirer.

The AVS condensed format begins with the left-most position and uses up to five numeric values that appear before the first alphabetic character or space. Once AVS finds a space or an alphabetic character, it stops interrogating the cardholder billing address, and constructs the condensed AVS key.

For example: 223 NW 31st Street, Apartment #3, in this case the match is 223.

Table 4.44 describes the Record Data values for DE 120 for the AVS usage.

Table 4.44—DE 120 Subfields for AVS Usage

Subfield	Position	Attribute	Value
Subelement tag identifier	1–2	n-2	03
Length of subelement	3–4	n-2	14
Cardholder postal/zip code	5–13	an-9	Cardholder postal zip code (left justified, blank filled)
Cardholder address	14–18	an-5	Cardholder billing address (left justified, blank filled)

Note **To receive a complete match, the issuer must base its keys using the AVS condensed algorithm logic.**

DE 121—Authorizing Agent Identification Code

This data element identifies the actual processing facility that approved or denied a Transaction Request message.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

n...011; LLLVAR

Usage

When a Stand-In or alternate authorizer processing facility performs an authorization or a financial transaction on behalf of a card issuer, it must insert this data element into the response message and any advice message transmitted to the actual card issuer. This procedure ensures that a transaction audit trail clearly identifies the authorizing agent that actually approved the transaction.

DE 122—Additional Record Data

By provision of the ISO 8583–1987 specification, MasterCard redefined this data element for use as "Additional Record Data."

Attribute

ans...100; LLLVAR

Usage

Additional Record Data (DE 122) is a "free-format" variable length data element used for transmitting file record data in various message types. In a File Update Request Response/0312 message, this data element is available to pass data sent to the issuer by the AMS in response to a File Update Request/0302 inquiry.

Table 4.45 indicates the data returned in DE 122 for accepted File Update Request/0302 updates.

Table 4.45—Message Type 0312 Data Element 122 Structure

Subelement	Position	Attribute	Description
Regional data on file			Nonpositional, may occur up to six times in ascending order.
Indicator	1	an-1	Valid regions are: **1** United States **A** Canada **B** Caribbean, Central America, Mexico and South America **C** Asia/Pacific **D** Europe **E** Middle East/Africa
Effective Date	2-7	yymmdd	Effective date of the listing within this region.
Purge Date	8-13	yymmdd	Purge date of the regional listing.

DE 123—Reserved for Future Use and Definition by MasterCard

This data element is for future definition and use by private organizations.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

ans...999; LLLVAR

DE 124—Member-defined Data

This data element is available for processors to send and to receive unedited private business-related data in selected messages.

Attribute

ans...999; LLLVAR

The current maximum length of the data portion of this data element is 99 bytes. For data length nn, length prefix value LLL = "0nn", which is then followed by the data.

Usage

Data Element 124 enables processors to send private data to each other. Use of data element 124 depends on message type and product. Table 4.46 provides a summary of this information. DE 124 is optional.

Table 4.46—Use of Data Element 124 by Message Type and Card Type

Message Type	Debit MC		Maestro		Cirrus	
	Acquirer	Issuer	Acquirer	Issuer	Acquirer	Issuer
0200	N/A	MDS to ISS	ACQ to MDS	MDS to ISS	ACQ to MDS	MDS to ISS
0210 [a]	N/A	ISS to MDS	MDS to ACQ	ISS to MDS	MDS to ACQ	ISS to MDS
0220 [b]	N/A	MDS to ISS	ACQ to MDS	MDS to ISS	ACQ to MDS	MDS to ISS
0230 [c]	N/A	ISS to MDS	N/A	ISS to MDS	N/A	ISS to MDS
0420	ACQ to MDS	N/A	ACQ to MDS	N/A	ACQ to MDS	N/A
0430 [d]	N/A	ISS to MDS	N/A	ISS to MDS	N/A	ISS to MDS

a The issuer may echo DE 124 to the MDS, send a different DE 124 value to the MDS, send DE 124 to the MDS without having received DE 124, or not send DE 124 at all. The MDS passes any value to the acquirer. If the issuer returns no value to the MDS, the MDS does not return DE 124 to the acquirer.

b The acquirer can send a different value in the 0220 message than it received in the 0210 message.

c If the issuer sends DE 124 in the 0230 message, the MDS does not pass DE 124 in the 0230 message to the acquirer.

d If the issuer sends DE 124 in an 0430 message, the MDS does not pass DE 124 in the 0430 message to the acquirer.

The MDS passes anything received in DE 124 from either acquirer or issuer to the other-end processor. The MDS will include the value in DE 124 received from the issuer in its 0210 message back to the acquirer, even if the issuer has declined the request. The MDS will not pass DE 124 to either processor if a message format error exists.

The MDS maintains a configuration record for each processor and uses a field in this configuration record to enable a processor to use DE 124.

DE 125—Reserved for Future Use and Definition by MasterCard

These data elements are for future definition and use by private organizations.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

ans...999; LLLVAR

DE 126—Switch Private Data

The MDS generates this information to facilitate its own message processing.

Attribute

ans...050; LLLVAR

Usage

The MDS uses Switch Private Data (DE 126) to contain Network-generated private-use information. This data is composed of a specific MDS settlement service identifier, and network symbolic information used by the MDS for internal system routing. DE 126 also contains the Cross-Border Transaction and Currency Indicators. When this data element is received in the online message, it must be returned unchanged in the response message from the processor. Oct 2005

Note **All new processors are required to support DE 126** Oct 2005

Note **Processors should be able to receive and echo the entire contents DE 126.**

Subelement Encoding Scheme

The overall length of the DE 126 is specified in its first three bytes (the "LLL" portion of the data element). The overall length of DE 126 is restricted to 050 bytes to accommodate practical operational limitations. Processors must be prepared to receive DE 126 with varying lengths.

Table 4.47 describes the subfields in DE 126.

Table 4.47—Switch Private Data

Subfield	Positions	Attribute	Value
Settlement Service Data	1-3	n-3	**000** Default cutoff/non-Debit MasterCard/non-Brazil ISIS **001** Brazil ISIS transactions **002** Debit MasterCard transactions The MDS may add settlement service values at any time. Processors must be prepared to receive any numeric three-digit value in this field.
MDS Private Data-1	4-13	ans…10	
Cross Border Transaction Indicator	14	ans-1	**Y** Qualifies as a Cross-Border transaction **N** Does not qualify as a Cross-Border transaction
Currency Indicator	15	ans-1	**X** Transaction does not qualify as a Cross-Border transaction **Y** Transaction was submitted in the currency of the merchant's country **N** Transaction was not submitted in the currency of the merchant's country.
MDS Private Data-2	16-50	ans…35	MDS private data-2 The length of MDS Private Data-2 may vary by transaction. Processors must be prepared to receive any combination of valid alpha, numeric or special characters in this field.

Oct 2005

DE 127—Processor Private Data

The MDS reserves this data element for the proprietary use of Customer Processing Systems (CPS) that connect directly to the MDS.

Attribute

ans...050; LLLVAR

Usage

Any message originator (for example, any CPS or INF facility communicating directly with the MDS) may use this data element to contain private-use data up to a maximum length of 50 characters. Data placed in this field is not passed through to the message receiver, but is stored temporarily by the MDS and returned to the message originator in any subsequent response or acknowledgment message.

Typically, this data element is used by CPS or INF processors to contain online transaction matching or queuing data that can be accessed readily upon receipt of the corresponding response to any originating request or advice message.

Values

The MDS does not perform edits on this data field.

DE 128—Message Authentication Code (MAC)

Message Authentication Code (MAC) (DE 128) validates the source and the text of the message between the sender and the receiver.

The last bit position within any bit map is reserved for DE 128. If a member is using authentication on a message, the final bit of the final bit map of that message indicates the MAC information. The final bit of all preceding bit maps must contain "0." For example, there must be only one DE 128 per message and that DE 128 must be the last data element of the message.

Note **The MasterCard® Debit Switch (MDS) does not use this data element.**

Attribute

b-64

5 Communication Protocols

This chapter describes the linking methods that customer processing systems (CPSs) use to connect to the MDS.

Overview

All customer processing systems (CPSs) participating in services offered by the MDS must link to the MDS in one of two ways:

1. Connect through MDS Virtual Private Network (VPN) via MIP/DIU
2. Connect through MDS Virtual Private Network (VPN) via direct router

MIP (Banknet) Connect to MDS

MasterCard transmits data through the Banknet telecommunications network. The Banknet network uses a peer-to-peer architecture and a mesh configuration. A peer-to-peer architecture allows data to follow the most efficient route to its destination and flows through distributed intelligence. Therefore, multiple locations are available for processing information, even during peak times. Another important feature of the architecture of the Banknet network is its on-demand dial back-up equipment.

MasterCard Interface Processor (MIP) and Debit Interface Unit (DIU)

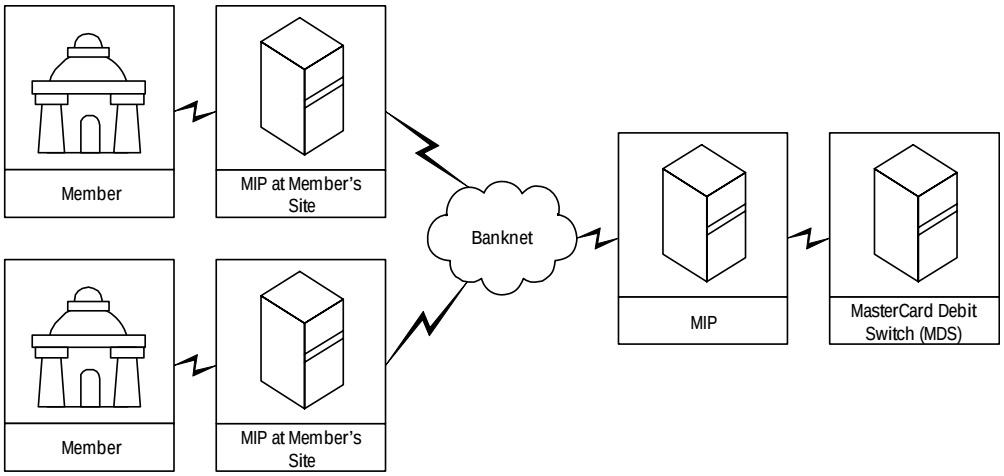
The MIP and DIU provide the hardware and software at the member site that allows the member host system to interface with the Banknet network in a standard, efficient manner. The MIP/DIU also permits distributed data processing functions to support the financial service applications of MasterCard.

Customers may already have a MIP on-site or may share a MIP/DIU with other financial institutions in the area. To accommodate Maestro and Cirrus processing, MasterCard will upgrade the MIP/DIU and route the online real-time financial transactions between the member and the MDS. Oct 2005

MasterCard needs to know the customer's communication protocol required for online debit processing. The precise configuration at a given customer site is engineered jointly by the customer and the MasterCard Network Engineering Group. Historical or anticipated transaction volume is the basis for the MIP configuration. Oct 2005

Figure 5.1 shows the customer host system's connection to the MDS through the Banknet network. Oct 2005

Figure 5.1—Connecting to the MasterCard® Debit Switch



Refer to the *Data Communications Manual* for additional descriptive technical information on the Banknet network and MIP/DIU options.

Note **If a customer selects the Banknet/MIP connectivity option, it must contact its MasterCard Regional Office, Debit Payment Systems—Implementation Support Manager, or both for more detailed requirements.**

Oct 2005

Virtual Private Network

This communications solution, MasterCard Virtual Private Network (VPN), is available for North American-based debit processors.

The VPN consists of a Frame Relay service infrastructure that uses Transport Control Protocol/Internet Protocol (TCP/IP). In order to access the network, each member site will be equipped by MasterCard with a Service Delivery Point (SDP) that typically consists of a Debit Interface Unit (DIU), dual state-of–the-art Cisco routers and dual Ethernet hubs. Oct 2005

Online Transaction Communications

For online transaction communications, customers can choose to continue to use their current data communications protocol rather than convert applications to TCP/IP. The Debit Interface Unit (DIU) will convert the Bisync or SNA protocol to TCP/IP for transport through the network. New processors connecting to the MDS network should use TCP/IP protocol. Oct 2005

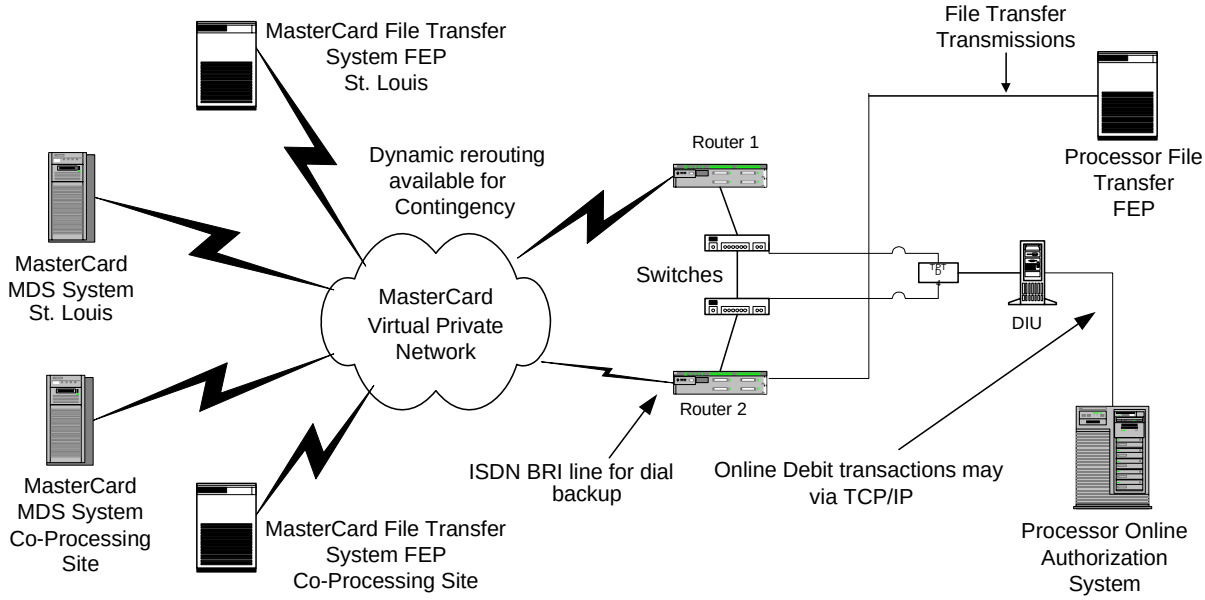
Batch File Transmission

Customers using batch file transmissions (Complex to Complex–CTC) in conjunction with VPN can utilize the TCP/IP protocol. This connection will normally reside on a separate interface (or in some cases a separate router) than the Online transactions, however a separate interface is not mandatory. Oct 2005

Dial Back-up and Data Priority

In the event that a problem occurs with the VPN, ISDN service (or analog dials if ISDN is unavailable) provides backup. The routers immediately initiate ISDN service upon detecting a problem across the primary Frame Relay circuit. The MasterCard Banknet VPN is configured as such that if there is any network congestion the Online transaction data receives a higher routing priority than batch file data.

Figure 5.2—Typical VPN Configuration



Oct 2005

VPN Infrastructure

There are two primary VPN components that are used for both Online and File Transfer communications: frame relay technology and the Service Delivery Point (SDP).

Frame Relay

Frame relay is a high-speed communications technology for sending information over a wide area network (WAN) that divides the information into frames, or packets. Each frame has an address that the network uses to determine the destination of the frame. The frames travel through a series of switches within the frame relay network and arrive at their destination. Frame relay supports the MasterCard Virtual Private Network and provides the foundation for connectivity for all MasterCard members.

The frame relay network is not a single physical connection between one endpoint and the other. Instead, logical path, or virtual circuit, are defined within the network. Oct 2005

MasterCard typically will have a single Data Link Channel Identifier (DLCI) that links from a member location to the nearest frame relay switch. Across this DLCI, there will be two Permanent Virtual Circuits (PVCs), each of which connects to one of MasterCard's two domestic Global Hub sites. Oct 2005

Service Interruption

If there is an interruption in the frame relay network there will be little, if any, service interruption unless both PVCs are impacted. If the customer access circuit (DLCI) is impacted by a Local Exchange Carrier (LEC) outage, both PVCs will be impacted and the processor connectivity will be restored through Integrated Services Digital Network (ISDN).

Service Delivery Points (SDP)

A typical MasterCard VPN Service Delivery Point (SDP) that encompasses the MasterCard equipment placed at a customer site includes:

- MasterCard equipment cabinet
- Debit Interface Unit (DIU)
- Drop Ethernet Splitter
- Two Ethernet Switches
- Two Cisco 26XX or 28XX series routers Oct 2005

- 8PK-CAS switch & analog modem
- Frame Relay Circuit
- ISDN Circuit

Oct 2005

MasterCard has worked very closely with AT&T to develop a highly reliable, highly redundant SDP (with regards to the communications equipment.) A typical SDP has automatic failover if any of the following components become inoperable:

- Primary Cisco Router
- Primary Ethernet Switch
- Frame Relay Circuit

Hot-Standby Routing Protocol (HSRP)

MasterCard VPN routers use Enhanced Internet Gateway Routing Protocol (EIGRP) to distribute updated network routing information between routers. EIGRP allows MasterCard to take advantage of a feature called Hot-Standby Routing Protocol (HSRP).

This feature equips the SDP with the ability to restore service automatically using ISDN in case of a failure of one or more of the above listed components. With HSRP, the two Cisco routers at the customer site are in constant communication with each other so that the secondary router will know if it is necessary to establish an ISDN connection to restore service.

If the primary router senses an outage on the Frame Relay circuit (affecting both PVCs) it will notify the secondary router to "take over." At that point, the secondary router will initiate an ISDN call to one of MasterCard's Global Hub locations so that connectivity to the VPN can be reestablished. In the event of a primary router failure or primary Ethernet switch failure, communication between the primary and secondary routers is lost, and the secondary router will restore the site on ISDN.

Oct 2005

The Debit Interface Unit (DIU) connects to the Ethernet switches via a dual output Ethernet transceiver. The transceiver takes the single Ethernet output from the DIU and splits it, connecting to both Ethernet switches. With this design, a single Ethernet switch failure will not isolate an SDP from the VPN.

The 8PK-CAS and analog modem are strictly used for out-of-band access into the routers and switches for troubleshooting purposes in the event that in-band management becomes inoperable.

Oct 2005

The SDP also can be configured to support direct connect data transfer customers using TCP/IP. To support data transfer via TCP/IP MasterCard will configure an additional Ethernet interface on the secondary router. This router interface will have all necessary access restrictions applied and will also perform Network Address Translation (NAT) functionality, converting customer host IP addresses to IP addresses that MasterCard recognizes for transport across the VPN.

Oct 2005

Online Communication Using MIP/DIU

A Debit Interface Unit (DIU) facilitates online communications between a customer and the MasterCard® Debit Switch (MDS). The DIU is a computer connected to the SDP at the customer site which allows a customer to send debit transactions to MasterCard across the VPN.

Oct 2005

The DIU supports legacy protocols (SNA and bisync) as well as IP. The customer will connect their host equipment to the DIU via a serial connection (for SNA or Bisync) to a DB25 (RS232 or V.35) interface on the DIU's multi-interface card. A DIU typically will have one or two of these serial interface cards. Each card can support either four or eight serial connections ranging in speeds from 4800 bps to 256,000 bps. (See note below regarding Legacy protocol support.)

Oct 2005

If the customer's preferred method of connectivity is IP, their host system will connect to a secondary Ethernet card in the DIU. The network interface Ethernet card is commonly referred to as the **primary** Ethernet card. The DIU receives transactions from the customer, performs certain logging, statistical, and routing functions (for example, transaction and program counters), and encapsulates the transactions into TCP/IP format for transport across the VPN.

Oct 2005

The MasterCard Network Command Center (NCC) has remote access to each DIU for troubleshooting purposes. Using this remote console access, the NCC is able to perform various monitoring and troubleshooting functions, which assist in problem determination and resolution.

Note

MasterCard does not support new member installations using the bisync or SNA protocol.

Effective 1 July 2005, MasterCard will no longer support the bisync protocol. All existing members must complete migration to TCP/IP.

File Transfer Using VPN

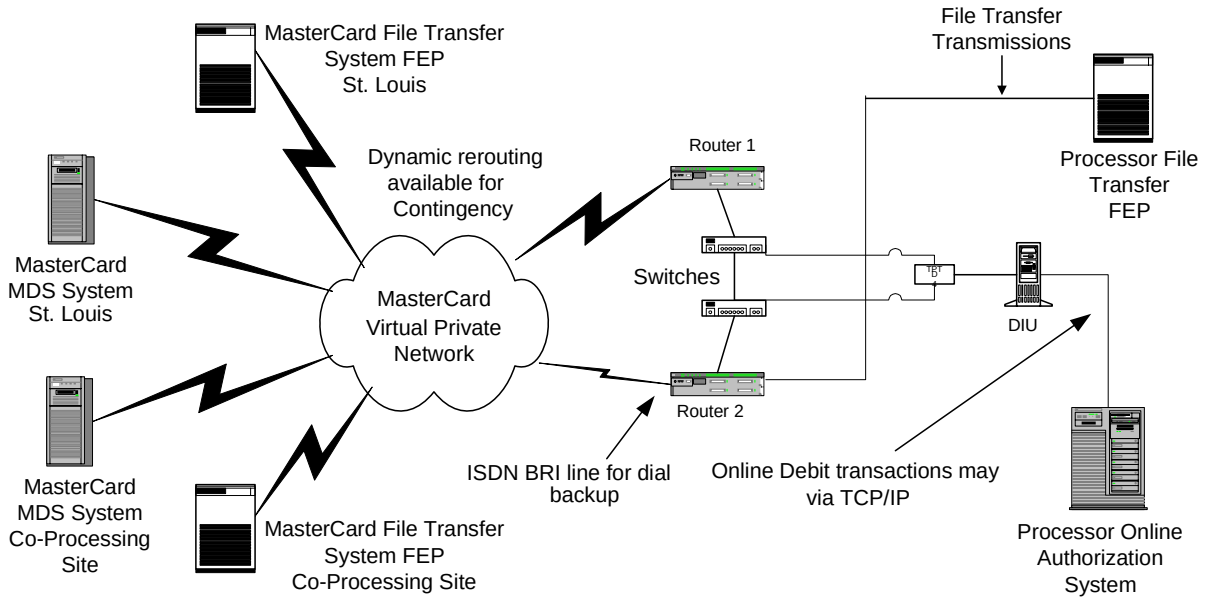
There is a TCP/IP solution for support of settlement detail and report file transmissions. The following subsections describe both options.

VPN File Transfer Using TCP/IP

MasterCard offers File Transfer support using SDP integrated TCP/IP. File Transfer traffic will be on a dedicated segment by providing a second Ethernet connection on router 2.

Oct 2005

Figure 5.3—Typical TCP/IP Configuration



Online Communication Using Direct Router

The MDS router-only solution provides access to the MasterCard Debit Network through a router, without the use of the Debit Interface Unit (DIU). A standard Service Delivery Point (SDP) would provide host communication connectivity, frame relay to the VPN with dial backup, and out-of-band management.

The designs for the router-only solution consist of a single or dual Cisco 2611XM router(s). Typically, all other peripheral devices used with the Service Delivery Point (SDP) would apply to this design with one exception, the Catalyst switch is not required. The below diagrams provide an overview of the design.

There are unique and specific requirements that must be met to use this type of connectivity. Contact your Member Relations Representative for more information.

Figure 5.4—Single 26xx Router for MDS Router Only Connectivity

Oct 2005

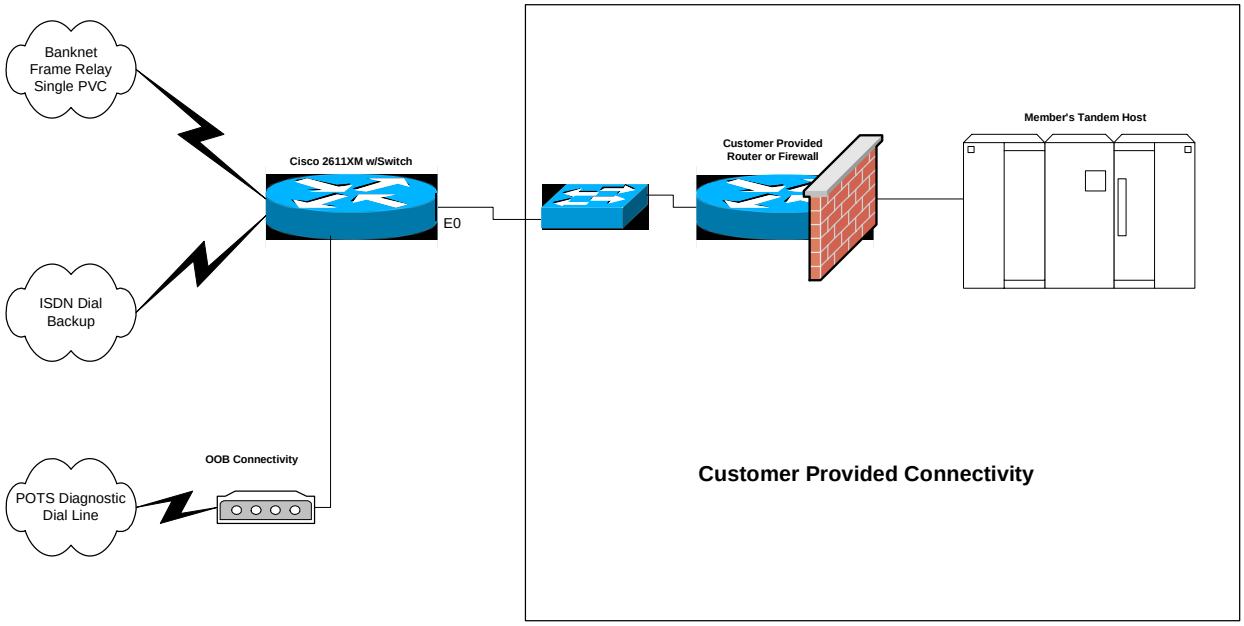
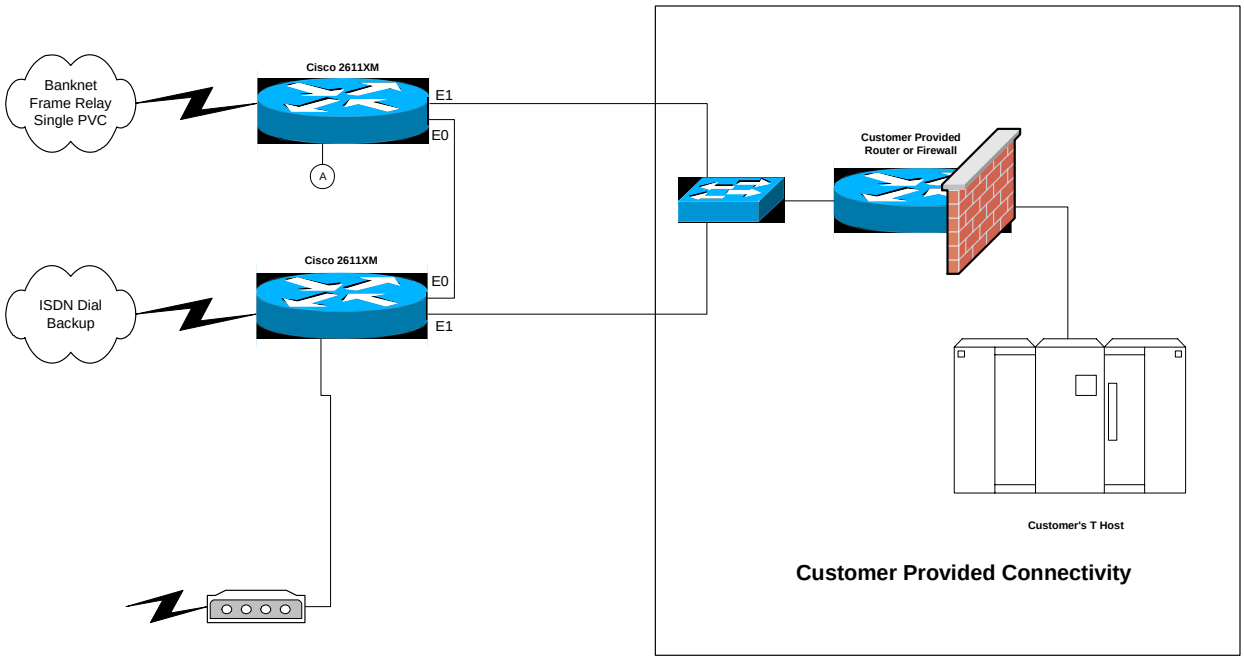


Figure 5.5—Dual 26xx Router for MDS Router Only Connectivity



Oct 2005

Requirements for Single or Dual Router Solutions

A standard SDP would provide host communication connectivity, frame relay to the VPN with dial backup, and out-of-band management. All standards and guidelines should be followed unless otherwise noted in these requirements.

- Customer applications must act as the server and use specific TCP ports assigned by MasterCard. That is, MasterCard MDS will initiate the session as the client. Oct 2005
- Customers must be able to accept and maintain two sessions per processor from the MDS. This ensures seamless connectivity in the event of an MDS site failure. Also the customer should provide "route-back" logic, meaning the session that receives a transaction request should be the same session to which the response message is sent. Oct 2005
- Specific customer TCP ports (6400-6449) and MasterCard ports (64000 – 64999) are to be assigned by MasterCard. For testing, 6450 – 6499 are listening ports for the customer side. Oct 2005
- Strict adherence to TCP port standards is required because MasterCard network routing priorities are based upon these ports.
- MDS will establish a separate TCP session for each assigned MDS Processor number. Oct 2005

Oct 2005

- Ethernet switches are not required, the demarcation point is the router interface.
- A dedicated LAN segment must be provided at the customer's edge. Refer to the *Data Communications Manual* for additional technical information.

6 Encryption

This chapter describes network key management, the exchange of encryption keys, and the maintenance of security in the MDS online environment.

Overview

Network key management involves the exchange and security of encryption keys in the MDS online environment.

The MasterCard® Debit Switch supports two options for Key Management:

- Dynamic
- Static

Note

MasterCard does not permit software encryption of PIN data within the MasterCard ATM network or the Maestro and Cirrus programs. All processors participating in the MasterCard ATM network or the Cirrus, and Maestro programs must use hardware encryption devices only.

Dynamic Key Encryption—Working Key

The online working key exchange uses the MDS ISO 8583-1987 Network Management/0800 message. The MDS Host security module (HSM) generates a random online working key (PIN encryption key). Only the MDS can send the key exchange; however, the member may request a key exchange at any time. Oct 2005

The MDS changes the working key, online, at least once every 12 hours. Processors connected to the MDS via an ISO 8583-1987 interface use the working key. Oct 2005

The member and the MDS jointly establish and use the communication key to encrypt the new working key in the online MDS ISO 8583-1987 Network Management/0800 message.

The member validates the check value and loads the new working key. The processor uses the check values to ensure that the MDS generated the new working key from the same unique communication key established between the processor and the MDS.

The MDS begins using the new working key immediately upon receipt of the processor's approved Network Management Request Response/0810 message. The MDS files the previous working key. Should the acquirer send a PIN block encrypted under the previous working key within the first five minutes of a successful key exchange, the MDS will attempt to process the encrypted PIN block using the old and new working key. This assures the acquirer sufficient time to load and use the new working key. It also limits sanity check errors from occurring on transactions in-flight during the key exchange sequence. The MDS recommends that issuers begin using the new working key immediately upon receipt of the MDS Network Management Advice/0820 key exchange confirmation.

The working key encrypts and decrypts the Personal Identification Number (PIN) Data (DE 52) of the ISO 8583-1987 Financial Transaction Request/0200 message or the Financial Authorization Request/0100 message that the member and the MDS send. The MDS and the member also use the working key to encrypt and decrypt the Positive ID data found in DE 112 subelement 22, for those that support the Positive ID service. The member uses the same working key for issuing and acquiring transactions. The working key supports both ATM and POS products.

MasterCard requests that processors submit new communication key components, used to encrypt the dynamically exchanged working keys, on an annual basis. MasterCard debit staff will contact the member, provide a copy of the MDS Production Communications Key Exchange form and schedule the exchange and loading of the new communication key at the MDS and member site.

Static Key Encryption—Working Key

The working key, used to encrypt the PIN in DE 52 of the Authorization Request/0100 authorization request message, is not exchanged online; it is entered manually (offline) and is used by processors who perform their own PIN verification. Some members connected to the MDS via the Banknet® telecommunications network Authorization Request/0100 message interface use this encryption method. The working key supports ATM and POS products.

The member and the MDS jointly establish and use the new working key. The member validates the check value and loads the new working key. The MDS uses the working key to encrypt the PIN for safe transmission to the issuer and the issuer uses it to decrypt the PIN before performing PIN Validation. The ing key or KPE (PIN Encryption Key) is changed annually.

MDS PIN Verification Services

The MDS provides PIN verification services for the following:

Credit card issuers using the Authorization Request/0100 Banknet network connection to interface with the MDS for ATM cash advances and MasterCard PIN for Purchase transactions. Issuers connected to the MDS via a Financial Transaction/0200 message interface who have opted for MDS Stand-In processing. If the issuer wants the MDS to perform PIN verification, they must provide the PIN Verification Key(s) and PIN processing parameters to the MDS. Please contact your MasterCard Regional Office representative for the required forms.

The MDS supports the following PIN Verification methods:

- IBM 3624
- ABA

Refer to the *Authorization System Manual* for more information about both PIN verification methods.

MDS Key Management

The MDS key management scheme is a method of exchanging encryption keys and maintaining encryption key integrity in an online environment. The MDS employs the following hierarchy of encryption keys:

- **Master file key**: Encrypts working keys and communication keys for safe storage on a database.
- **Communication key**: Encrypts a working key for transmission between the MDS and the processor during the online key exchange.
- **Working key**: Encrypts a PIN for transmission between the processors and the MDS.

Master File Keys

Master file keys are unique to the MasterCard® Debit Switch and each processor that connects to the MDS. Their function is to protect the communication keys and working keys for storage at each site (processor and MDS).

It is the joint responsibility of the MDS and each processor to generate and securely maintain a proprietary master file key.

Communication Keys

Both the MDS and the processor share communication keys. These keys encrypt the new working keys during the dynamic online key exchange.

It is the joint responsibility of the MDS and each processor to generate the unique communication key used to exchange/encrypt working keys.

MasterCard recommends that the communication key for each processor be generated and exchanged at least once every twelve-month period. Members should follow these procedures:

1. Members must use the "MDS Communications Key Part Exchange Form" to request a new communication key exchange. The processor can obtain this form from their MasterCard Regional Office representative or their Debit Services Implementation Manager.
2. Processor Sending Key Officer generates and records the processor clear key component, making an original and a copy. The original is stored in a sealed envelope. The MDS Receiving Key Officer receives the copy in a sealed envelope via courier. Members must use the "MDS Communications Key Part Exchange Form" to accomplish this task. The processor can obtain this form from their MasterCard Regional Office representative or their Debit Services Implementation Manager.
3. MDS Sending Key Officer generates and records the MDS clear key component and a check value. This key component consists of either sixteen (16), thirty-two (32) or forty-eight (48) hexadecimal characters with odd parity on each pair of digits. The MDS Receiving Key Officer makes an original and a copy; storing the original in a sealed envelope. The Processor Receiving Key Officer receives the copy in a sealed envelope via courier.
4. At each site, each key officer enters the key part in his custody into the host security module to be used to generate the communication key (for example, an Atalla security device). A dual control environment handles the management of key components. The system performs a binary "Exclusive-Or" function on the two key parts, thus generating the communication key.

   The processor's master key encrypts this communication key and the resulting cryptogram is stored in the database for use during the online key exchange of working keys.
5. The key parts at each site are stored under dual custody in sealed envelopes for thirty days then destroyed after that time.
6. The generation of new key parts occurs at least once a year on the anniversary of first use.

Working Key

PIN encryption keys are working keys generated by the MDS for each direct connect online processor. These keys encrypt the PIN in Data Element 52 of the online authorization request message.

It is the responsibility of the MDS to generate and distribute the working key.

New working keys are changed dynamically and have the following life cycle:

Oct 2005

- Used for no more than 12 hours.
- Changed after five consecutive "sanity check" errors.
- Changed upon request by the intermediate network facility (INF, acquirer processor, or issuer processor).

It is the responsibility of the processor to safely store this working key by encrypting it under a proprietary master key using hardware security procedures. The processor must use this working key to encrypt all PINs (using ANSI PIN Block formatting) sent to the MDS as well as to decrypt all PINs received from the MDS.

MDS Security Requirements

Within the MDS environment, security considerations include measures for ensuring message security and integrity as well as protection against cardholder personal identification number (PIN) disclosure. The MDS uses secure PIN encryption to protect all PINs. This chapter describes the key management implementation scheme within the MDS, which provides an enhanced degree of protection against PIN disclosure.

The MDS employs PIN encryption using the Data Encryption Standard (DES) algorithm for network security management. Security under DES is dependent on the secrecy of the keys used, and therefore on the management of those keys. The MDS implements the "zone" approach to key management with dynamic keys. MasterCard chose this approach instead of an "end-to-end" approach for the following reasons:

1. Key exchange is required only between connected intermediate network facilities (INF), acquirer processor systems (APS), and issuer processing systems (IPS).
2. Keys are not required to be loaded at the terminal for every issuer participating in the ATM or POS programs.

Figure 6.1 and Figure 6.2 outline the "zone" approach and the flow of key exchange and PIN validation.

In ATM and POS programs, all PINs must be encrypted at the point of entry (the terminal) using the DES algorithm and the approved ANSI PIN block format. The PIN will remain encrypted until the issuer receives it for verification. It will be translated from one zone's working key to another zone's working key as it is passed from one processor to another through the MDS. The MDS must receive the PIN encrypted using the ANSI PIN Block Format.

Members must execute all PIN encryption, translation, and decryption for the ATM or POS programs using hardware encryption through physically secure devices. Both the host and the point of entry, such as the ATM or POS terminal, must use physically-secure hardware.

Physically Secure Device (PSD)

A physically secure device (PSD) is a hardware device that cannot be penetrated successfully to disclose all or part of any key or PIN resident within such a device. Penetration of a PSD shall cause the automatic and immediate erasure of all PINs, keys, and all useful residue of PINs and keys contained within the device.

The member's host computer system must use a hardware security module (HSM) to ensure that the cardholder PIN and the PIN keys used to encrypt the PIN do not reside within the processor's host system.

The ATM must use a PSD such as an encryption board or a keyboard encryption controller to encrypt the PIN before it leaves the terminal and is sent to the acquirer's host.

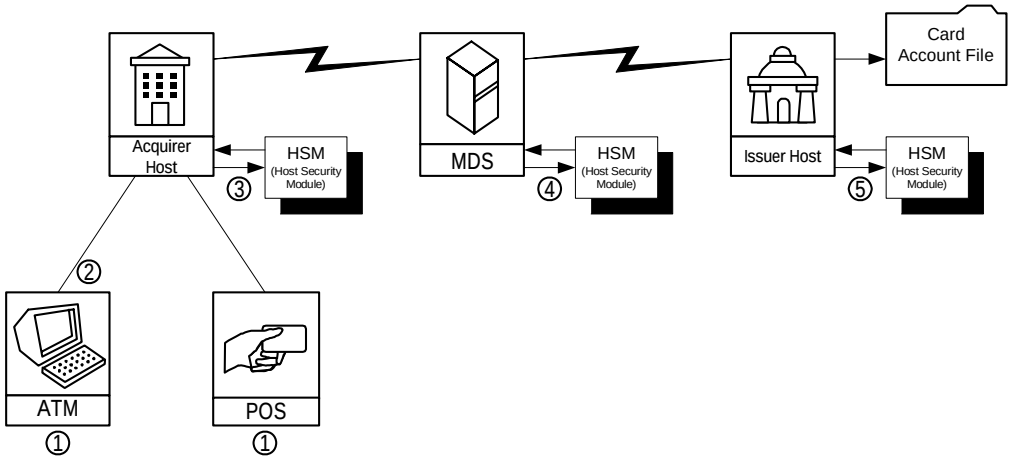
PIN Encryption/Decryption Process

PIN encryption, translation, or decryption must not be performed using software DES routines. Use of DES software in acquirer processing systems (APS), issuer processing systems (IPS), or intermediate network facilities (INF) is a violation of the rules. Following are the PIN encryption/decryption steps:

1. Cardholder enters PIN at point of entry.
2. The terminal encrypts the PIN in hardware under a PIN encryption key and sends it to the acquirer's host.

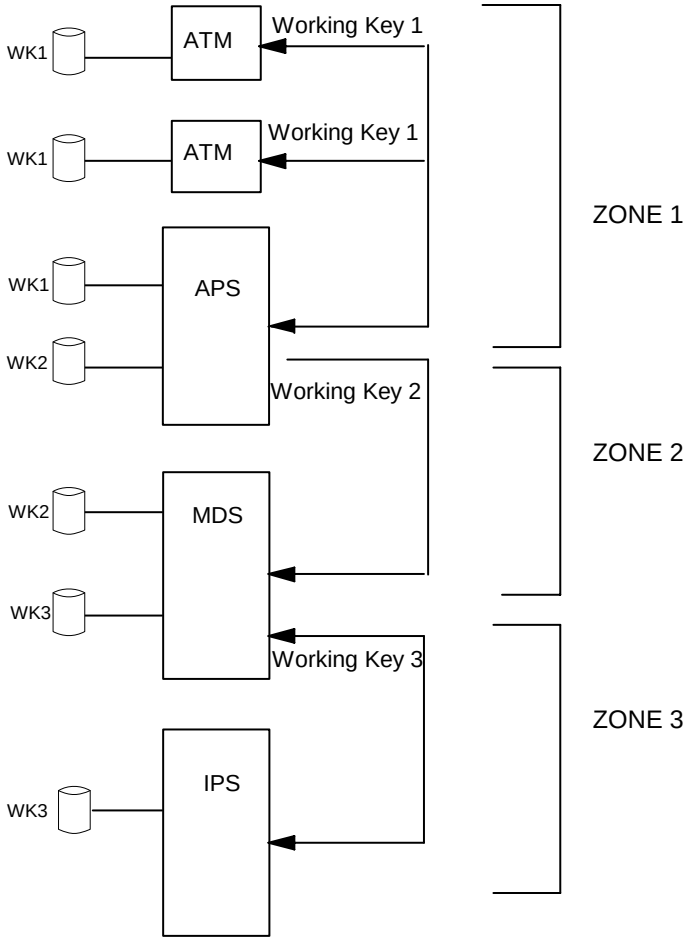
3. The acquirer's host receives the encrypted PIN, which is then decrypted in hardware using the terminal working key. The host system then encrypts it in hardware under a different key that the acquirer and the MDS share. The MDS then receives the newly encrypted PIN.
4. The MDS decrypts the PIN in hardware. It re-encrypts the PIN using a different key that the MDS and the issuer share. The MDS sends the newly encrypted PIN in hardware to the issuer for verification.
5. The issuer decrypts the PIN using the key it shares with the MDS and verifies that the PIN is valid.

Figure 6.1—PIN Encryption/Decryption Process



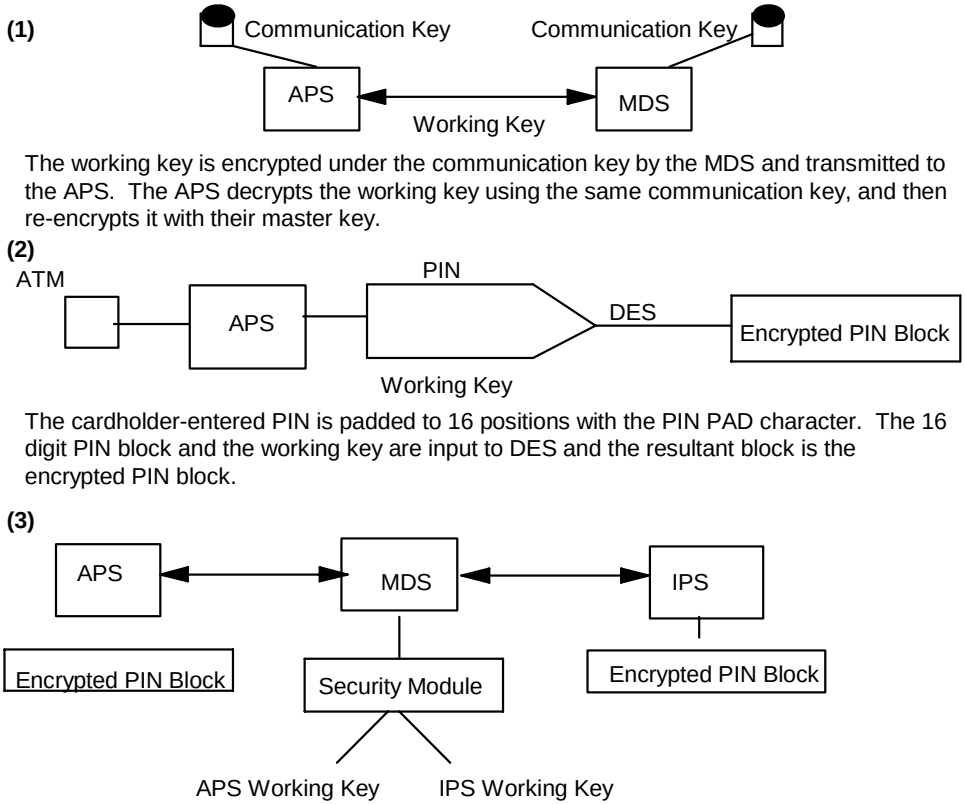
Zone Key Management

Figure 6.2—Zone Key Management



Key Exchange and PIN Validation Data Flows

Figure 6.3—Key Exchange and PIN Validation Data Flows



The working key is encrypted under the communication key by the MDS and transmitted to the APS. The APS decrypts the working key using the same communication key, and then re-encrypts it with their master key.

The cardholder-entered PIN is padded to 16 positions with the PIN PAD character. The 16 digit PIN block and the working key are input to DES and the resultant block is the encrypted PIN block.

The encrypted PIN block is routed to the MDS, where it is translated from the APS working key to the IPS working key. The MDS then routes the encrypted PIN block to the IPS for verification.

The encrypted PIN block and the IPS working key are then input to DES, with an offset if the issuer uses customer selected PINs. The resultant is then verified.

Triple DES

In February 2000, the International Security Committee (ISC) endorsed the migration of members and processors to the triple DES standard. MDS encryption support currently uses the triple DES encryption method to effectively counter sophisticated "brute force" key attacks.

Member Requirements

MDS processors will need to establish a new communications key with the MDS as part of the processor's conversion effort to triple DES support. Implementation of the new communications key is a manual process managed by the MasterCard Debit Customer and Technology Support group.

Note **The MDS testing environment is available to generate key exchange (08xx) message sequences using the expanded length key.**

The MasterCard encryption mode for the encryption of multiple-length keys in an online key exchange is electronic codebook (ECB). MasterCard will not support cipher block chaining (CBC) mode in the initial triple DES implementation.

MasterCard will require that all keys for a defined key zone be of the same length. For example, both the zone master key (KEK) and the zone working key (KPE) for a processor link must be double length, or both must be triple length.

Single Key Length

Currently, processors use the ISO 0800/0810/0820 message sequence to complete encryption key exchanges with the MDS. The key information is stored in data element (DE) 48, subelement 11 in the following format:

Table 6.1—Key Information Format

Subfield	Attribute	Value
Subtag ID	n-2	11
Subtag Length	n-2	38
Key Class Identifier	an-2	PK (PIN key exchange)
Key Index Number	n-2	00 (constant
Key Cycle Number	n-2	00-99
Encrypted Key	an-16	Hexadecimal characters 0-9, A-F; **single key size**
Key Check Value	an-16	Hexadecimal characters 0-9, A-F

Double Key Length

Processors that use double length keys under triple DES will follow the key exchange process below in ISO 0800/0810/0820 message sequences to complete encryption key exchanges with the MDS. The key information is stored in DE 48, subelement 11 in the following format:

Table 6.2—Key Information Format

Subfield	Attribute	Value
Subtag ID	n-2	11
Subtag Length	n-2	54
Key Class Identifier	an-2	PK (Pin key exchange
Key Index Number	n-2	00 (constant)
Key Cycle Number	n-2	00-99
Encrypted Key	an-32	Hexadecimal characters 0-9, A-F; **double key length**
Key Check Value	an-16	The key check value consists of the first four hexadecimal characters (0-9, A-F) of the calculated check value followed by spaces.

Triple Key Length

Processors using triple length keys under triple DES will follow the key exchange process below in ISO 0800/0810/0820 message sequences to complete encryption key exchanges with the MDS. The key information is stored in DE 48, subelement 11 in the following format:

Table 6.3—Key Information Format

Subfield	Attribute	Value
Subtag ID	n-2	11
Subtag Length	n-2	70
Key Class Identifier	an-2	PK (Pin key exchange
Key Index Number	n-2	00 (constant)
Key Cycle Number	n-2	00-99
Encrypted Key	an-48	Hexadecimal characters 0-9, A-F; **triple key length**
Key Check Value	an-16	The key check value consists of the first four hexadecimal characters (0-9, A-F) of the calculated check value followed by spaces.

Member Testing

The MasterCard Debit Financial Simulator version includes enhancements to support testing of triple DES encryption. During testing, MasterCard requires acquirers and issuers to test with the MDS, verifying that they are able to support triple DES encryption. The MDS tracks the encryption method used at the issuer and processor levels and generates the appropriate key exchanges and PIN translations.

For more information about the conversion to triple DES encryption, please contact Debit Customer and Technology Support:

Telephone: 1-914-249-5620

Fax: 1-914-249-4301

Network Key Management Responsibilities

MasterCard Debit Switch

1. Identify, authorize, and brief the appropriate staff for management of the master key and the communications keys.
2. Appoint communication key-part holders.
3. Keep the key parts in dual custody.
4. Coordinate the exchange of new communication keys with each processor on an annual basis.
5. Initiate dynamic online key exchanges as required.

Processors

1. Select and purchase a hardware security module.
2. Demonstrate ability to receive and process working key exchange requests.
3. Demonstrate ability to translate PINs from one key to another in hardware.
4. Develop procedure for managing the communication key.
5. Identify, authorize, and brief the appropriate staff for management of the master key and the communications keys.
6. Appoint communications key-part holders.
7. Keep the logical key parts under dual control.

Note **It is recommended that security officers selected for key management not have extensive technical backgrounds.**

All PINs must be encrypted at the point of entry using the DES algorithm and the approved ANSI PIN Block Format. The ANSI PIN block is the only format supported by the MDS. Below is the description of the PIN block creation.

ANSI PIN Block Format

A technical staff member builds the ANSI PIN block by performing a binary "Exclusive OR" of the two sixteen-hexadecimal digit data elements together.

1. The first hexadecimal data element contains cardholder PIN information.
   a. The first digit is zero.
   b. The second digit is the length of the PIN (such as 4-9, A (10), B (11), or C (12). The maximum length is twelve digits.
   c. The third digit is the start of the cardholder PIN; twelve is the maximum length.
   d. The PIN is padded on the right with hexadecimal "F"s to complete the 16-digit data element.
2. The second hexadecimal data element contains Primary Account Number (PAN) information.
   a. The first four digits are set to zero.
   b. The next 12 digits of the data element contain the right-most 12 digits of the Primary Account Number (PAN), excluding the check digit. If the PAN contains 12 or less digits, then the entire PAN excluding the check digit is used. The field is padded on the left with zeros to complete the 16-digit data element.

The two hexadecimal data elements are "Exclusive OR'ed" to obtain the ANSI PIN Block result.

PIN Encryption

The acquirer must send the entered PIN to the MasterCard® Debit Switch, encrypted in an ANSI block format (Figure 6.4). The acquirer must meet the following requirements when encrypting a PIN:

1. The first digit of the first block will contain the control character 0, followed by a number representing the length of the PIN, and then the PIN itself. The remaining digits of the block are filled with the pad character "F".
2. The first four characters of the second block will contain 0000, followed by the 12-rightmost digits of the PAN, excluding the check digit.
3. In formatting an ANSI block, the acquirer will "Exclusive-OR" (XOR) the two 16-digit blocks.

4. After creation of the PIN block, it is sent through the DES algorithm with the 16-digit, 32-digit or 48-digit key (KPE), producing the encrypted PIN block, which is sent to the MDS.
5. The MDS will translate the PIN block from encryption under the KPE it shares with the acquirer to encryption under the KPE that it shares with the issuer.
6. The MDS then forwards the newly encrypted PIN block in the authorization request message to the issuer.

Note

The MDS performs PIN validation services for some issuers using the Authorization Request/0100 message type. For those issuers, the MDS will not translate the acquirer's encrypted PIN block as described in the steps above. The MDS will perform PIN validation. The Authorization Request/0100 message to the issuer will not contain the PIN block.

Figure 6.4—ANSI PIN Block

ENTERED PIN "1234"
PAD "F"
KPE "935A342A1122B33B"
ACCOUNT# "5415973333334456"
PARTIAL PAN "597333333445"

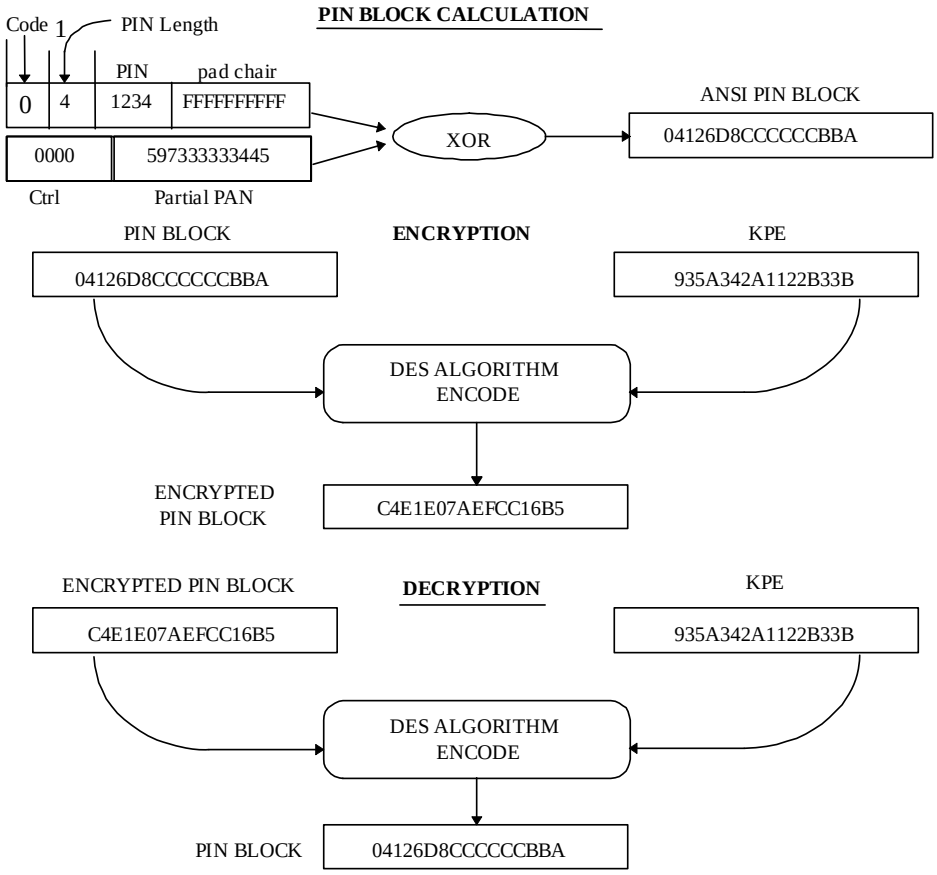


Figure 6.5—ANSI PIN Block Encryption - Double Length Key

ENTERED PIN "1234"
PAD "F"
KPE "5EA10DEFB073E586 EF68FD7A612A19F2"
ACCOUNT# "5415973333334456"
PARTIAL PAN "597333333445"

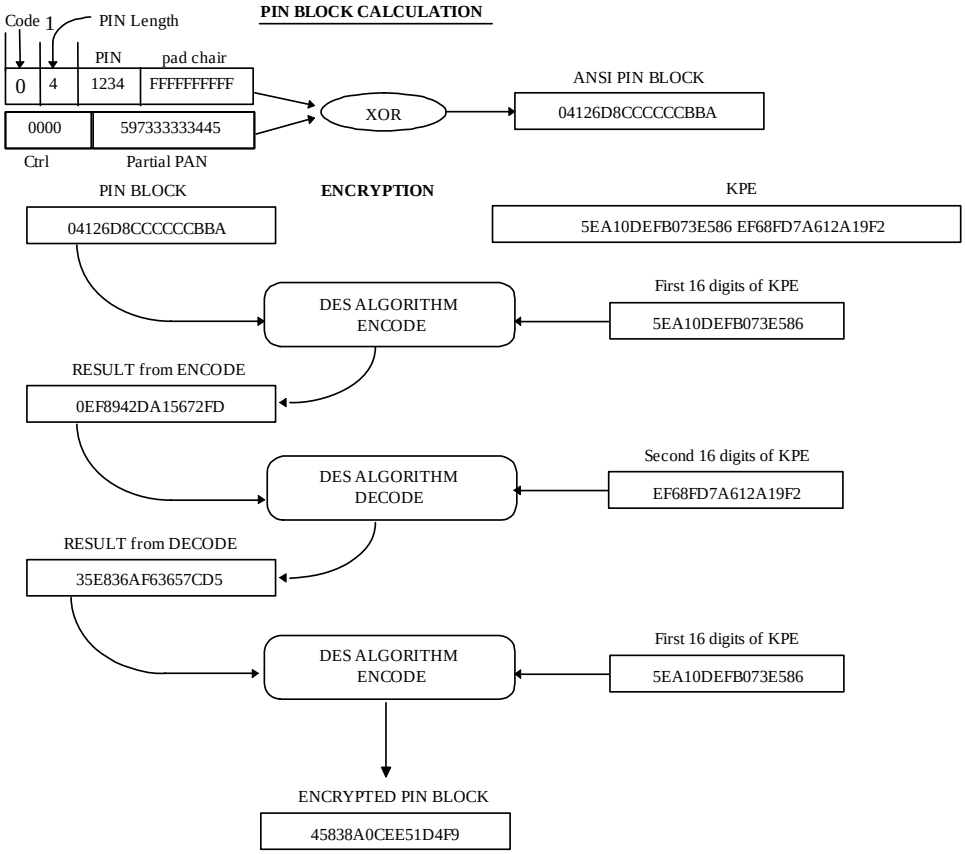


Figure 6.6—ANSI PIN Block Decryption - Double Length Key

ENTERED PIN "1234"
PAD "F"
KPE "5EA10DEFB073E586 EF68FD7A612A19F2"
ACCOUNT# "5415973333334456"
PARTIAL PAN "597333333445"

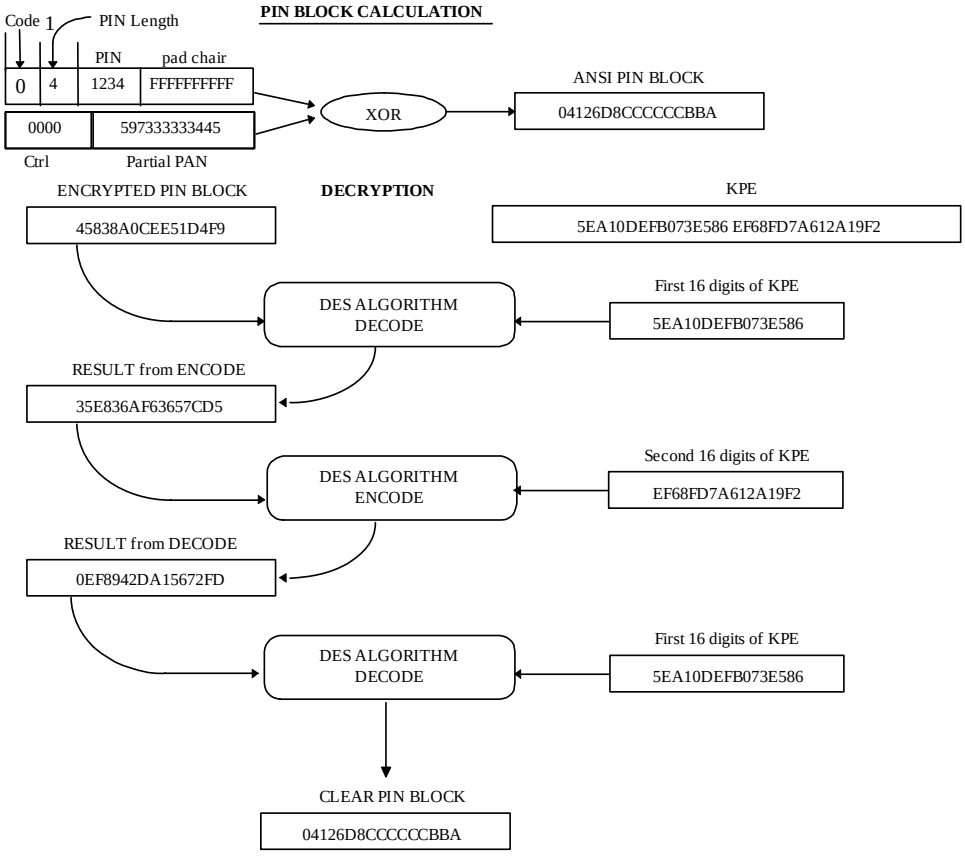


Figure 6.7—ANSI PIN Block Encryption - Triple Length Key

ENTERED PIN "1234"
PAD "F"
KPE "9297F7B58A0E1649 9E58F48CBA1C57C2 37B35EC2A715707F"
ACCOUNT# "5415973333334456"
PARTIAL PAN "597333333445"

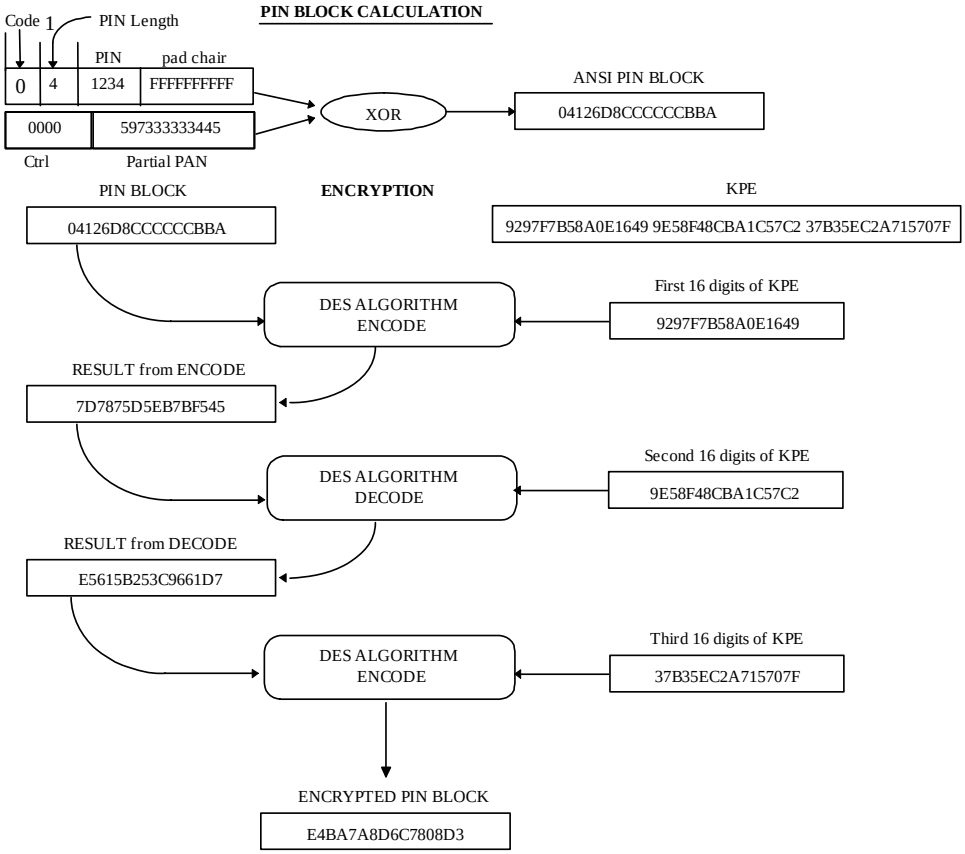
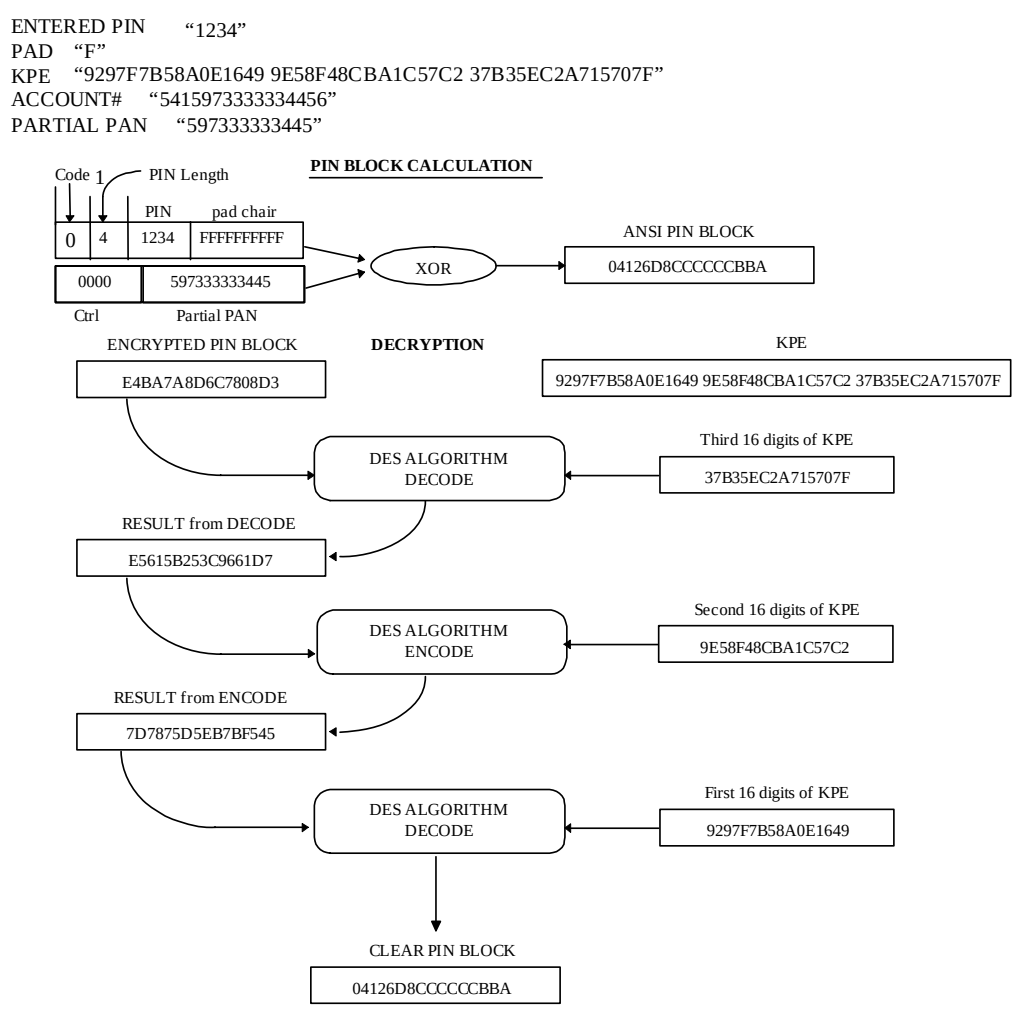


Figure 6.8—ANSI PIN Block Decryption - Triple Length Key



Sanity Checks

All physically-secure devices (PSD) must be able to detect possible working key corruption by verifying that the clear text PIN block is in the expected format. Failure of this sanity check should result in a denied transaction and the initiation of the key exchange sequence between the processor and MDS.

Security Provisions

The security provisions at the MasterCard® Debit Switch require adherence to the following:

- All terminals must encrypt PINs in a physically secure device using the ISO approved algorithm(s) for PIN encipherment listed in ISO 9564–2 (DES algorithm) and a working key that is used at the terminal (ATM or POS). Working keys that are loaded manually must be loaded in a dual control environment.
- MasterCard recommends that the same working key not be assigned to any two terminals driven by the same hardware, software, or both in a predictable manner.
- All keys must be stored encrypted using the ISO approved algorithm(s) for PIN encipherment listed in ISO 9564-2 (DES algorithm) and a proprietary master key. Alternately, keys may be stored within a physically secure device. All encryption/decryption processing must occur within a physically secure device.
- All intermediate network facilities (INFs) between the terminal and the issuer processor must receive and send customer entered PINs in the form of a cryptogram to other INFs using the ISO approved algorithm(s) for PIN encipherment listed in ISO 9564-2 (DES algorithm) and working keys statically or dynamically maintained by the INFs processing MDS activity.
- PINs may be decrypted and re-encrypted, during INF transmission processing, to change the format of the PIN block or the working key used to protect the PIN. It must be translated in a physically secure device.
- Working keys maintained dynamically must be used for no more than 12 hours.

Oct 2005

PIN Generation Verification

The MDS supports two methods of PIN generation verification. Below is a description of each methodology.

IBM 3624

To generate PINs using the IBM 3624 method (Figure 6.9), the institution must determine whether it will support customer-selected PINs and establish the following:

- Validation data
- PAN pad character
- Decimalization table
- DES Key (KPV)

The validation data is a portion of the PAN used in constructing the first 16-digit block. If the portion of the PAN being used is less than 16 digits, this data is left- or right-justified, and padded with the PAN pad character. This block, along with the 16-digit KPV, is sent through the DES algorithm to produce a 16-digit generated PIN block.

The decimalization table is then applied to the generated PIN block to map all alphabetic characters to numeric digits. The resulting block is called the natural PIN block.

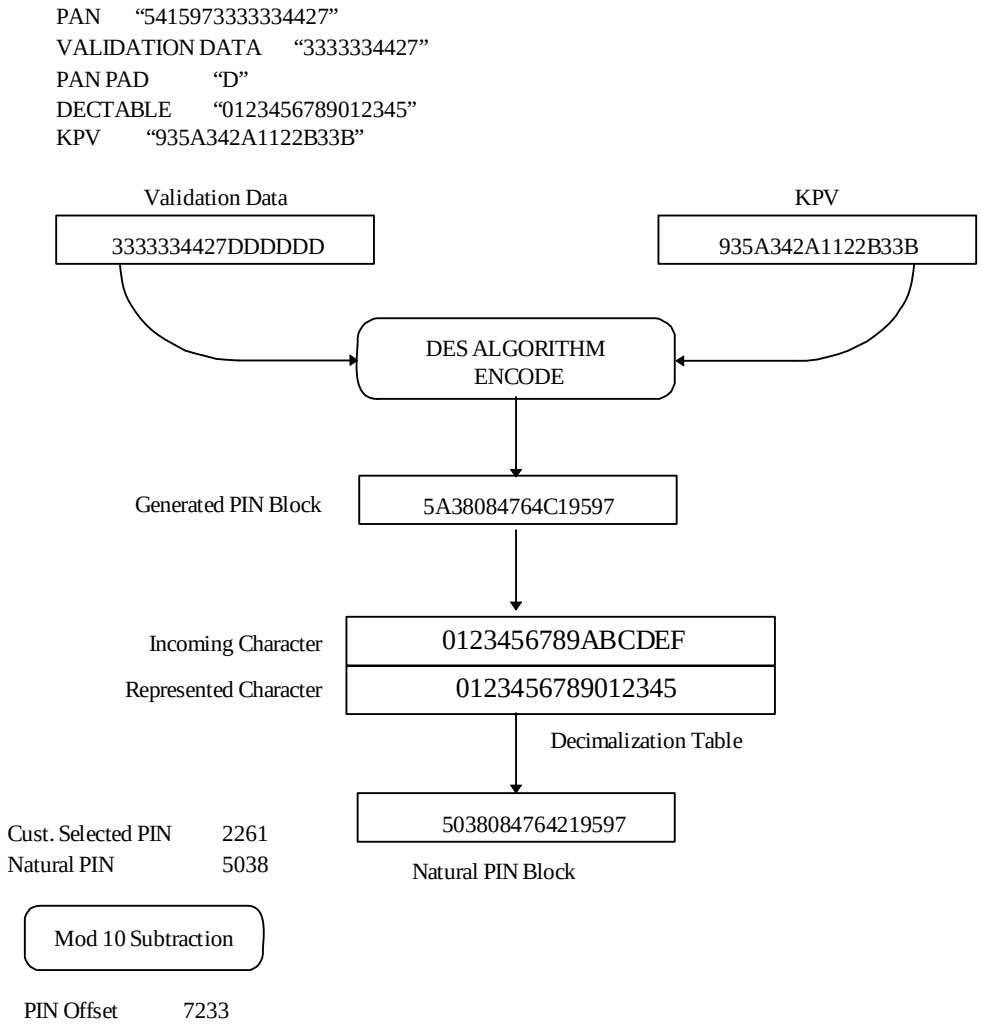
The MDS security hardware requires that the member use at least eight distinct digits to create the decimalization table. The member may not use any digit more than four times.

If customer-selected PINs are supported, then the MDS will need the location of the PIN offset that is produced during generation; this is encoded on Track-2 of the card's magnetic stripe.

If the institution does not support customer-selected PINs, the first 4 through 12 digits are the PIN assigned to the customer. This PIN, called the natural PIN, explicitly implies that the PIN offset is all zeros.

The customer-selected PIN is module 10 subtracted from the natural PIN block to produce the PIN offset.

Figure 6.9—IBM 3624 PIN Generation



ABA

To generate PINs using the ABA method (Figure 6.10) the institution must determine the following:

- Validation data
- PVKI (PIN verification key index)
- Key left
- Key right
- PIN (customer-selected)

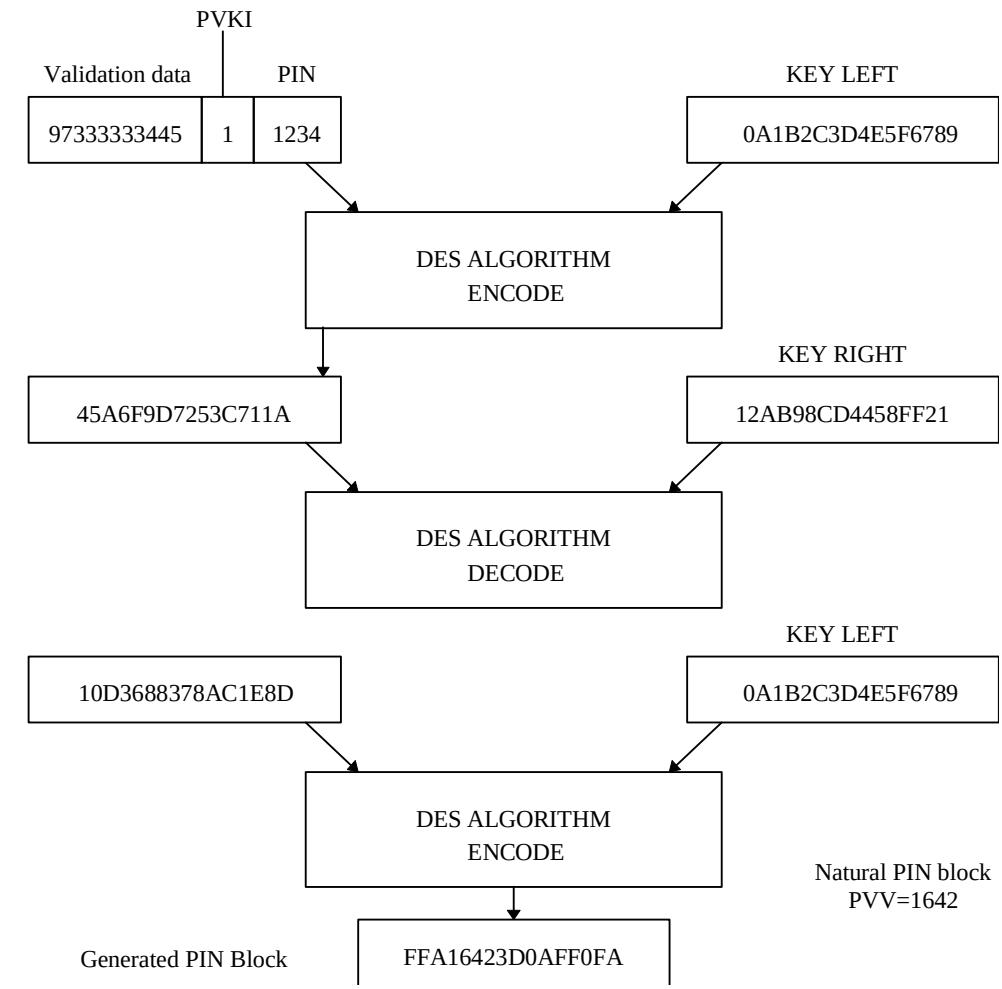
This generation process will produce a PVV (PIN verification value), which is encoded on track 2 of the card's magnetic stripe.

The validation data is the last 11 digits of the PAN, excluding the check digit. The PVKI is appended to the validation data, which is in turn appended by the PIN to complete the 16-digit block.

This block along with the 16-digit key left is sent through the DES algorithm to produce another 16-digit block. The resultant block is sent through DES using the 16-digit key right, producing a new 16-digit resulting block. This new block is sent through DES with the key left to produce the final block called the generated PIN block.

The PVV is determined by taking the first four numeric digits of the natural PIN block. If there are not four numeric digits, the A-F are mapped to 0-5, and the remaining digits of the PVV are completed.

Figure 6.10—ABA PIN Generation



Any intermediate network facility (INF) that is not a processor and does not translate, use, or verify PIN or key data for any transaction processed by such INF is not subject to any of the provisions listed above.

Required Functionality

Using a physically secure device (PSD) only, a processor must be able to support the functionality indicated in Table 6.4 and Table 6.5.

Note **Software emulation of these DES security functions are not permitted under MasterCard/ Cirrus® and Maestro® Operating Rules.**

Table 6.4—Key Management Functions

Functionality	MDS	Processors	Others [a]	Terminals
Store Master Key	Required	Required	Required	N/A
Establish/reset Communication Key	Required	Required	Required	Required
Generate working key	Required	Optional	Optional	N/A
Receive working key	N/A	Required	Optional	Required

[a] Processors or networks not directly connected to the MDS.

Table 6.5—PIN Processing Functions

Functionality	MDS	Processors	Others [a]	Terminals
Encrypt PIN	Required	Required	Required	Required
Verify PIN	N/A	Required (IPS)	Optional	Optional (IPS)
Translate from ANSI to ANSI	Required	Optional	Optional	N/A
Translate from PIN PAD to ANSI	N/A	Required	Optional	N/A
Translate from ANSI to PIN PAD	N/A	Optional	Optional	N/A
Translate from Clear to ANSI	Required	Required	Required	N/A
Translate from ANSI to Clear	Required	Required	Required	N/A

[a] Processors or networks not directly connected to the MDS.

Detection of Working Key Corruption

All PSDs must be able to detect possible working key corruption by verifying that the clear text PIN block is in the expected format. Failure to perform this sanity check should result in a denied transaction and the initiation of a key exchange sequence between the INFs where the corruption is detected.

After there has been a successful working key exchange, it is the responsibility of the processor and of the MDS to preserve the old working key for a period of five minutes. If the system receives a sanity check error during this five-minute period, the system should try the old working key before returning an error. If the stored key receives a sanity check, the system should return a response code appropriate to the type of message format used.

Fallback to Clear Text

In the event of a major problem with security equipment (for example, a faulty PSD or DES circuit board), the MDS will have no choice but to suspend all transaction processing with the processor.

Note **Use of clear text processing of transactions is expressly prohibited by the Operating Rules.**

Emergency Communication Key Procedures

In the event that a successful working key exchange cannot be performed, the MDS will invoke the emergency communication key procedure using the following procedures:

1. The MDS marks the faulty processor as down.
2. Authorized MDS personnel randomly generate an emergency communication key (generating both parts of the key).
3. MDS personnel call the security or operations staff at the processor. The emergency communication key is given verbally to the processor.
4. Both the MDS and the processor insert the new emergency communication key in their security modules.
5. The MDS initiates key exchange and log-on, using the new emergency communication key.

The emergency communication key procedure is to be used only as an interim measure to enable a processor to resume transaction processing with the MDS as quickly as possible following a key exchange failure. The personnel responsible for key management must be notified immediately of the security failure situation and must conduct a secure key exchange at the earliest possible time.

Use of the emergency communication key in any one occurrence is limited to six business days. After such time, the processor must have reestablished the jointly established communication key, in accordance with the provisions outlined in this chapter.

Key Naming Convention

The master key encrypts the working key and communication key for storage.

The communication key is used to encrypt and decrypt the working key in the MDS or CIS ISO 8583-1987 Network Management/0800.

The working key is used to encrypt the PIN block in DE 52 of the Financial Transaction Request (Pre-Authorization)/0200 message.

Table 6.6—Functional versus Vendor-Specific

FUNCTIONAL	ATALLA	RACAL
Master	MFK (Master File Key)	LMK (Local Master Key)
Communication	KEK (Key Exchange Key)	ZMK (Zone Master Key)
Working	KPE (Key PIN Encryption)	ZPK (Zone PIN Key)

7 Database Forms

This chapter describes the procedures for completing the forms to establish the member participation database in the MDS network.

Overview

This chapter describes the procedures for completing the forms to establish the member participation database on the MDS. The MDS requires two forms: the Institution Routing Table form and the Institution Definition File form. The Institution Routing Table form establishes the card prefix for routing purposes (issuer-only participation). The Institution Definition File form defines the financial institution (issuing and acquiring participation).

MasterCard encourages members and processors to complete the Institution Routing Table and Institution Definition File forms using the electronic version of the forms and submitting them to the designated e-mail address. Members and processors may also use this e-mail address to request an electronic copy of the forms:

E-mail: MDS_Database_Forms@mastercard.com

Contact Debit Product Support for any questions concerning the Institution Routing Table or Institution Definition File forms or procedures.

Phone: 1-914-249-5620

Institution Definition File (IDF)

The MDS database identifies each financial institution participating in the MDS network through a unique routing and transit number established on the Institution Definition File form. This pertains to issuing and acquiring. The Institution Definition File form also defines the products supported by the acquiring institution and the processor providing the acquiring service.

Procedures to Complete an Institution Definition File Form

Table 7.1 lists the descriptions of all field names on the Institution Definition File form.

Note **A financial institution requesting to add a new member, modify (see exceptions below), or transfer to a new processor must complete the applicable licensing contracts before the MDS can update any information on the MDS database.**

Table 7.1—IDF Field Descriptions

Field	Description
Indicate Action	Indicates a new or change in status of members
	Add — Request to add a new member/routing and transit number
	Modify — Request to modify any existing information on the form The following changes require a new licensing contract: • Name change • City and/or State change • Network participation change (Cirrus issuer and acquirer to acquirer-only member or acquirer-only member to Cirrus issuer and acquirer) • Change in acquirer supported products (adding Plus and Visa) To modify an existing routing and transit number (R&T), two Institution Definition File forms must be submitted; one to delete the old R&T and the other to add the new routing and transit number (R&T).
	Delete — Request to delete a routing & transit number The Operating Rules require six months' notification to leave the network. The financial institution must submit a letter of termination with the Institution Definition File six months before deletion.
	Transfer — Request to change acquiring processor Financial institutions transferring to a new processor must obtain approval from their current principal member. A signature from the principal member is required on the Institution Definition File form before the transfer can become effective in the MDS network. Processor-only changes (when the principal member remains the same) do not require a new licensing contract. However, the principal member must submit the paperwork.
New Principal Member Contact	The name of the new principal member contact
– Phone	The contact number of the new principal member contact
Current Principal Member Institution	The name of the current principal member institution
– Phone	The contact number of the current principal member institution
Current Principal Member Approval (Print)	The name of the current principal member approving the request
Current Principal Member Approval (Signature)	The signature of the current principal member approving the request
– Date	The date the current principal member approved/signed the request

Field	Description
Effective Date	MasterCard must receive the Institution Definition File form no later than ten (10) business days prior to the requested effective date. MasterCard considers any request within this period expedite processing and will levy a fee. Refer to the "Exceptions" subsection for additional information.
Institution (R&T) Number	The Federal Reserve routing and transit number of the institution or a nine-digit number assigned by MasterCard to identify the financial institution as a member of the network
Institution Name	The name of the participating institution (limit to a maximum of 25 alphanumeric characters)
ICA Number	A six-digit identification number (assigned by MasterCard) of a financial institution, third-party processor, or other type of customer, identifying the participant as a member of MasterCard MasterCard requires ICA number assignments for all MasterCard BINs within the 51-55 BIN range. Contact the Franchise Management Department for all ICA number assignments.
City	The city where the main office of the institution is located (limit to a maximum of 12 alphanumeric characters)
State	The State where the main office of the institution is located This field must contain the ISO defined state code (refer to the *Quick Reference Booklet*)
Numeric Currency Code	The local currency of the institution This field must contain the ISO-defined numeric currency code (refer to the *Quick Reference Booklet*).
Numeric Country Code	The ISO-defined Country Code of the institution (refer to the *Quick Reference Booklet*).
Processor Number	A unique number the MDS assigns to identify a specific processor
Processor Name	The name of the processor providing the network services (limit to a maximum of 25 alphanumeric characters)
Principal Member Name	The Principal Member that sponsors the institution into the MDS network
Acquirer-Only Participation	Check **Yes** or **No** to indicate if the member is an acquirer-only participant
Acquirer Product Participation	The specific products the acquirer will support in the MDS network Identify the product(s) supported by checking the boxes next to the specific products.
Additional Comments	Any other relevant instructions or information
Prepared by	The name of the principal member completing the form
– Date	The date the principal member completed the form

Field	Description
– Phone	The contact number of the principal member completing the form
Approved by	The name of the principal member approving the request
– Date	The date the principal member approved the request
– Phone	The contact number of the principal member approving the request

Institution Routing Table (IRT)

The MDS database identifies each card prefix for an issuing financial institution participating in the MDS network through the information established on the Institution Routing Table form. The Institution Routing Table form also defines the products supported by the issuing institution and the processor that is providing the authorization service for each product.

Procedures to Complete an Institution Routing Table Form

Table 7.2 lists the descriptions of all field names on the Institution Routing Table form.

Table 7.2—Institution Routing Table Field Descriptions

Field	Description	
	Indicates a new or change in status of members	
	Add	Request to add a new BIN
	Modify	Request to modify any existing information on the form To modify an existing BIN, two IRT forms must be submitted; one to delete the old BIN and the other to add the new BIN. Members must use the Institution Definition File form to request a name change.
	Delete	Request to delete a BIN The Operating Rules require six months' notification to leave the network. The financial institution must submit a letter of termination with the Institution Routing Table form, six months before deletion.

Field	Description
	Transfer Request to change issuing processor Financial institutions transferring BINs to a new processor must obtain approval from their current principal member. A signature from the principal member is required on the IRT form before the transfer can become effective in the MDS network. Processor-only changes (when the principal member remains the same) do not require a new licensing contract. However, the principal member must submit the paperwork.
New Principal Member Contact	The name of the new principal member contact
– Phone	The contact number of the new principal member contact
Current Principal Member Institution	The name of the current principal member institution
– Phone	The contact number of the current principal member institution
Current Principal Member Approval (Print)	The name of the current principal member approving the request
Current Principal Member Approval (Signature)	The signature of the current principal member approving the request
– Date	The date the current principal member approved/signed the form
Effective Date	MasterCard must receive the Institution Routing Table form no later than ten (10) business days prior to the requested effective date. MasterCard considers any request within this period expedite processing and will levy a fee. Refer to the "Exceptions" subsection for additional information.
Prefix Number (BIN)	The ISO (MasterCard or Visa assigned) BIN number encoded on the card to identify the owner of the prefix. The BIN number must be 5–11 positions in length and is used for transaction routing.
MDS Priority Routing	A service identified at the BIN level to indicate if the BIN will be priority routed to the MDS as the "preferred" network.
PAN Length	The length of the Primary Account Number (PAN). The Institution Routing Table form must indicate if the BIN supports multiple PAN lengths.
Institution (R&T) Number	The Federal Reserve routing and transit number of the institution or a nine-digit number assigned by MasterCard to identify the financial institution as a member of the network
Card Type	Indicates if the prefix is a debit or credit BIN
Institution Name	The name of the participating institution (limit to a maximum of 25 alphanumeric characters)

Field	Description
ICA Number	A six-digit identification number (assigned by MasterCard) of a financial institution, third-party processor, or other type of customer, identifying the participant as a member of MasterCard MasterCard requires ICA number assignments for all MasterCard BINs within the 51-55 BIN range. Contact the Franchise Management Department for all ICA number assignments.
State	The State where the main office of the institution is located This field must contain the ISO defined state code (refer to the *Quick Reference Booklet*)
Numeric Currency Code	The local currency of the institution Members must use the ISO-defined numeric currency code in the field (refer to the *Quick Reference Booklet*)
Numeric Country Code	The ISO-defined Country Code of the institution (refer to the *Quick Reference Booklet*)
Processor Number	A unique number the MDS assigns to identify a specific processor
Processor Name	The name of the processor providing the network services (limit to a maximum of 25 alphanumeric characters)
Principal Member Name	The Principal Member that sponsors the institution into the MDS network
PIN Validation	Indicates if the MDS or the issuer will perform the PIN validation on ATM transactions for 0100 MasterCard credit card BINs processed through the Banknet interface If the MDS performs PIN validation, the PIN Processing Profile form must be completed with the Institution Routing Table form to indicate the PIN validation methodology and the specific parameters for the MDS database.
GSI	For MasterCard use only
Mirror BIN	Indicates an existing BIN in production which has the same set up on the MDS database that is being requested
ATM Product Participation	The specific ATM product(s) the issuer will support in the MDS network Identify the product(s) supported by checking the boxes next to the specific products
Maestro ATM Processor Number	The Maestro ATM processor number if different from the Maestro POS processor
ATM Credit Processor Number	The processor number providing the credit authorization services
POS Product Participation	The POS product(s) the issuer will support in the MDS database Identify the product(s) supported by checking the boxes next to the specific products
POS Processor Number	The POS processor number for each specific product type

Field	Description
Prepared by	The name of the principal member completing the form
– Date	The date the principal member completed the form
– Phone	The contact number of the principal member completing the form
Approved by	The name of the principal member approving the request
– Date	The date the principal member approved the request
– Phone	The contact number of the principal member approving the request

Exceptions

This subsection includes information about pseudo routing and transit numbers, BIN deletes, and expedite/emergency database changes.

Pseudo Routing and Transit Numbers

A pseudo routing and transit number is a nine-digit number (assigned by MasterCard) that identifies a financial institution as a member of the network (under the following conditions):

- As a temporary assignment to accommodate an issuing and/or acquiring member conversion to a new processor. The pseudo number identifies the member under the new processor until the actual routing and transit number can convert.
- To support dual sponsored memberships
- To establish Non-Member Terminal Agreement and Service Mark License members
- To facilitate a processor's internal settlement and reconciliation process

BIN Deletes

All BIN delete requests in the MDS network are performed weekly and occur on Monday. This exception minimizes the impact to members and their cardholders if a BIN is deleted in error, and provides the opportunity to reactivate the BIN before the next BIN file distribution to MDS processors on Thursdays.

Expedite/Emergency Database Changes

The Institution Routing Table form and the Institution Definition File form must be completed and submitted to MasterCard no later than ten (10) business days prior to the requested effective date. MasterCard may, at its discretion and upon request and approval from a principal member, facilitate file updates of IRT and IDF input documents received less than the required ten (10) business days.

In these cases, the principal member will be subject to a forms handling fee per BIN and routing and transit number (see Table 7.3).

Table 7.3—Handling Fees

Submission Time Frame	Fee amount (USD)
Within 5-9 business days of effective date	500
Less than 5 business days of effective date	1000
Within 24 hours of effective date	3000
MDS PIN validation set-up (per BIN)	250

Note **MasterCard will validate each request to confirm the applicable license contract is in place before processing any IRT and IDF expedite update requests.**